



# VIPER SC™ VIPER SC+™ IP ROUTER FOR LICENSED SPECTRUM



User Manual  
PN 001-5008-000 Rev 11  
Revised August 2011

## REVISION HISTORY

REV	DATE	DESCRIPTION
REV 0	Jan 2008	Initial Release as 001-5008-000.
REV 1	May 2008	Update Dual Port Viper SC information.
REV 2	Sept 2008	Added information about SNMP. Updated Firmware Upgrade instructions.
REV 3	Dec 2008	Added information about TCP Client Server Mode. Added information about Saving/Restoring User Configuration files.
REV 4	Apr 2009	Added information about V1.5 Viper SC code release. Added information about TCP Proxy Feature. Added note to RF Acknowledgment section. Corrected Viper SC Power Cable Part in Accessory Table. Added specifications and part number for 900 MHz Viper SC. Updated RF Exposure Compliance requirements. Added Choosing an IP Addressing Scheme
REV 5	Jul 2009	Added information about V1.6 Viper SC code release. Added information about Listen Before Transmit Disable feature. Added section about RF MAC override feature. Added section about the Periodic Reset feature. Added screen shot and information for the "Add Static Entry" function
REV 6	Sept 2009	Added Listen Before Transmit Disable Feature. (Previously Read: Added Listen Before Talk Disable Feature).
REV 7	Nov 2009	Updated user manual for product name change from ViPR to Viper SC
REV 8	Jun 2010	Added UL information. Added information and specifications for Viper SC-200. Added information about V1.7 Viper SC firmware Release. Corrected radio firmware upgrade command line instructions errors in Section 13.3 that were introduced in revision 7 of the user manual. Added section about VPN. Added section about Radius. Updated SNMP section. Updated screen captures and descriptions
REV 9	Sept 2010	Rebranded for Viper SC, Updates to Security – VPN Section 4.5.3.
REV 10	Aug 2011	Added VHF ETSI Viper Part Numbers and ETSI Base Station part numbers (Section 1.5). Added sensitivity numbers for VHF ETSI Viper (Appendix A). Added additional regulatory certifications for VHF ETSI Viper (Appendix B). Updated VHF ETSI frequencies from 136-174 to 142-174MHz. Added frequency ranges for ETSI and AS/NZ compliant models in section 1.2. Rearranged model number layout in Appendix A. Added standards information to Appendix B. Updated RF Exposure Compliance Recommendations. Updated Unit Identification and Status mode selection, section 4.1.1. Updated Diagnostics Info – SNR from RF-MAC, section 4.1.2. Channel Table/Current Settings mode selection changed, section 4.3.3. Multicast section updated, section 4.4.3. IP Optimization updates, section 4.4.4. VPN Configuration updates, section 4.5.3. Remote Statistics added, section 4.6.3. SINAD Meter added to RF Tests, section 4.7.5. Wing Commander pages added, section 4.7.6.
REV 11	Aug 2011	Updated EU and EFTA Member States' Acceptable Frequency Table in Appendix B.
REV 12a	July 2013	Add ViperSC+ Model Numbers

## 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 Viper SC are used in a normal manner with a well-constructed network. Viper SC 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 Viper SC, or for the failure of Viper SC to transmit or receive such data.

## Copyright Notice

© 2010 CalAmp. All rights reserved.

Products offered may contain software proprietary to CalAmp. The offer of supply of these products and services does not include or infer any transfer of ownership. No part of the documentation or information supplied may be divulged to any third party without the express written consent of CalAmp. 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.

## RF Exposure Compliance Requirements



The Viper SC radio is intended for use in the Industrial Monitoring and Control and SCADA markets. The Viper SC 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.

Min Safety Distance (cm @max power)	Antenna Gain		
	5 dBi	10 dBi	15 dBi
VHF	123cm	219cm	389cm
UHF	122cm	217cm	386cm
900 MHz (Model # 1405098304)	66 cm	117 cm	208 cm
900 MHz (Model # 1405098504)	64 cm	114 cm	202 cm

*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 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.*

Viper SC 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.

Recommended safety guidelines for the human exposure to radio frequency electromagnetic energy are contained in the Canadian Safety Code 6 (available from Health Canada), the Federal Communications Commission (FCC) Bulletin 65 and the Council of the European Union's Recommendation of 12 July 1999 on the limitation of exposure of the general public to electromagnetic fields (0 Hz to 300 GHz) (1999/519/EC).

## **Class A Digital Device Compliance**

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

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.

<b>1</b>	<b>PRODUCT OVERVIEW</b>	<b>1</b>
1.1	General Description	1
1.2	Operational Characteristics	1
1.3	Physical Description	2
1.3.1	Chassis Dimensions	2
1.3.2	LED Panel	2
1.3.3	Front Panel	3
1.4	Product Warranty	5
1.5	Models and Availability	5
<b>2</b>	<b>NETWORK ARCHITECTURE AND SYSTEM PLANNING</b>	<b>9</b>
2.1	Network Architecture	9
2.1.1	Point-to-Point	10
2.1.2	Point-to-Multipoint	10
2.1.3	Report by Exception	11
2.1.4	Extending the Coverage Area with a Relay Point	11
2.2	IP Forwarding Modes	11
2.2.1	Bridge Mode	12
2.2.2	Router Mode	14
2.2.3	Multispeed Networking	16
2.3	System Planning	17
2.3.1	Understanding RF Path Requirements	17
2.3.2	Terrain and Signal Strength	18
2.3.3	Radio Interference	18
2.3.4	Selecting Antenna and Feedline	18
<b>3</b>	<b>QUICKSTART</b>	<b>20</b>
3.1	PC LAN Setup	20
3.2	Install the Antenna	20
3.3	Measure and Connect Primary Power	20
3.4	Connect Viper SC to Programming PC	21
3.5	Configure Your Viper	21
3.5.1	Initial Installation Login	21
3.5.2	Setup Wizard	22

- 4 WEB INTERFACE ..... 26**
- 4.1 Unit Status ..... 27**
  - 4.1.1 General..... 27
  - 4.1.2 Diagnostics ..... 28
- 4.2 Setup Wizard ..... 31**
- 4.3 Basic Setup ..... 31**
  - 4.3.1 General..... 31
  - 4.3.2 IP Settings ..... 33
  - 4.3.3 Channel Table ..... 34
  - 4.3.4 Serial Ports ..... 36
- 4.4 Setup (Advanced) ..... 41**
  - 4.4.1 RF Optimizations/MAC Advanced Settings ..... 42
  - 4.4.2 IP Services ..... 44
  - 4.4.3 IP Addressing..... 55
  - 4.4.4 IP Optimization ..... 57
  - 4.4.5 IP routing..... 59
  - 4.4.6 Time Source ..... 59
  - 4.4.7 Alarm Reporting/Diagnostic Settings..... 60
  - 4.4.8 User Settings ..... 61
- 4.5 SECURITY ..... 62**
  - 4.5.1 Password and Encryption..... 62
  - 4.5.2 Radius..... 62
  - 4.5.3 VPN ..... 65
- 4.6 STATISTICS..... 72**
  - 4.6.1 Ethernet Interface..... 73
  - 4.6.2 Serial Interface ..... 73
  - 4.6.3 RF Interface ..... 73
- 4.7 MAINTENANCE ..... 75**
  - 4.7.1 Ping Test..... 75
  - 4.7.2 Config Control ..... 76
  - 4.7.3 Package Control ..... 77
  - 4.7.4 Net Tests ..... 77
  - 4.7.5 RF Tests ..... 80
  - 4.7.6 Wing Commander ..... 80
  - 4.7.7 Feature Options ..... 83

<b>4.8</b>	<b>NETWORK MANAGEMENT/NEIGHBOR TABLE .....</b>	<b>83</b>
4.8.1	Neighbor Discovery .....	84
4.8.2	Status .....	89
4.8.3	Maintenance .....	89
<b>5</b>	<b>NETWORK OPTIMIZATION .....</b>	<b>90</b>
<b>5.1</b>	<b>Maximizing TCP/IP Throughput .....</b>	<b>90</b>
<b>5.2</b>	<b>Maximizing Throughput with a Weak RF Link .....</b>	<b>90</b>
5.2.1	Use Router Mode with RF Acknowledgements Enabled .....	90
5.2.2	Reduce RF Network Bit Rate .....	90
5.2.3	Increase OIP and MAC Retries Limit .....	91
<b>6</b>	<b>UPGRADING YOUR FIRMWARE .....</b>	<b>92</b>
<b>6.1</b>	<b>Upgrade Procedure (Modem) .....</b>	<b>92</b>
<b>6.2</b>	<b>Upgrade Procedure (Radio) .....</b>	<b>92</b>
<b>6.3</b>	<b>Verify File Integrity .....</b>	<b>94</b>
	<b>APPENDIX A – SPECIFICATIONS .....</b>	<b>95</b>
	<b>APPENDIX B – REGULATORY CERTIFICATIONS .....</b>	<b>102</b>
	<b>APPENDIX C – PRODUCT WARRANTY .....</b>	<b>106</b>
	<b>APPENDIX D – DEFINITIONS .....</b>	<b>107</b>

## 1 PRODUCT OVERVIEW

Viper SC provides any IP-enabled device with connectivity to transmit data. This DSP-based radio was designed for industrial applications utilizing 136-174 MHz, 215-240 MHz VHF, 406.1-512 MHz UHF, 880-902 and 928-960 MHz frequencies.

Operational as a wideband IP Modem or Router, Viper SC is optimized for use in SmartGrid, Distribution Automation, and SCADA applications. SCADA applications are defined as those with 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.

### 1.1 GENERAL DESCRIPTION

Designed to replace wire lines, the Ethernet and RS-232 serial ports allow direct connection to Programmable Logic Controllers (PLCs) or Remote Terminal Units (RTUs). Viper supports serial and Ethernet/IP Remote Terminal Units (RTU) and programmable logic controllers (PLC). It is standard IEEE 802.3 compliant. Viper 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

Viper has the following operational characteristics:

- Frequency range of 136-174 MHz, 215-240 MHz, 406.1-470 MHz, 450-512 MHz, 880-902 or 928-960 MHz
- 142-174 MHz, 406.1-470 MHz, and 450-512 MHz frequency ranges certified for European Union (ETSI EN300 113)
- 142-174 MHz, 406.1-470 MHz, and 450-512 MHz frequency ranges certified for Australia/New Zealand (ACMA AS/NZS 4925-2004 (Spectrum Impact Assessment))
- User-selectable data rates – up to 128 kbps @ 50 kHz
- Wide input power range of 10 to 30 volts DC
- 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
- Advanced AES 128-bit data encryption and security designed to meet FIPS 140-2 requirements
- 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
- Rugged die-cast aluminum and steel case
- UL Certified when powered by a listed Class 2 source



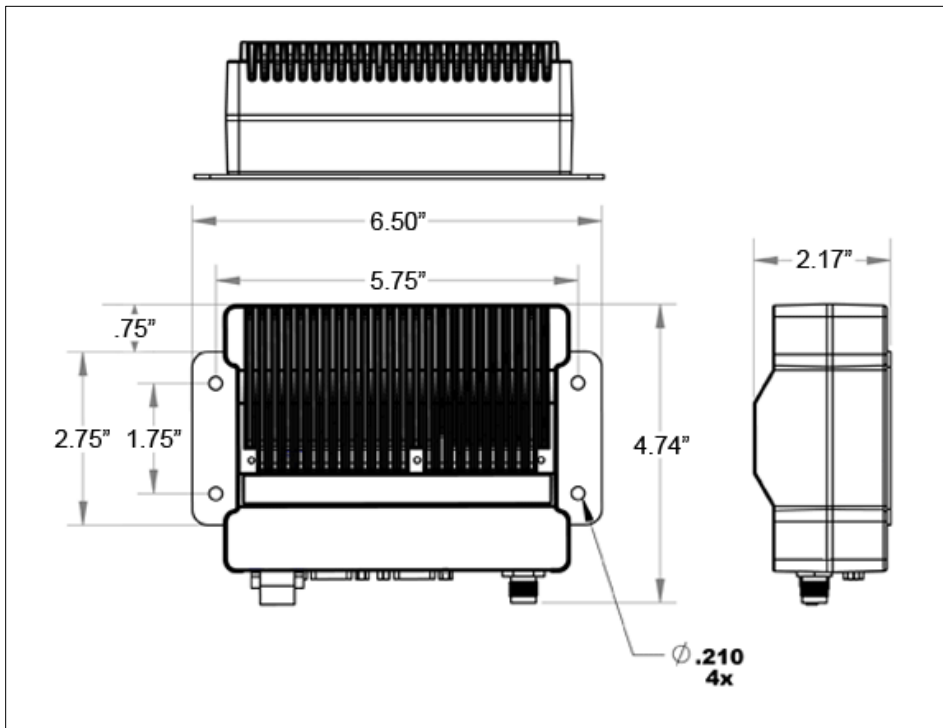
### 1.3 PHYSICAL DESCRIPTION

Viper 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.

#### 1.3.1 CHASSIS DIMENSIONS

Figure 1 shows the dimensions of the chassis and mounting plate.

**Figure 1 – Chassis and Mounting Plate**



**The equipment is intended for installation only in a RESTRICTED ACCESS LOCATION per EN60950-1:2006**

#### 1.3.2 LED PANEL

There are five (5) Tri-Color LEDs. Their functionality is shown in **Table 1**.

**Table 1 – LED Functionality**

LED	Color	Definition
Power	Green	Viper SC ready, normal operations
	Red	Viper SC hardware fault
Status	Green	Viper SC no faults, normal operations
	Blinking Green	Viper SC scanning for neighbors
	Red	Viper SC has a fault condition, check unit status
	Amber (Solid or Blinking)	Viper SC detects high background noise

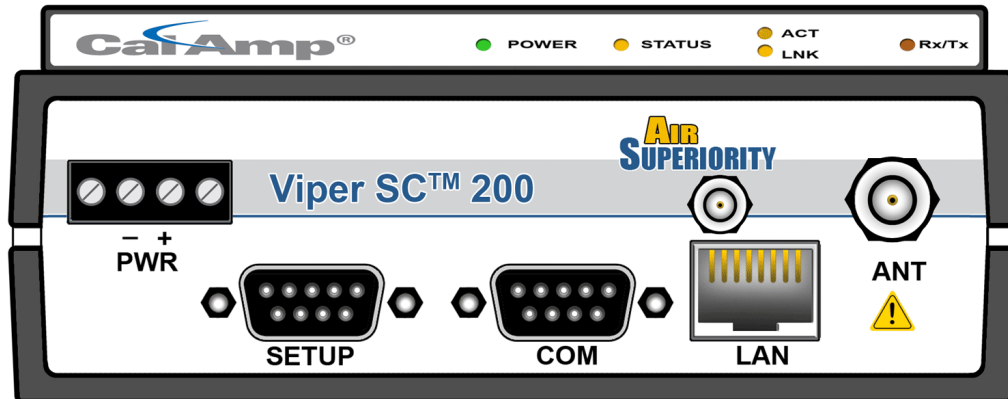
LED	Color	Definition
ACT	Blinking Green Off	Ethernet activity detected on PHY link (RJ45) No Ethernet activity on PHY link (RJ45)
Lnk	Green Off	Ethernet connection established (RJ45) No Ethernet connection (RJ45)
Rx/Tx	Green Red	Receiving data Transmitting data

### 1.3.3 FRONT PANEL

Shown in Figure 2, 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

Figure 2 – Front Panel (Dual Port Viper-200 Shown)



#### 1.3.3.1 ETHERNET LAN PORT

The Ethernet LAN port is an RJ-45 receptacle with a 10 BaseT Ethernet connection and Auto-MDIX. Refer **Table 2** for pin out descriptions and Section 4.6.1 to configure the LAN settings for this port.

Table 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

Contact	10 Base-T Signal
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.

### 1.3.3.2 SETUP AND COM PORTS

The SETUP and COM serial connections are DE-9F RS-232 ports. Refer to Table 3 for pin out descriptions and Section 4.3.4 for control line configuration of DCD, DTR, RTS and CTS control lines.

Serial port considerations:

- Viper SETUP and COM ports are Data Communication Equipment (DCE) devices
- In general, equipment connected to the Viper SC's serial ports is Data Terminal Equipment (DTE) and a straight-through cable is recommended.
- If a DCE device is connected to the Viper serial ports, a null modem cable/adaptor is required.

**Table 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*

### 1.3.3.3 POWER CONNECTOR

Viper is supplied with a right-angle power connector (10-30 VDC). Table 4 shows the pin-out of the power connector.

**Table 4 – Power Connector Pin-out**

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

The White Enable line must be tied to the red positive lead of the connector for the Viper SC to function.



**WARNING – EXPLOSION HAZARD- Do not disconnect unless power has been removed or the area is known to be non-hazardous**

#### 1.3.3.4 ANTENNA CONNECTOR

Standard Viper models have a 50-ohm TNC female antenna connector. This connection functions for both transmit and receive. Dual-Port models feature 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 is ideal for 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 Viper SC. 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.



**WARNING – EXPLOSION HAZARD- Do not disconnect unless power has been removed or the area is known to be non-hazardous**



**WARNING -EXPLOSION HAZARD-Substitution of components may impair suitability for Class I, Division 2. The unit must be powered with a Listed Class 2 or LPS power supply or equivalent.**

The antenna connector is for connection to antennas housed inside of a suitable enclosure.

### 1.4 PRODUCT WARRANTY

It is our guarantee that every Viper SC Radio modem will be free from physical defects in material and workmanship for ONE YEAR 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 C – PRODUCT WARRANTY.

If the product proves defective during the warranty period, contact our Customer Service Department at (800) 992-7774 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 number online at [www.calamp.com](http://www.calamp.com).

### 1.5 MODELS AND AVAILABILITY

Viper SC is available in various models. Each is available with a range features, kits, and accessories. Refer to Table 5 for product availability and ordering information. Refer to Table 6 for Viper SC antenna and antenna kits and Table 7 for Viper SC accessories.

**Table 5 – Viper SC Order Information**

Model Number	Frequency Range	Description
140-5018-502	136 - 174 MHz	Viper SC-100
140-5018-503	136 - 174 MHz	Viper SC-100 (Dual Port)

Model Number	Frequency Range	Description
250-5018-500	136 - 174 MHz	Viper SC-100 Demo Kit
140-5118-502	136 - 174 MHz	Viper SC-100 Standard Base Station
140-5318-502	136 - 174 MHz	Viper SC-100 Redundant Base Station
140-5028-502	215 - 240 MHz	Viper SC-200
140-5028-504	215 - 240 MHz	Viper SC+-200
140-5028-503	215 - 240 MHz	Viper SC-200 Dual Port
250-5028-502	215 - 240 MHz	Viper SC-200 Demo Kit
140-5128-502	215 - 240 MHz	Viper SC-200 Standard Base Station
140-5328-502	215 - 240 MHz	Viper SC-200 Redundant Base Station
140-5048-302	406.1 - 470 MHz	Viper SC-400 (Range 3)
140-5048-303	406.1 - 470 MHz	Viper SC-400 (Range 3) Dual Port
250-5048-300	406.1 - 470 MHz	Viper SC-400 (Range 3) Demo Kit
140-5148-302	406.1 - 470 MHz	Viper SC-400 (Range 3) Standard Base Station
140-5348-302	406.1 - 470 MHz	Viper SC-400 (Range 3) Redundant Base Station
140-5048-502	450 - 512 MHz	Viper SC-400 (Range 5)
140-5048-503	450 - 512 MHz	Viper SC-400 (Range 5) Dual Port
140-5048-600	450 - 512 MHz	Viper SC-400 (Range 5), AS/NZ Compliant
250-5048-500	450 - 512 MHz	Viper SC-400 (Range 5) Demo Kit
140-5148-502	450 - 512 MHz	Viper SC-400 (Range 5) Standard Base Station
140-5348-502	450 - 512 MHz	Viper SC-400 (Range 5) Redundant Base Station
140-5098-304	880 - 902 MHz	Viper SC+-890
140-5098-502	928 - 960 MHz	Viper SC-900
140-5098-504	928 - 960 MHz	Viper SC+-900
140-5098-503	928 - 960 MHz	Viper SC-900 Dual Port
250-5098-500	928 - 960 MHz	Viper SC-900 Demo Kit
140-5198-502	928 - 960 MHz	Viper SC-900 Standard Base Station
140-5398-502	928 - 960 MHz	Viper SC-900 Redundant Base Station
<b>EN 300 113 Compliant, AS/NZ Compliant Versions</b>		
140-5018-600	142 - 174 MHz	Viper SC-100 EN 300 113 Compliant, AS/NZ Compliant
140-5018-601	142 - 174 MHz	Viper SC-100 Dual Port EN 300 113 Compliant, AS/NZ Compliant
140-5118-600	142 - 174 MHz	Viper SC-100 Standard Base Station EN 300 113 Compliant, AS/NZ Compliant
140-5318-600	142 - 174 MHz	Viper SC-100 Redundant Base Station EN 300 113 Compliant, AS/NZ Compliant

Model Number	Frequency Range	Description
140-5048-400	406.1 - 470 MHz	Viper SC-400 (Range 3) EN 300 113 Compliant, AS/NZ Compliant
140-5048-401	406.1 - 470 MHz	Viper SC-400 (Range 3) Dual Port EN 300 113 Compliant, AS/NZ Compliant
140-5148-400	406.1 - 470 MHz	Viper SC-400 (Range 3) Standard Base Station EN 300 113 Compliant, AS/NZ Compliant
140-5348-400	406.1 - 470 MHz	Viper SC-400 (Range 3) Redundant Base Station EN 300 113 Compliant, AS/NZ Compliant
140-5048-600	450 - 512 MHz	Viper SC-400 (Range 5) EN 300 113 Compliant, AS/NZ Compliant
140-5048-601	450 - 512 MHz	Viper SC-400 (Range 5) Dual Port EN 300 113 Compliant, AS/NZ Compliant
140-5148-600	450 - 512 MHz	Viper SC-400 (Range 5) Standard Base Station EN 300 113 Compliant, AS/NZ Compliant
140-5348-600	450 - 512 MHz	Viper SC-400 (Range 5) Redundant Base Station EN 300 113 Compliant, AS/NZ Compliant

**Table 6 – Antenna Kits**

Part Number	Frequency	Description
250-0211-007	138-143 MHz	6.5 dB Antenna Kit
250-0211-010	138-143 MHz	9.5 dB Antenna Kit
250-0211-107	143-148 MHz	6.5 dB Antenna Kit
250-0211-110	143-148 MHz	9.5 dB Antenna Kit
250-0211-207	148-152 MHz	6.5 dB Antenna Kit
250-0211-210	148-152 MHz	9.5 dB Antenna Kit
250-0211-307	152-157 MHz	6.5 dB Antenna Kit
250-0211-310	152-157 MHz	9.5 dB Antenna Kit
250-0211-407	157-163 MHz	6.5 dB Antenna Kit
250-0211-410	157-163 MHz	9.5 dB Antenna Kit
250-0211-507	163-169 MHz	6.5 dB Antenna Kit
250-0211-510	163-169 MHz	9.5 dB Antenna Kit
250-0211-607	169-174 MHz	6.5 dB Antenna Kit
250-0221-007	216-222 MHz	6.5 dB Antenna Kit
250-0221-010	216-222 MHz	9.5 dB Antenna Kit
250-0200-025		25 feet antenna feedline (LMR400), N-Male
250-0200-055		50 feet antenna feedline (LMR400), N-Male
250-0241-507	450-470 MHz	7 dB Antenna Kit
250-0241-510	450-470 MHz	10 dB Antenna Kit
250-0241-507	450-470 MHz	7 dB Antenna Kit

Part Number	Frequency	Description
250-0241-510	450-470 MHz	10 dB Antenna Kit
250-5099-011	890-960 MHz	6.4 dB Antenna Kit
250-5099-021	890-960 MHz	10 dB Antenna Kit

Antenna Kits include premium antenna, mounting bracket, surge protector, grounding kit, cable ties, 18” TNC male to N-male jumper cable and weather kit.

- UHF and 900 kits include 25 feet of LMR400.
- VHF kits require feedline be purchased separately. LMR400 feedline is available in 25 and 50 feet.

**Table 7 – Accessories**

Model Number	Description
250-0200-100	Barrel Connector, RF1 N type, Female
250-0697-103	TNC-Male to N-Male 18”
250-0697-104	TNC-Male to N-Male 48”
250-0697-105	TNC-Male to N-Male 72”
250-0697-106	TNC-Male to N-Female 18”
897-5008-010	Viper SC Power Cable
150-5008-001	Factory Installed Viper SC Fan Kit
150-5008-002	Field Installed Viper SC Fan Kit

## 2 NETWORK ARCHITECTURE AND SYSTEM PLANNING

This section discusses network architecture, basic network types, interfacing modems and DTE, data protocols for efficient channel operation, as well as providing tips for selecting an appropriate site, antenna selection, and reducing the chance of harmful interference.

### 2.1 NETWORK ARCHITECTURE

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 may corrupt data. Most SCADA networks have a device that is configured to be the 'polling master'. It is the responsibility of this polling master to control RF traffic so RF collisions do not occur.

Viper 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. However, these technologies must still 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 Viper data 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 Viper SC. Viper SCs will buffer reply messages because the dominant RTU/radio is transmitting (carrier is present). A Viper SC 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.

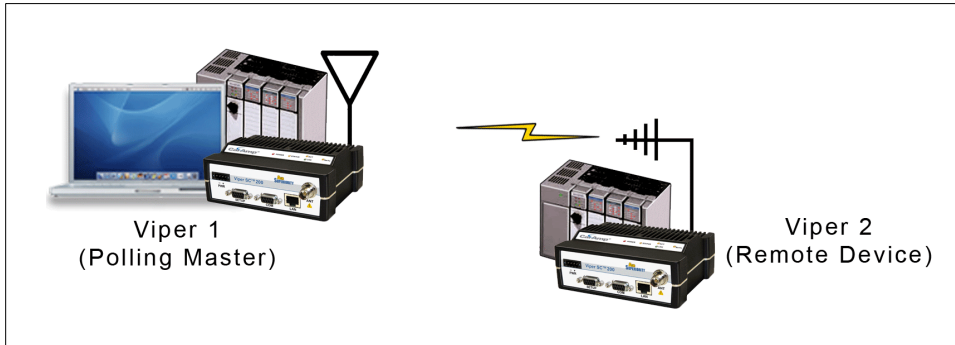
Because the Viper SC has the ability to use two completely different and separate SCADA polling protocols, it is important to have interaction between the two protocols. The Viper SC can send out an Ethernet TCP/IP polling message and also an RS232 polling message, which may or may not be generated by 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.



### 2.1.1 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, or a wide variety of other networking applications.

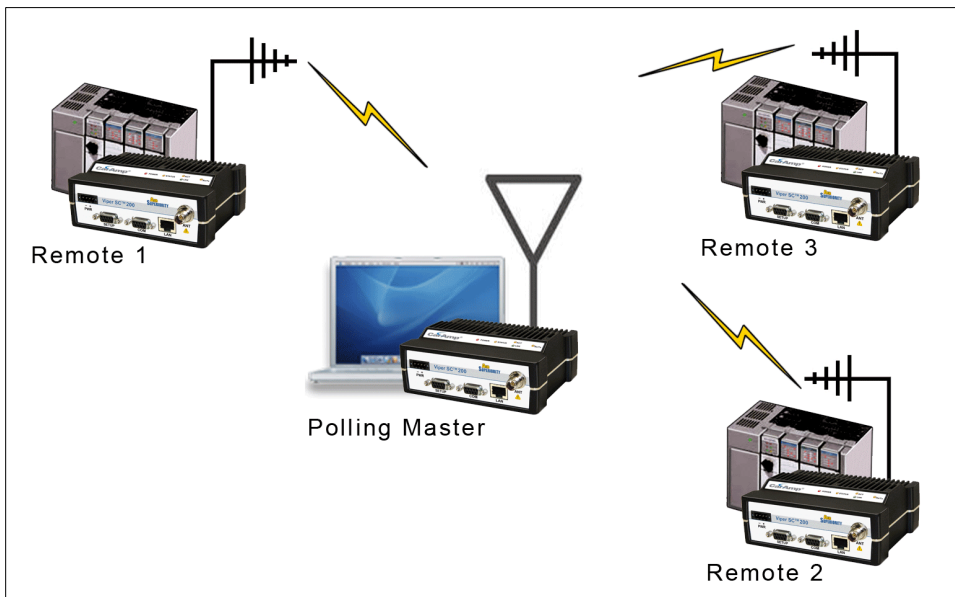
**Figure 3 – Point to Point Network**



### 2.1.2 POINT-TO-MULTIPOINT

A Point-to-Multipoint network is a common network type used in SCADA and other polling systems. The Master Polling 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 4 – Point to Multipoint Network**



### 2.1.3 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.

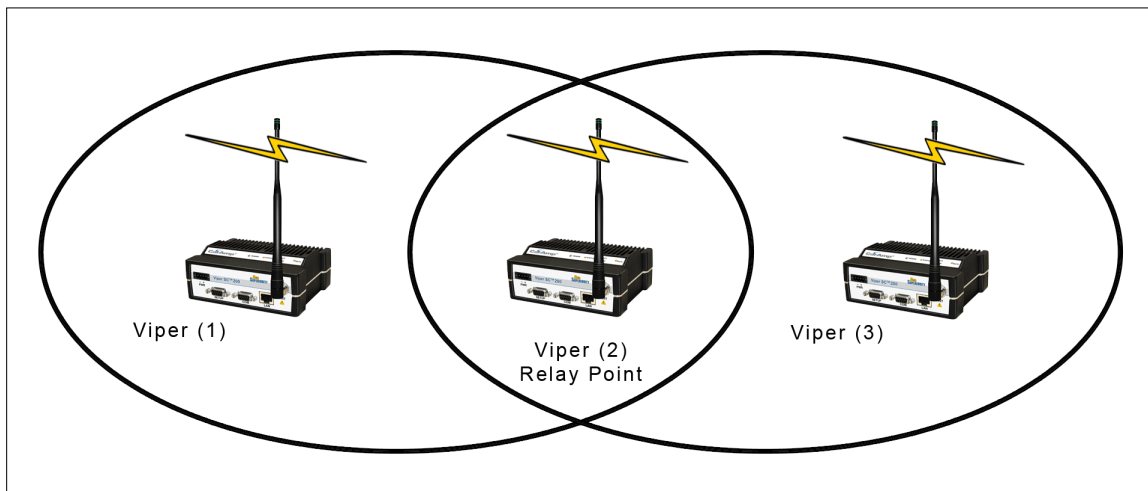
Viper has several collision avoidance features to help minimize collisions. Viper is a “polite radio”. This means Viper will check the RF traffic on the receive channel before transmitting. If there is no RF traffic present (no carrier present) it will transmit. If there is RF traffic (carrier present) the Viper SC will buffer the data. Viper will transmit the buffered data when there is no RF traffic present.

### 2.1.4 EXTENDING THE COVERAGE AREA WITH A RELAY POINT

A Viper can be configured as a **Relay Point**. Relay Points provide store and forward repeating of necessary information from one coverage area to the next. In Bridge mode all traffic is forwarded. In Router mode, only Broadcast Packets and address specific packets are forwarded. There may be multiple Relay Points to extend coverage over several hops. Multiple relay points in a single network may slow the flow of data traffic.

To configure your Viper as a Relay point, refer to Section 3.5.2.

**Figure 5 – Two Coverage Areas**



## 2.2 IP FORWARDING MODES

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

---

## 2.2.1 BRIDGE MODE

Bridge mode is the simplest configuration for all Viper networks. Viper may be configured for bridge mode only when all devices are located on the same Local Area Network (LAN). Thus, all units in the network can communicate directly with all other units in the network.

Each Viper has only one IP address assigned to it and the subnet mask is the same for every Viper in the network. Bridge communications does not require each Viper to have a unique IP address, but it is highly recommended and necessary for remote programming of the radio.

Every Viper ships from the factory with the default Ethernet IP address of 192.168.205.1 and a subnet mask of 255.255.255.0. The default subnet of the Viper 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.

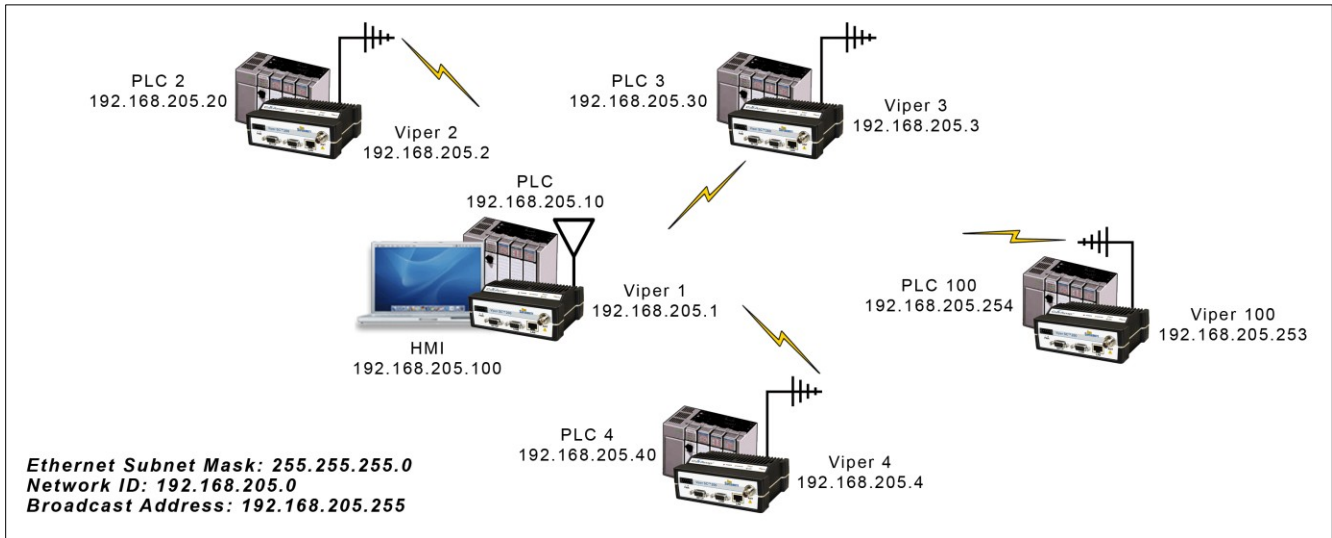
### Bridge Mode Example 1

Example one illustrates a sample Viper network. The subnet consists of IP addresses ranging from 192.168.205.0 to 192.168.205.255. The subnet mask is 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 first address 192.168.205.0 is reserved for the Network ID. The last address 192.168.205.255 is reserved for the broadcast address. There are 254 valid IP addresses that may be assigned to hosts on the network.

<i>Ethernet Subnet Mask</i>	255.255.255.0
<i>Network ID</i>	192.168.205.0
<i>Broadcast Address:</i>	192.168.205.255
<i>Viper #1</i>	192.168.205.1/24
<i>PLC/RTU #</i>	192.168.205.10/24
<i>Computer #1</i>	192.168.205.100/24
<i>Viper #2</i>	192.168.205.2/24
<i>PLC/RTU #2</i>	192.168.205.20/24
<i>Viper #3</i>	192.168.205.3/24
<i>PLC/RTU #3</i>	192.168.205.30/24
<i>Viper #4</i>	192.168.205.4/24
<i>PLC/RTU #4</i>	192.168.205.40/24
...	
<i>Viper #100:</i>	192.168.205.253/24
<i>PLC/RTU #100:</i>	192.168.205.254/24

**Figure 6 – Bridge Mode Example 1**



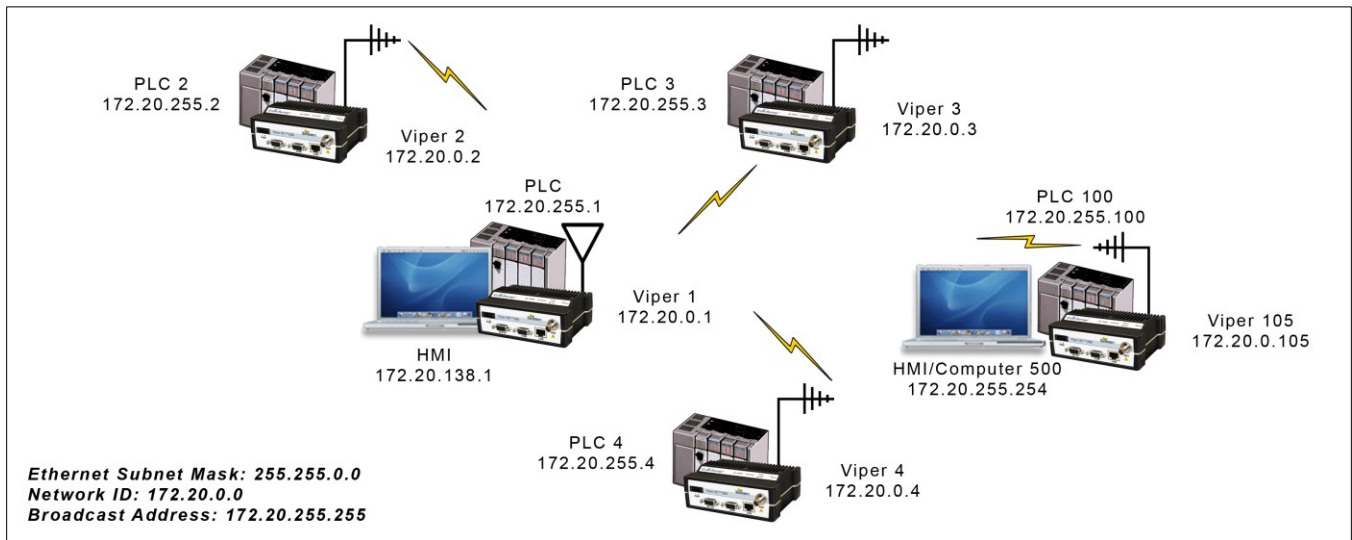
**Bridge Mode Example 2**

The subnet for this Viper network is comprised of devices with IP addresses ranging from 172.20.0.0 to 172.20.255.255. The subnet mask is 255.255.0.0. The shorthand notation is: 172.20.0.1/16 since the subnet mask 255.255.0.0 contains 16 ones then 16 zeros when it is converted to binary.

The first address 172.20.0.0 is reserved for the Network ID. The last address 172.20.255.255 is reserved for the broadcast address. There are 65534 valid IP addresses available to be assigned to hosts on the network.

- Ethernet Subnet Mask:* 255.255.0.0
- Network ID:* 172.20.0.0
- Broadcast Address:* 172.20.255.255
  
- Viper #1:* 172.20.0.1/16
- Viper #2:* 172.20.0.2/16
- Viper #3:* 172.20.0.3/16
- ...
- Viper #105:* 172.20.0.105/16
  
- PLC/RTU #1:* 172.20.255.1/16
- PLC/RTU #2:* 172.20.255.2/16
- PLC/RTU #3:* 172.20.255. 3/16
- ...
- PLC/RTU #250:* 172.20.255.250/16
  
- Computer #1:* 172.20.138.1/16
- ...
- Computer #500:* 172.20.255.254/16

Figure 7 – Bridge Mode Example 2



## 2.2.2 ROUTER MODE

Router mode allows greater network configuration flexibility, allows the use of a variety of protocols, and also adds RF diagnostics capability to Viper networks. Diagnostics can be retrieved through the Ethernet port of the Viper. For more information on Viper RF Diagnostics, refer to **Section 4.1.2**

Router mode requires the setup of Ethernet IP and Serial IP addresses and is recommended only for users who have IT/Network support readily available to them and/or the authorization required to make changes in to the network.

In Router mode, each Viper uses two IP addresses:

- The Ethernet IP Address
- The RF IP Address

Every Viper is factory configured with a default Ethernet IP Address 192.168.205.1 and a unique RF IP address. This RF IP address will have the form 10.x.y.z where x, y, and z is based on the last 6 digits of the unit's Ethernet MAC address. The default network is 10.0.0.0/8.

In Router mode, each Viper must have its Ethernet IP Address on a **unique** network and all Vipers must have their RF IP addresses on the **same** network. **For consistent and reliable communication, the RF network addresses should not overlap or contain any of the IP Addresses in the Ethernet network.**

### Router Mode Example 1

In this example, each Viper has an Ethernet IP address on a unique network. For Vipers #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 Viper #4's local Ethernet port has 65534 valid IP addresses.

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

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

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

*Ethernet Subnet Mask: Varies from Viper to Viper.*

*RF Subnet Mask for all units: 255.0.0.0*

*Viper 1: Ethernet IP Address: 192.168.205.1/24 RF IP Address: 10.11.12.25/8*

*PLC 1: 192.168.205.2/24*

*Computer/HMI 1: 192.168.205.3/24*

*Viper 2: Ethernet IP Address: 192.168.206.1/24 RF IP Address: 10.9.7.251 / 8*

*PLC #2: 192.168.206.2 / 24*

*Viper #3 Eth IP Address: 192.168.207.1/24 RF IP Address: 10.8.0.52 / 8*

*PLC #3: 192.168.207.2/24*

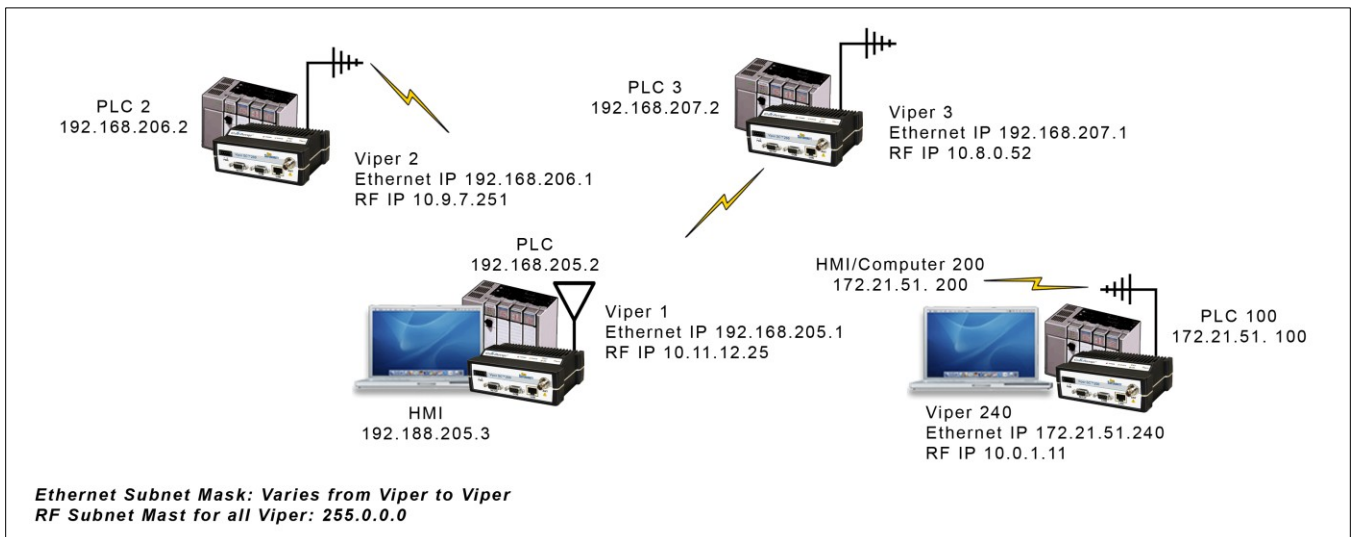
*Computer #3: 192.168.207.3/24*

*Viper #4 Eth IP Address: 172.21.51.105/16*

*RF IP Address: 10.0.1.11/8*

*PLC #4: 172.21.51.106/16*

**Figure 8 – Router Mode Example 1**



**Router Mode Example 2:**

Each Viper has an Ethernet IP address on a unique network.

In this example, each network connected to the Viper's local Ethernet port has 14 valid IP addresses that may be used for the Viper, 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 Viper has an RF IP address in the network and that no RF IP address is used twice.

Ethernet Subnet Mask for all units: 255.255.255.240

RF Subnet Mask for all units: **255.255.0.0**

Viper #1 Eth IP Address: 10.200.1.1 / 28 RF IP Address: 10.0.0.1 / 16

Viper #2 Eth IP Address: 10.200.1.17 / 28 RF IP Address: 10.0.0.2 / 16

Viper #3 Eth IP Address: 10.200.1.33 / 28 RF IP Address: 10.0.0.3 / 16

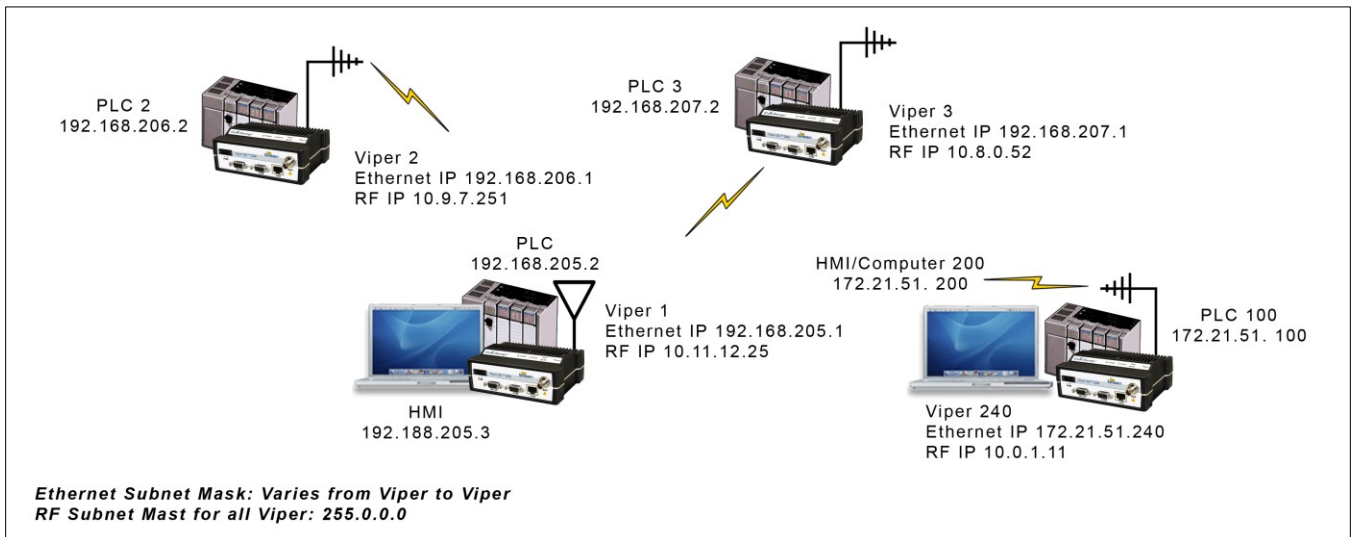
Viper #4 Eth IP Address: 10.200.1.49 / 28 RF IP Address: 10.0.0.4 / 16

...

Viper #177 Eth IP Address: 10.200.12.1 / 28 RF IP Address: 10.0.0.177 / 16

Viper #178 Eth IP Address: 10.200.12.17 / 28 RF IP Address: 10.0.0.178 / 16

**Figure 9 – Router Mode Example 2**



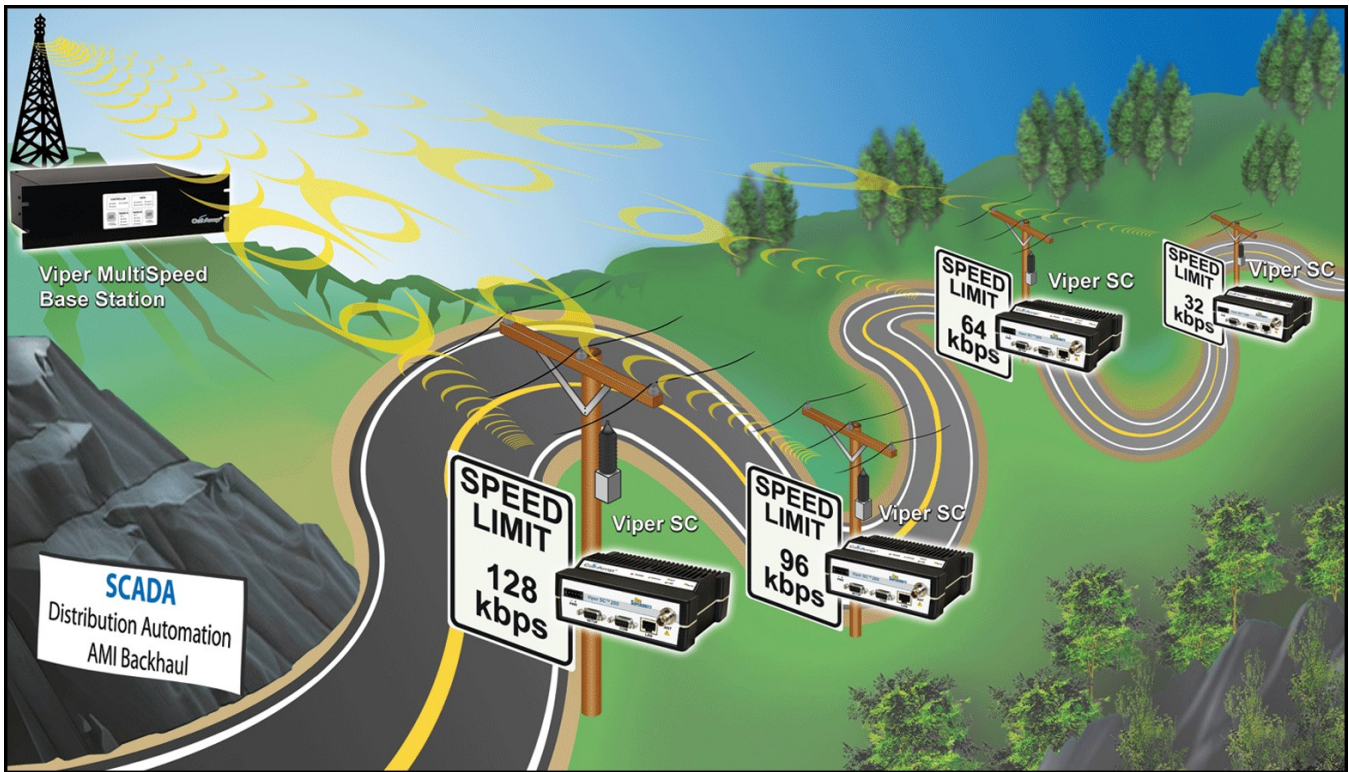
### 2.2.3 MULTISPEED NETWORKING

When using Viper SC with a Viper SC 19" rack mount base station, the user can configure the network for multispeed operation. With the Base enabled as a 'rate-controller', the remote device becomes a 'rate follower'. The rate-controller can be configured to talk at different over-the-air data rates for each remote Viper. This allows the user to uniquely control the data rate for each RF link in the system from the Base Station web pages. The user can program RF links with strong signal strength to communicate at fast data rates and RF links with low signal strength can be programmed to communicate at more robust, slower data rates. Even if data rates vary from Viper to Viper, every Viper in the network must be programmed with the same bandwidth.

Refer to Section 4.3.1 for multispeed configuration options.



Figure 10 – Multispeed Illustration



## 2.3 SYSTEM PLANNING

A Site Survey is a propagation study of the RF path between two points or between one point and multiple points. Signal propagation may be 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.

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

### 2.3.1 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.

---

### 2.3.2 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, 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 conditions. CalAmp recommends a 20 dB fade margin for most projects.

---

### 2.3.3 RADIO INTERFERENCE

Interference is possible in any radio system. However, since the Viper 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.

- 1) 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.
- 2) 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.
- 3) 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.
- 4) 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.

---

### 2.3.4 SELECTING ANTENNA AND FEEDLINE

Viper can be used with a variety of antenna types. Viper has been tested and approved with antennas having a maximum gain of 10 dBi. Refer to **Section 1.5** for a list of tested antenna recommendations. These antennas are FCC approved for use with Viper. 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.

- **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.
- **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.
- **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.

---

### 2.3.4.1 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 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.

---

### 2.3.4.2 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 8** for feedline recommendations.

**Table 8 – 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" Heliac	0.68 dB	1.51 dB	2.09 dB
7/8" Heliac	0.37 dB	0.83 dB	1.18 dB
1 5/8" Heliac	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.

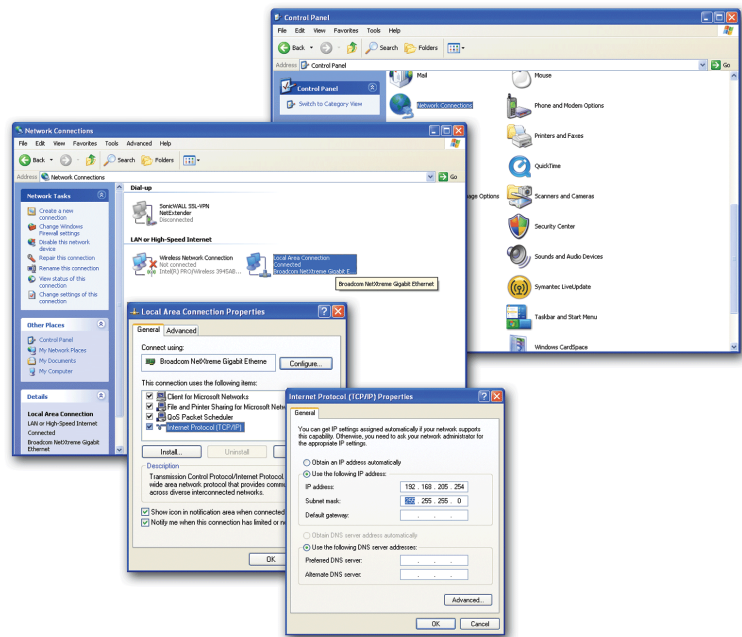
### 3 QUICKSTART

It is easy to set up a Viper network to verify basic operation and to experiment with network designs and configurations. To eliminate unnecessary disruption of traffic on the existing network while you become familiar with Viper, you should use a network IP subnet address different from others currently in use in your test area.

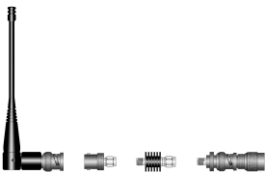
#### 3.1 PC LAN SETUP

On a PC running MS-Windows with an existing LAN connection, connect to the Ethernet input of the Viper SC and complete the following steps.

- 1) From the PC, select **Start** → **Settings** → **Control Panel** → **Network Connections**.
- 2) Right-click **Local Area Connection** to open the Properties box.
- 3) From the list, select **Internet Protocol (TCP/IP)** and click **Properties** to open the TCP/IP Properties box.
- 4) Select **Use the Following IP Address** and enter:
  - a. IP Address: 192.168.205.100
  - b. Subnet Mask: 255.255.255.0
  - c. Default Gateway: Leave empty
- 5) Click **OK** to apply your changes. Some Operating systems may require you to reboot your computer to complete this connection process.



#### 3.2 INSTALL THE ANTENNA



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

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 MEASURE AND CONNECT PRIMARY POWER

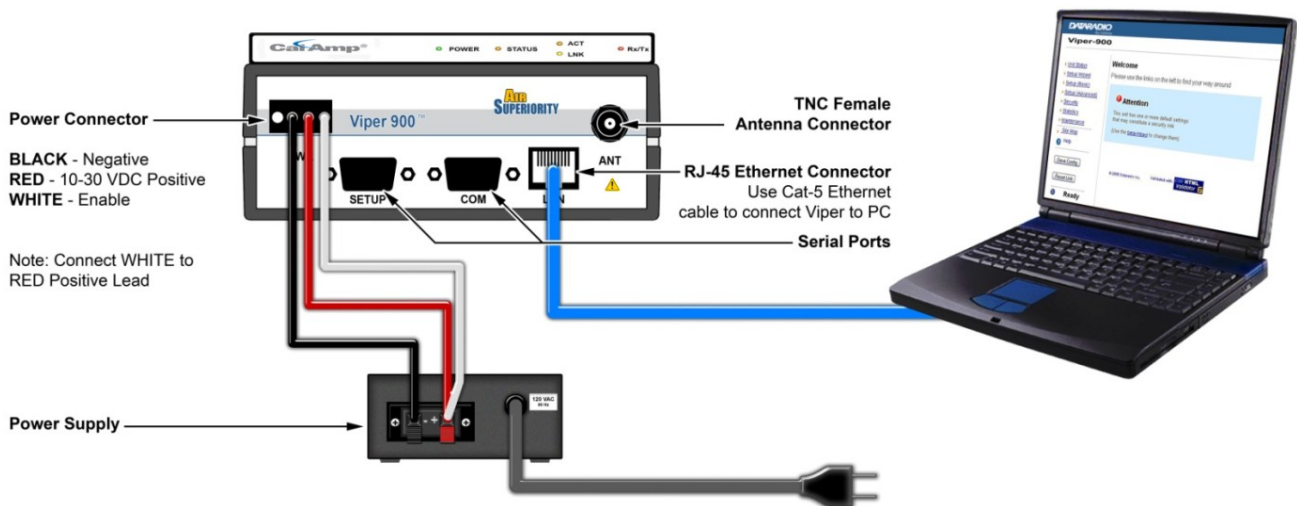
Primary power for Viper must be within 10-30 VDC and be capable of providing a minimum of:

- 10 watt supply for Tx @ 1W
- 40 watt supply for Tx @ 5W, or
- 60 watt supply for Tx @ 10 W

Viper Demo Kits contain a power connector with screw-terminals. Observe proper polarity when connecting the cables to the Power Supply. **The white wire must be connected to red wire.**

### 3.4 CONNECT VIPER SC TO PROGRAMMING PC

Connect a PC's Ethernet port to the LAN port using a CAT 5 Ethernet cable. Wait for the LINK LED to glow green.



### 3.5 CONFIGURE YOUR VIPER

Viper must be configured using the Setup Wizard. This quick start will use the Setup Wizard to configure your Viper for bridge mode operation.

For other configuration options:

- Refer to Section 4.3 for Basic Setup
- Refer to Section 4.4 for Advanced Setup.

#### 3.5.1 INITIAL INSTALLATION LOGIN

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

For initial installation, enter a User Name and the default password.

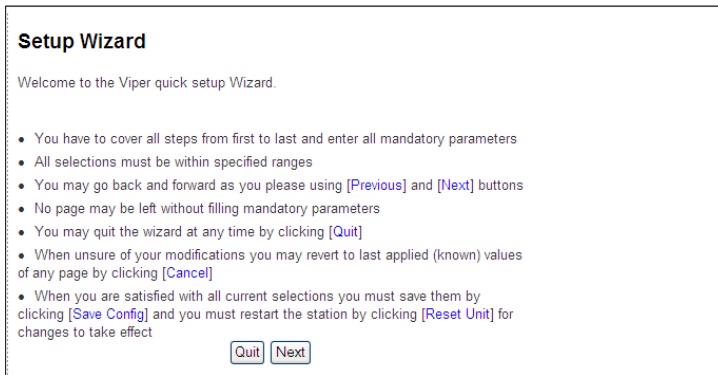
- User Name: 1 to 15 characters
- Default Password: **ADMINISTRATOR**. Password is case sensitive.
- Click **OK**. The web interface WELCOME screen opens.

To change the password for your Viper, refer to Section 4.5.1.1.

### 3.5.2 SETUP WIZARD

From the navigation frame, select **Setup Wizard** to guide you through Viper configuration for operation. Read the onscreen instructions carefully before proceeding.

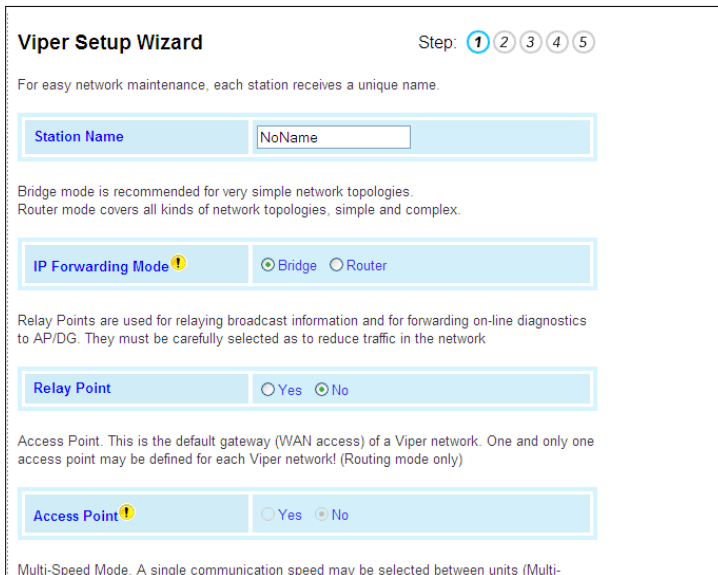
**Figure 11 – Setup Wizard Welcome**



**Quit** to exit the Setup Wizard; **Next** to proceed.

### STEP 1

**Figure 12 – Setup Wizard (STEP 1)**



Station Name: Assign a unique Station Name

IP Forwarding Mode: Select Bridge (Mode)

Relay Point: Select No

Access Point: Select No

Multi-Speed Mode: Select Disabled

Click **Apply**. Click **Next**.

---

## STEP 2

**Figure 13 – Setup Wizard (STEP 2)**

**Viper Setup Wizard** Step: 1 2 3 4 5

If you keep the default IP address on all units on your network, they will be accessible via their local Ethernet port. To monitor or change configurations remotely, each unit needs a unique IP address. This will be the address that you will point your browser to access these pages in the future.

Changing this address will not affect your application data but the address shall not be used elsewhere in your network

Enter a unique IP-address for the unit. If you will be administering it from a different IP subnet, enter the Default Gateway for this network. You do not need to set a Default Gateway if you will only be connecting to your Vipers from the same IP subnet.

IP Address	<input type="text" value="192.168.205.1"/>	default: 192.168.205.1
Network Mask	<input type="text" value="255.255.255.0"/>	default: 255.255.255.0
Default Gateway	<input type="text" value="0.0.0.0"/>	

**Note:**  
The symbol indicates that this parameter will require a 'Reset' before it takes effect.

Each Viper SC is programmed with these defaults:

IP Address: 192.168.205.1

Network Mask: 255.255.255.0

Default Gateway: 0.0.0.0

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

Figure 14 – Setup Wizard (STEP 3)

**Viper Setup Wizard** Step: 1 2 3 4 5

One radio channel must be properly set up for this station to communicate with its neighbors.

Channel #	1	Default: 1 Range: [1..32]
Bandwidth [KHz]	12.5	
Data And Control Packet Bit Rate [Kbps]	16	
RX Frequency [MHz]	0.000000	Range [215.000000..240.000000]
TX Frequency [MHz]	0.000000	Range [215.000000..240.000000]
TX Power [Watts]	5.0	Default: 5.0 Range [1.0..10.0]

Apply Cancel Quit Previous Next

Note:  
The symbol indicates that this parameter will require a 'Reset' before it takes effect.

### Verify FCC license before completing this step.

- Channel ID: Enter 1 for Channel ID
- Bandwidth: Enter Bandwidth (in KHz)
- Data and Control Packet Bit Rate: Select desired bit rate (in kbps)
- RX Frequency: Enter RX Frequency
- TX Frequency: Enter TX Frequency
- TX Power: Enter 5.0 W

Click **Apply**. Click **Next**.

## STEP 4

Figure 15 – Setup Wizard (STEP 4)

**Viper Setup Wizard** Step: 1 2 3 4 5

Encryption  Enabled  Disabled

Viper uses AES-128-bit encryption to protect your data from eavesdropping and to prevent intruders from changing your configuration. Use of encryption is optional but we strongly recommend it for actual networks. The encryption phrase and key must be common to all units in a given network.

Encryption Pass Phrase Dataradio

Encryption Key b3 35 b0 7b ba 8d eb 5d 44 66 3c 3a a7 16 f1 80

Apply Cancel Quit Previous Next

Note:  
The symbol indicates that this parameter will require a 'Reset' before it takes effect.

The Viper SC 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: Select to Enable. Default = Disabled.

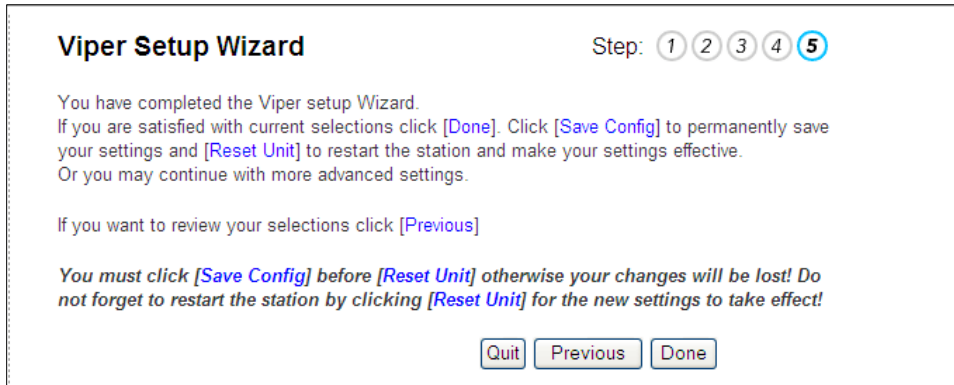
If encryption is enabled, you must enter an **Encryption Pass Phrase**. This phrase must be the same for all units in the network. The default pass phrase is Dataradio.

Click **Apply**. Click **Next**.

---

## STEP 5

**Figure 16 – Setup Wizard (STEP 5)**



Click **Done**. Click **Save Config** to save the network parameters for your Viper SC. You will see a green success icon on the bottom left of the page when save is complete. Click **Reset Unit** to cycle device power. This is necessary if you changed any parameters marked with a yellow!

You have completed the Viper Setup Wizard. Your unit is now functioning in Bridge Mode.



## 4 WEB INTERFACE

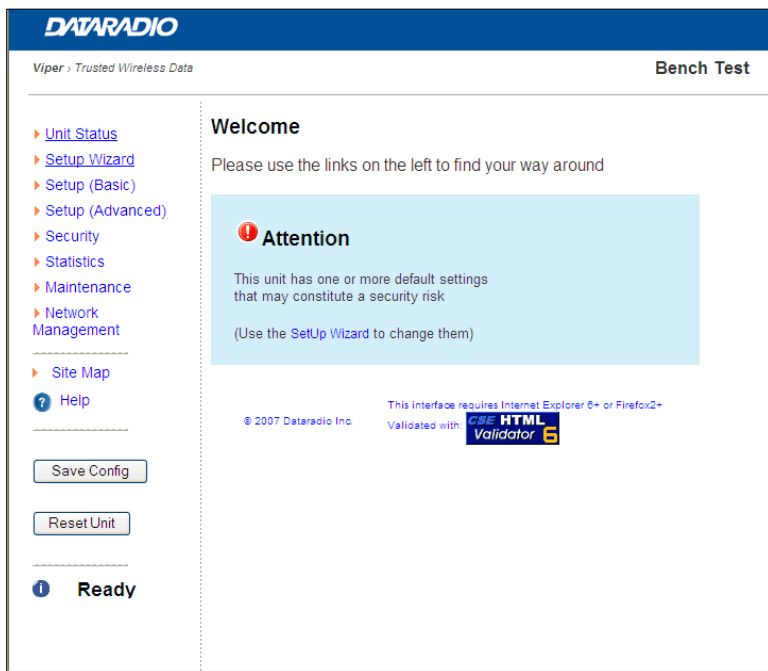
Viper is designed for easy installation and configuration. All operating parameters are set using a web browser. A built-in web server makes configuration and status monitoring possible from any browser-equipped computer, either locally or remotely. The Interface is divided into two frames. On the left, the navigation frame allows the user to navigate the main menu.

- Unit Status (see **Section 4.1**)
- Setup Wizard (see **Section 4.2**)
- Basic Setup (see **Section 4.3**)
- Advanced Setup (**Section 4.4**)
- Security (see **Section 4.5**)
- Statistics (see **Section 4.6**)
- Maintenance see (**Section 4.7**)
- Network Management (see **Section 0**)

The navigation frame also contains the **Save Config** and **Reset Unit** command buttons.

- **Save Config.** This command saves the Viper SC parameters into flash memory. Failure to use this command 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 this command 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.

**Figure 17 – Web Management Welcome Screen**



The frame on the right displays the selected web page and any system commands applicable to the current page.

- **Apply.** Use this command to write 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 this command before leaving a web page will result in the loss of entered selections, addresses, and values.
- **Cancel.** This command only affects the dialog boxes or radio buttons in the opened window.

## 4.1 UNIT STATUS

From the navigation frame, select **Unit Status** to display General and Diagnostic data for the device.

### 4.1.1 GENERAL

The **Identification and Status** banner displays the software revision information (Ex. Vx.y\_Rxxx). Vx.y is revision number, and Rxxx represents the Package Release Build Number.

**Figure 18 – Unit Identification and Status**

Dataradio Viper FAMA PROD V3.3_R201106081500	
Station Name	800D3D
Local Time	2007-10-04 14:45:57
CWID	Enabled
CWID Callsign	
CWID Interval	30
IP Forwarding Mode	Router
Station Relay Point	No
Multi-Speed Mode	Disabled
Mode	ANSI
On-line Diagnostics Interval	30
VPN Status	Ready
Unit Status	Ok
<input type="button" value="Refresh"/> <input type="button" value="Acknowledge Unit Status"/>	

- **Station Name.** Displays the name of the connected unit.
- **Local Time.** Displays time zone configuration using UTC time and the selected Time Zone. Unless an SNTP server is configured, this parameter will be restored to the factory default when device power is cycled. An SNTP server can be configured in **Section 4.4.6**.
- **CWID.** Display only. Continuous Wave Identification (CWID) is configured in **Section 4.3.1.1**.

- **IP Forwarding Mode.** Display **Bridge/Router**. Default = **Bridge**. IP forwarding mode is configured in **Section 4.3.1**.
- **Station Relay Point.** Display **Yes/No**. Default = **No**. The Station Relay Point is configured in **Section 4.3.1**.
- **Multi-Speed Mode.** Display **Enabled/Disabled**. Default = **Disabled**. Refer to Section 4.3.1 for multispeed configuration.
- **Mode.** Indicate the mode of operation (ANSI, ANSI 900, ETSI)
- **On-line diagnostics Interval.** Displays the time interval (in seconds) when the On-line Diagnostics string will be transmitted. This interval is configured in **Section 4.3.1.2**.
- **VPN Status.** Displays the status of the VPN (virtual private network). **OK/Ready** when operational. If device is not operational display will read **Not Ready** and a reason will be shown (Ex. **VPN service disabled**).
- **Unit Status.** Displays the status of the Viper SC 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 ACKNOWLEDGE UNIT STATUS and REFRESH buttons to reset the modem. If the problem persists, contact CalAmp Technical Services for additional information.
- **Refresh.** Click to **Refresh** the parameters on the current page.
- **Acknowledge Unit Status.** Allows the user to acknowledge and clear errors. Errors remain stored, even after cycling power, to aid in troubleshooting intermittent faults. Click to return web page displays and Status LED function to normal operation.

---

#### 4.1.2 DIAGNOSTICS

From the navigation frame, select **Unit Status** → **Diagnostics** to view diagnostic data for the local device. Each Viper can be configured to continually monitor and report its operating conditions and local environment.

**Figure 19 – Diagnostics Info**

<b>Date and Time</b>	2007-10-01 12:18:40
<b>Time Since Reset</b> [DD:HH:MM:SS]	0:00:18:52
<b>Modem Firmware Version</b>	DATARADIO Viper (HW:PCB-280-03470) (CodeBase:ipr_3.3_R201106081500)
<b>Radio Firmware Version</b>	FIRM-03_10-R
<b>RSSI From RF-MAC 80:0D:3D</b>	-80.063 dBm
<b>SNR From RF-MAC 80:0D:3D</b>	38.477 dB
<b>DC Input Voltage</b>	14.8 V
<b>TX Frequency</b>	230.000000 MHz
<b>RX Frequency</b>	235.000000 MHz
<b>Transmit Power Level</b>	1.0 Watts
<b>Transceiver Temperature</b>	38.0 C
<b>PA Forward Power</b>	0.0 Watts (normal)
<b>PA Reverse Power</b>	0.0 Watts (normal)
<b>Power State</b>	Full (normal)

- **Date and time.** Displays the time and date. To configure date and time using an SNTP server, refer to **Section 4.4.6 – Advanced Setup** → 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. Formatted as 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.
- **SNR from RF-MAC.** Displays the Signal-to-Noise ratio from the unit with the MAC address shown. The SNR is defined as the ratio of signal power to background noise power corrupting the signal. The higher the ratio, the less corruptive the background noise is.
- **DC Input Voltage.** Displays the DC Input Voltage for the unit.
- **TX Frequency.** Displays the current operating transmit frequency for the active channel. Configured in Section 4.3.3.
- **RX Frequency.** Displays the current operating receiver frequency for the active channel. Configured in Section 4.3.3.
- **Transmit Power Level.** Displays the programmed power level for the active channel. Configured in Section 4.3.3.
- **Transceiver Temperature.** Displays the transceiver’s internal temperature in Celsius or Fahrenheit.
- **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 Viper SC 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 Viper SC radio can be configured to send an SNMP trap if the Reverse Power goes into a “fault” state.
- **Power State.** Reports **Full (normal)/Fault**. 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 transmitter will shutdown completely to protect the radio from permanent damage. When Viper is at Full power this line will report “(normal)”. If the Viper SC’s PA goes into Foldback or Shutdown this line will report “(fault)”. The Viper SC radio can be configured to send an SNMP trap if the Power State reports a fault.
- **Refresh.** Click to **refresh** the parameters for the current page.

---

## 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. Backhaul adds to 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. Viper 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 Viper SC’s web browser interface.

### 4.1.2.1.1 OUTPUT FORMAT

---

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). 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. Note: no overhead is generated in the Viper SC unit if no online diagnostic connection is actually made.

**Figure 20 – Diagnostic Output sample**

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,

**Table 9 – Diagnostics Output Definitions**

Output 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 IPSPD enabled. IPSPD can be enabled/disabled under Setup (Advanced) <input type="checkbox"/> 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 Viper SC. In Router mode, this address displays the IP Address of the source Viper SC. The source is the Viper SC 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 Viper SC. In Router Mode, this address displays the IP Address of the destination Viper SC. This is the destination station from the point of view of RSSI measurements.
A	Temperature of the source Viper SC in Celsius or Fahrenheit. Temperature units can be configured on the source Viper SC under Setup (Advanced) User <input type="checkbox"/> 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 Viper SC for the last message received from the destination Viper SC. This is also referred to as the Local RSSI. The value displayed shall be interpreted as shown in Table 10.
D	RSSI measured at the destination Viper SC for the last message received from the source Viper SC. This is also referred to as the Remote RSSI. The value displayed shall be interpreted as shown in Table 10.
E	Radio/antenna forward power measured in 10ths of watts at the source Viper SC. A value of 51 shall be interpreted as 5.1W.
F	Radio/antenna reverse power measured in 10ths of watts at the source Viper SC. 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 10 – Online Diagnostics RSSI Display**

Value	RSSI	Notes
0	NA	The RSSI Value is not Available
1	> -60.25 dBm	The RSSI Value is greater than -60.25 dBm
20	-65.00 dBm	
255	< -123.75 dBm	RSSI is less than -123.75 dBm
X		$RSSI = -60 - (X * 0.25)$ , for X not equal to 0

## 4.2 SETUP WIZARD

Refer to **Section 3.5.2 – Quick Start** to use the Setup Wizard to configure your Viper.

## 4.3 BASIC SETUP

From the navigation frame, select Basic Setup to configure General, IP, Channel Table and Serial Port settings.

- General Settings (see **Section 4.3.1**)
- IP Settings (see **Section 4.3.2**)
- Channel Table Settings (see **Section 4.3.3**)
- Serial Port Settings (**Section 4.3.4**)

### 4.3.1 GENERAL

**Figure 21 – Setup(Basic)→General Settings**

Station Name	<input type="text" value="NoName"/>
IP Forwarding Mode	<input checked="" type="radio"/> Bridge <input type="radio"/> Router
Bridge Forwarding	<input type="radio"/> Everything <input checked="" type="radio"/> IP and ARP types only
<b>Note: when selecting Router forwarding mode, all relevant IP settings must be configured</b>	
Relay Point	<input type="radio"/> Yes <input checked="" type="radio"/> No
Access Point	<input type="radio"/> Yes <input checked="" type="radio"/> No
Multi-Speed Mode	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
CWID	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
CWID Call Sign	<input type="text"/>
CWID Interval	<input type="text" value="30"/> minutes
On-line Diagnostics Interval	<input type="text" value="300"/> seconds
Unit Automatic Reset	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Unit Reset Interval	<input type="text" value="1440"/> minutes

— **Station Name.** Enter a string up to forty characters in length.

- **IP Forwarding Mode.** Select **Bridge/Router**. Default = **Bridge**.
- **Bridge Forwarding.** Select **Everything/IP and ARP only**. Default = **IP and ARP only**. (Ethernet II types: 0x0800, 0x0806). Select **Everything** to forward all 802.3 Ethernet II packet types. Use this setting to transport protocols such as IPX, 802.1Q, etc. Bridge Forwarding is not available in Router mode.
- **Relay Point.** Select **Yes/No**; Default = **No**. Refer to Section 2.1.4 (pg 11) before configuring your Viper as a Relay Point.
- **Access Point.** Select **Yes/No**; Default = **No**. This is the default gateway (WAN access) of a Viper SC network. One, and only one, access point may be defined for each Viper SC network. All Viper SCs in the network will set their default route to point towards the Access Point. Viper can only be configured as an Access Point if it is operating in Router Mode.
- **Multi-Speed Mode.** Select **Disabled/Enabled**. *Default = Disabled*. When **Disabled** all Vipers in the network communicate at a fixed data rate. (Refer to Appendix A for data rates by model). Select **Enabled** to configure the Viper unit to be a **rate-follower**. This means the Viper will adjust its over-the-air data rate to that of the **rate-controller**. Rate-control can only be programmed in the 19" rack mount Viper SC Base Station.

---

#### 4.3.1.1 CWID (CONTINUOUS WAVE IDENTIFICATION)

Select **Enabled/Disabled**; Default = **Disabled**. If enabled, the unit will broadcast the FCC Call Sign in Morse code at a given interval. Enter **CWID Call Sign** and **CWID Interval**. **CWID Call sign** is the FCC Call sign to be broadcast. **CWID Interval** is the time interval (in minutes) after which the call sign will be broadcast.

---

#### 4.3.1.2 ON-LINE DIAGNOSTICS INTERVAL

**Enter a value.** *Default = 300*. This interval represents the amount of time (in seconds) in which the unit will broadcast the diagnostic string. Refer to **Section 4.1.2** for more information about the diagnostic string.

---

#### 4.3.1.3 UNIT AUTOMATIC RESET

Select **Enabled/Disabled**. *Default = Disabled*. Select **enable** to make the radio completely shut down and restart after a set period of time. Enter a **Unit Reset Interval** value to represent the time (in minutes) between resets.

## 4.3.2 IP SETTINGS

Figure 22 – Setup(Basic)→IP Settings

Ethernet Interface	
DHCP Client !	<input checked="" type="radio"/> Static <input type="radio"/> Dynamic
IP Address !	<input type="text" value="192.168.205.1"/> (default: 192.168.205.1)
Netmask !	<input type="text" value="255.255.255.0"/> (default: 255.255.255.0)
DHCP Server !	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Start Address !	<input type="text" value="192.168.205.2"/>
Number of Leases !	<input type="text" value="10"/>
Lease Duration !	<input type="text" value="0"/> Minutes (0:Infinite)
Gateway !	<input type="text" value="0.0.0.0"/>
MTU !	<input type="text" value="1500"/> (default: 1500)
MAC Address	00:0A:99:80:0D:44

RF Interface	
IP Address !	<input type="text" value="10.128.13.68"/> (default: 10.128.13.68)
Netmask !	<input type="text" value="255.0.0.0"/> (default: 255.0.0.0)
MTU !	<input type="text" value="1500"/> bytes (default: 1500 bytes)
MAC Address !	<input type="text" value="80:0D:44"/> (default: 80:0D:44)

Default Gateway	<input type="text" value="0.0.0.0"/>
-----------------	--------------------------------------

### 4.3.2.1 ETHERNET INTERFACE

- **DHCP Client.** Select **Static/Dynamic**. *Default = Static*. Select **Static** to enable user entry of IP address of the unit. Select **Dynamic** to set the unit to be a DHCP client, which will allow the unit to accept an IP address from an external DHCP server. 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.
- **IP Address.** Default = **192.168.205.1**). Set a valid unique **IP address** and **Netmask**. (Default = **255.255.255.0**). for each Viper in the network. In Bridge mode, all the Viper SCs must be configured for the same IP subnet; in Router mode, each Viper SC must be configured for a unique subnet.
- **DHCP (Dynamic Host Configuration Protocol) Server.** Select **Enabled/Disabled**. *Default = Enabled*. DHCP provides a framework for passing configuration information. E.g.: Assigns IP address to Hosts (i.e. PC/RTU) on a TCP/IP network. Requires **Start Address**, **Number of Leases**, **Lease Duration** (in minutes, where 0=Infinite), and **Gateway**.



- **Start Address.** Represents the 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, Viper automatically calculates the Lease Start Address (equal to Ethernet IP Address plus one).
- **Number of Leases.** Represents the 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.** Displays the IP address of the gateway assigned by the DHCP server. In Bridge mode, the default gateway is 0.0.0.0. In Router mode, the default gateway is the IP address of the unit itself. To override the default setting, enter a valid IP address in the text field.
- **MTU (Maximum Transfer Unit).** Enter a value from **576-1500**. *Default = 1500*. The MTU is the maximum number (in bytes) the unit will send in a packet.
- **MAC (Media Access Control) Address.** This is the unique address that a manufacturer assigns to each networking device. Users can not change the MAC address.

---

#### 4.3.2.2 RF INTERFACE

- **IP Address.** *Default = 10.128.13.68*. The RF IP address is the address that is used when sending data and control packets in a Viper network. The **Netmask** (*Default = 255.0.0.0*.) must be the same for all Viper in the network.
- **MTU (Maximum Transfer Unit).** Enter a value from **576-1500**. *Default = 1500*. This value represents the maximum number of bytes Viper will send in a packet.
- **MAC Address.** *Default = 00:0E:81*. The RF MAC Address is a shortened version of the Ethernet MAC address which is used to identify the radio to other Viper SCs 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). While users cannot change the Ethernet MAC address, they may enter a new RF MAC address for the device. The RF MAC address must be unique for each Viper in the network. When the network is configured for router mode, this feature is useful when replacing a Viper in the field with a new one. The new Viper can be programmed to have the same RF MAC, Ethernet IP Address, and RF IP Address as the Viper that is being replaced. When the new Viper is installed, neighboring Vipers in the network will not know the original Viper was replaced. Neighboring Vipers will not need to have their neighbor tables updated.
- **Default Gateway.** *Default = 0.0.0*. Allows the user to enter the IP address of the access point to be used as the gateway to the management network. If there is one Viper SC configured as an Access Point in the network, all the other Viper will set their Default Gateway equal to the RF IP address of the Access Point.

---

#### 4.3.3 CHANNEL TABLE

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

Figure 23 – Setup(Basic)→Channel Table

Radio Capabilities					
<b>Rx Frequency Range</b>	Min 215.000000 MHz		Max 240.000000 MHz		
<b>Tx Frequency Range</b>	Min 215.000000 MHz		Max 240.000000 MHz		
<b>Bandwidth</b>	Max 50 KHz				
<b>Output Power Range</b>	Min 1.0 Watts		Max 10.0 Watts		

Current Settings					
<b>RX Frequency</b>	235.000000 MHz	<b>Output Power</b>	1.0 Watts		
<b>TX Frequency</b>	230.000000 MHz				
<b>Bandwidth</b>	50 KHz	<b>Bit Rate</b>	128 Kbps	<b>Modulation</b>	16 FSK
<b>Multi-Speed Mode</b>	Disabled	<b>Mode</b>	ANSI		

Channels					
<input checked="" type="radio"/> Transmitter Disabled					
#	RX (MHz)	TX (MHz)	PA Power (Watts)	Bandwidth (KHz)	Data And Control Packet Bit Rate (Kbps)
<input type="radio"/> 1	<input type="text" value="000.000000"/>	<input type="text" value="000.000000"/>	<input type="text" value="5.0"/>	<input type="text" value="12.5"/> ▾	<input type="text" value="16"/> ▾
<input type="radio"/> 2	<input type="text" value="000.000000"/>	<input type="text" value="000.000000"/>	<input type="text" value="5.0"/>	<input type="text" value="12.5"/> ▾	<input type="text" value="16"/> ▾
<input type="radio"/> 3	<input type="text" value="000.000000"/>	<input type="text" value="000.000000"/>	<input type="text" value="5.0"/>	<input type="text" value="12.5"/> ▾	<input type="text" value="16"/> ▾
<input type="radio"/> 4	<input type="text" value="000.000000"/>	<input type="text" value="000.000000"/>	<input type="text" value="5.0"/>	<input type="text" value="12.5"/> ▾	<input type="text" value="16"/> ▾
<input type="radio"/> 5	<input type="text" value="000.000000"/>	<input type="text" value="000.000000"/>	<input type="text" value="5.0"/>	<input type="text" value="12.5"/> ▾	<input type="text" value="16"/> ▾
<input type="radio"/> 25	<input type="text" value="000.000000"/>	<input type="text" value="000.000000"/>	<input type="text" value="5.0"/>	<input type="text" value="12.5"/> ▾	<input type="text" value="16"/> ▾
<input type="radio"/> 26	<input type="text" value="000.000000"/>	<input type="text" value="000.000000"/>	<input type="text" value="5.0"/>	<input type="text" value="12.5"/> ▾	<input type="text" value="16"/> ▾
<input type="radio"/> 27	<input type="text" value="000.000000"/>	<input type="text" value="000.000000"/>	<input type="text" value="5.0"/>	<input type="text" value="12.5"/> ▾	<input type="text" value="16"/> ▾
<input type="radio"/> 28	<input type="text" value="000.000000"/>	<input type="text" value="000.000000"/>	<input type="text" value="5.0"/>	<input type="text" value="12.5"/> ▾	<input type="text" value="16"/> ▾
<input type="radio"/> 29	<input type="text" value="000.000000"/>	<input type="text" value="000.000000"/>	<input type="text" value="5.0"/>	<input type="text" value="12.5"/> ▾	<input type="text" value="16"/> ▾
<input type="radio"/> 30	<input type="text" value="000.000000"/>	<input type="text" value="000.000000"/>	<input type="text" value="5.0"/>	<input type="text" value="12.5"/> ▾	<input type="text" value="16"/> ▾
<input type="radio"/> 31	<input type="text" value="000.000000"/>	<input type="text" value="000.000000"/>	<input type="text" value="5.0"/>	<input type="text" value="12.5"/> ▾	<input type="text" value="16"/> ▾
<input type="radio"/> 32	<input type="text" value="000.000000"/>	<input type="text" value="000.000000"/>	<input type="text" value="5.0"/>	<input type="text" value="12.5"/> ▾	<input type="text" value="16"/> ▾
<input type="button" value="Clear Channel Table"/>					

---

#### 4.3.3.1 RADIO CAPABILITIES

Transmit and Receive (TX/RX) Frequency Range and Output Power Range is factory set.

- 140-5018-502: VHF, 136.000-174.000 MHz, 1-10W
- 140-5028-502: VHF, 215.000-240.000 MHz, 1-10W
- 140-5028-504: VHF, 215.000-240.000 MHz, 1-10W
- 140-5048-302: UHF Range 3, 406.125-470.000 MHz, 1-10W
- 140-5048-502: UHF Range 5, 450.000-511.975 MHz, 1-10W
- 140-5098-304: PCS, 880.000-902.000 MHz, 1-8W
- 140-5098-502: ISM, 928.000-960.000 MHz, 1-8W
- 140-5098-504: ISM, 928.000-960.000 MHz, 1-8W

European, Australian, and New Zealand Compliant Models

- 140-5018-600: VHF, 142.000-174.000 MHz, 1-10W
- 140-5048-400: UHF Range 3, 406.125-470.000 MHz, 1-10W
- 140-5048-600: UHF Range 5, 450.000-511.975 MHz, 1-10W

---

#### 4.3.3.2 CURRENT SETTINGS

Displays the current RX/TX frequencies, output power, channel type, bandwidth, bit rate, modulation, multi-speed and ETSI parameters.

---

#### 4.3.3.3 CHANNELS

Factory set to **Transmitter Disabled** until a valid frequency has been entered. Viper will not transmit until valid RX and TX frequencies have been entered and this radio button has been deselected.

There are 32 channels available. 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 Viper in the network must be set to the same bandwidth.

Refer to **Appendix A – Specifications** for available bandwidths and data rates by model. 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.

---

#### 4.3.4 SERIAL PORTS

Viper has two serial ports (SETUP/COM). Each port must be activated independently. 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.

Check the **Enabled** box at the top to activate.



Figure 24 – Setup (Basic)→Serial Ports

SETUP Port	COM Port
<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled
Speed 19200	Speed 9600
Data bits <input type="radio"/> 7 <input checked="" type="radio"/> 8	Data bits <input type="radio"/> 7 <input checked="" type="radio"/> 8
Stop bits <input checked="" type="radio"/> 1 <input type="radio"/> 2	Stop bits <input checked="" type="radio"/> 1 <input type="radio"/> 2
Parity <input type="radio"/> Odd <input type="radio"/> Even <input checked="" type="radio"/> None	Parity <input type="radio"/> Odd <input type="radio"/> Even <input checked="" type="radio"/> None
DCD Control Never asserted	DCD Control Envelope mode
Packet Forwarding Threshold 4 MARK character time	Packet Forwarding Threshold 4 MARK character time
Flow Control CTS-based	Flow Control None
Connection Control Switched (DTR bringup/teardown)	Connection Control Permanent (3-wire)
IP Gateway Service <input checked="" type="radio"/> CLI Service <input type="radio"/> Serial/RF bridge - DOX mode <input type="radio"/> Online Diagnostics <input type="radio"/> Custom	IP Gateway Service <input type="radio"/> CLI Service <input checked="" type="radio"/> Serial/RF bridge - DOX mode <input type="radio"/> Serial/RF bridge - RTS/CTS mode <input type="radio"/> Online Diagnostics <input type="radio"/> Custom
IP Gateway Transport TCP Client	IP Gateway Transport 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 <input type="checkbox"/> Send all buffered data before negating CTS <input type="checkbox"/> Fragment large messages <input type="checkbox"/> Discard all buffered data when entering flow control Status: READY

- **Speed.** Select Baud Rate to match connected device. **SETUP** 300/1200/2400/4800/9600/19200 Baud Rate. Default = **19200**. **COM** 300/1200/2400/4800/9600/19200/38400/57600/115200. Default = **9600**.
- **Data bits.** Number of bits making up the data word. Select **7/8**. Default = **8**.
- **Stop bits.** Select **1/2**. Default = **1**. Marks the end of the serial port data byte.
- **Parity.** Select **Even/Odd/None** Default = **None**. Identify the sum of bits.
- **DCD (Data Carrier Detect) Control.** Select **Never Asserted/Always Asserted/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. Request to Send/Clear to Send. Flow control requires a 5 wire connection to the Setup Port or Com Port.
- **Connection Control.** Select **Permanent (3-wire)/Switched (DTR bringup/teardown)**. Configure to match connected device settings. **Permanent (3-wire)**, serial port is always enabled. Select **Switched (DTR bringup/teardown)** to enable/disable the serial connection. DTR on the serial port can be used to open and close the TCP connection.

---

#### 4.3.4.1 IP GATEWAY SERVICE

Serial port(s) can be configured to provide several different services.

- **CLI Service.** Command Line Interface; Access to the Command Line Interface command shell is password protected and is reserved for authorized personnel only.
- **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 Viper SC returns a CTS signal to the device. This setting is unique to the COM Port.
- **Online Diagnostics.** TCP/IP based RF diagnostics for the entire Viper SC network will be collected and sent to the serial port.
- **Custom.** Select to enable **IP Gateway Transport** configuration. *Setup Port Default = CLI Service. COM Port Default = Serial/RF Bridge.*

---

#### 4.3.4.2 IP GATEWAY TRANSPORT

Viper allows the user to select between two commonly used protocols for sending data to/from the serial port: UDP/TCP

- **UDP** is a simple method of sending data. Connections do not need to be opened or closed before sending data. No handshaking is required; therefore, there is no acknowledgement or retries built into the UDP protocol. In UDP mode, Viper 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** is a reliable method of data transmission, with acknowledgements and retries built into the protocol. TCP 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. **TCP** 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 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 the Remote IP Address and the Remote Port Number when there is data received on the serial port AND there is no TCP connections already established.

In **TCP Client** mode, Viper 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 Viper will try to reestablish the TCP connection.

In **TCP Server** mode the Viper SC 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 Viper TCP server will leave the TCP connection open indefinitely, whether or not data is being sent. However, if the Viper is unable to send data successfully to the TCP Client (ie. no TCP acknowledgements are received from the remote endpoint) the Viper SC's terminal server will close the faulty TCP connection. For more information on TCP acknowledgements, refer to **Section 4.4.4**.

**Table 11 – TCP/UDP Parameter Usage**

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

- **Local IP Address.** The local IP address can be set to one of three values: Ethernet IP address, RF IP address, or either (0.0.0.0).
  - **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.

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

---

#### 4.3.4.3 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 data will be sent before the Viper SC 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.

### 4.4 SETUP (ADVANCED)

From the navigation frame, select **Setup (Advanced)** to open **RF Optimizations**. From here, you may also select:

- IP Addressing (See Section 4.4.3).
- IP Optimization (See Section 4.4.4).
- IP Routing (See Section 4.4.5).
- Time Source (See Section 4.4.6).
- Alarm Reporting (See Section 4.4.7).
- User Settings (See Section 4.4.8).



#### 4.4.1 RF OPTIMIZATIONS/MAC ADVANCED SETTINGS

Figure 25 – Setup(Advanced)→RF Optimizations/MAC Advanced Settings

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) ▼

- **Duplicates Detection Period.** Enter a value from 1000 to 15000 to specify the time period (in milliseconds) Default = **5000 ms**. Viper 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**. Enter a value to specify the number of times the MAC layer will try to resend a packet if the unit does not receive an acknowledgement reply from the receiving device. Increasing the retries may improve marginal RF paths. For this field to be active, Viper must be programmed for RF Acknowledgments **Enabled** as shown in Section 4.4.4.
- **RTS Threshold.** *Default = 128.* Viper 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 Viper 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 Viper SC network to avoid collisions in networks with multiple coverage areas. Before transmitting an RTS frame, a Viper SC 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 Viper SC will always use over-the-air RTS/CTS handshaking. A value equal to the RF\_MTU (OTA maximum transmit unit) means the Viper SC will never use RTS/CTS handshaking. A value of 128 means the Viper SC will use RTS/CTS for packets larger than 128 bytes. Note: This value should not be confused with RTS/CTS for RS232 Serial ports.
- **Carrier Sense Level Threshold.** *Default = -110 dBm.* The threshold Viper uses to determine whether a received RF signal is a valid message or unwanted noise. If RF level above threshold is detected, Viper will not transmit data. Signals are received and decoded. Outgoing data is buffered until the channel becomes available. Threshold may be raised to prevent false detection in noisy environments or lowered to gain extra receive sensitivity. Lower thresholds should only be used when ambient RF noise is very low. Receive sensitivity depends upon the channel bandwidth/speed being used. Refer to Product Specifications for Carrier Sense by model.
- **Listen Before Transmit.** Default = **Enabled (listen to noise and data)**.

- **Enabled (listen to noise and data).** Viper listens on the Rx frequency and determines if the RF channel is available. Channel is available so long as received level is higher than the carrier sense threshold. When the channel is busy, Viper receives and decodes all remote messages Data is buffered and sent when the channel becomes available.

Received level is above the carrier sense threshold if:

- Viper is receiving valid data
  - Viper is not receiving data because two or more Viper SCs are transmitting at the same time causing a collision
  - Viper is not receiving data because the RF level is right at or below data sensitivity or
  - There is interference from another RF system or electrical devices on the frequency that Viper is operating on.
- **Enabled (listen to data only).** Viper SC will monitor the RF level on the receive channel. When the received level is above the carrier sense threshold, Viper SC will try to receive and decode any and all messages from remote Viper SCs. When data is ready to transmit, Viper SC will first check the receive level. If the receive level is below the carrier sense threshold, Viper will immediately transmit data. If the receive level is above the carrier threshold, Viper will try to determine if it is receiving valid data or just noise. If it is receiving noise, Viper will go ahead and transmit. If it is receiving valid data, Viper will wait until the complete packet has been received before transmitting. Viper SC will typically takes 5-250 ms to determine if it is receiving valid data or just noise.
  - **Disabled.** Viper will attempt to receive/decode data when the received RF level is above the carrier sense threshold. When the Viper SC has data to transmit it will immediately transmit the data. The Viper SC will immediately stop receiving any packets and will transmit over any other Viper SCs 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.

#### 4.4.2 IP SERVICES

From the navigation frame, select **Setup(Advanced)** → **IP Services** to configure RIPV2, IPSD, NAT and SNMP.

**Figure 26 – IP Services**

<b>RIPV2</b> ⓘ	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled		
<b>IPSD</b> ⓘ	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled		
<b>NAT</b> ⓘ	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled		
<b>SNMP</b>			
<b>SNMP AGENT</b> ⓘ	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled		
<input type="radio"/> Add ⓘ <input type="radio"/> Delete	<input type="text"/>		
<b>Trap IP List</b>	192.168.206.100 192.168.205.20 192.168.205.10		
<b>MIB</b>	<a href="#">Download mibs.zip</a>		
<b>NAT Private Network Table</b>			
	IP Address	Netmask	Enable
<b>ETH</b> ⓘ	192.168.254.0	255.255.255.252	<input type="checkbox"/>
<b>RF</b> ⓘ	10.0.0.0	255.0.0.0	<input type="checkbox"/>
<b>USER1</b> ⓘ	<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>	<input type="checkbox"/>
<b>USER2</b> ⓘ	<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>	<input type="checkbox"/>
<b>USER3</b> ⓘ	<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>	<input type="checkbox"/>
<input type="button" value="Clear Table"/>			

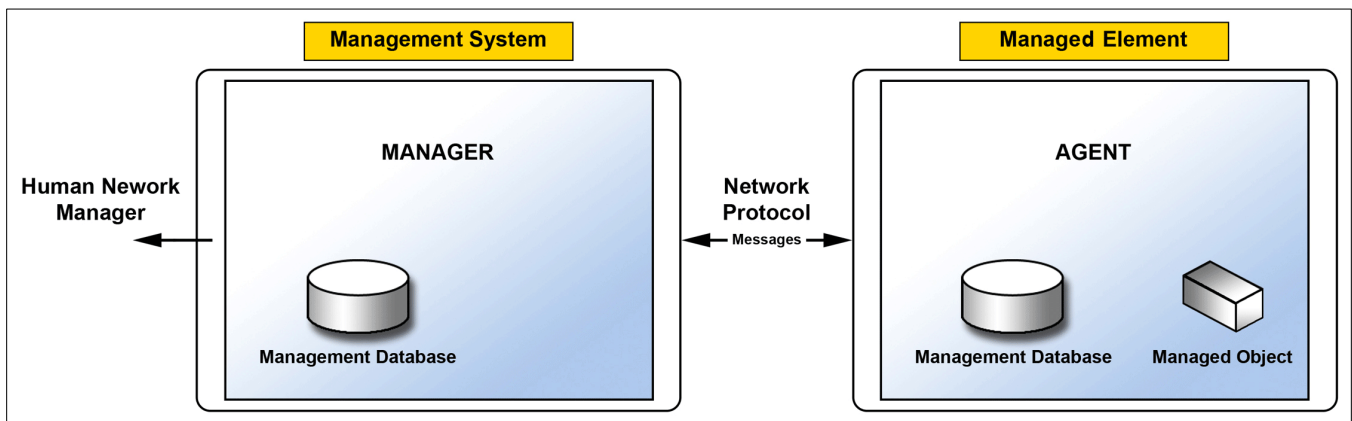
<b>NAT Port Forwarding Table</b>				
Protocol	Public Port Number First Last	Private IP Address	Private Port Number	Enable
ⓘ <input type="text" value=""/>	<input type="text" value="0"/> - <input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0"/>	<input type="checkbox"/>
ⓘ <input type="text" value=""/>	<input type="text" value="0"/> - <input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0"/>	<input type="checkbox"/>
ⓘ <input type="text" value=""/>	<input type="text" value="0"/> - <input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0"/>	<input type="checkbox"/>
ⓘ <input type="text" value=""/>	<input type="text" value="0"/> - <input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0"/>	<input type="checkbox"/>
ⓘ <input type="text" value=""/>	<input type="text" value="0"/> - <input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0"/>	<input type="checkbox"/>
<input type="button" value="Clear Table"/>				

- **RIPV2.** Select **Enabled/Disabled.** *Default = Disabled.* 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 (IP Services Delivery).** Select **Enabled/Disabled.** *Default = Enabled.* Enables the generation of locally provided IP Services such as online diagnostics, etc.
- **NAT (Network Address Translation).** Select **Enabled/Disabled.** *Default = Disabled.* For more information on NAT, refer to **Section 4.4.2.2.**

#### 4.4.2.1 SNMP

- **SNMP (Simple Network Management Protocol) Agent.** Select **Enabled/Disabled.** *Default = Disabled.* Enable to allow the MIB (Management Information Base) in the Viper to be viewed using an external MIB browser or network management software.

**Figure 27 – SNMP Model: Manager/Agent**



SNMP 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. SNMP uses basic messages (such as GET, GET-NEXT, SET, and TRAP) to communicate between the manager and the agent.

SNMP provides means to monitor, collect, and analyze diagnostic information.

The Viper SC is compatible with SNMPv2c.

Traps – Traps (or alarms) can be automatically generated by the Viper SC whenever the forward, reverse or PA power goes out of specification.

Note: To configure and enable individual traps, navigate to Setup (Advanced) → Alarm Reporting.

These traps can be sent to user-specified IP addresses. To add an address to the Trap IP List: Select “Add” and type the new IP address to be added to the read-only Trap IP list. Click “Apply” at the bottom of the page. The “Trap IP List” section will expand downward to show all addresses in the list.

The traps can be forwarded to all defined SNMP servers present in the Trap IP List.

To delete an address from the Trap IP List: Select “Delete” and type the IP address to be deleted from the read-only Trap IP list. Click “Apply” at the bottom of the page. The IP address should disappear from the Trap IP List.

Download mibs.zip - The Viper MIB is bundled with each unit's firmware. Click "Download mibs.zip" and a pop-up dialog box will appear in your browser asking you to open or save the file to your PC. Save the zip file to a desired location. Unzip the contents of mibs.zip file to a location where your SNMP manager can find it.

Caution: Certain MIB Browsers (standalone or integrated in SNMP Manager) may require you to modify the MIB files extension (for example, from .MIB to .TXT).

- **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.

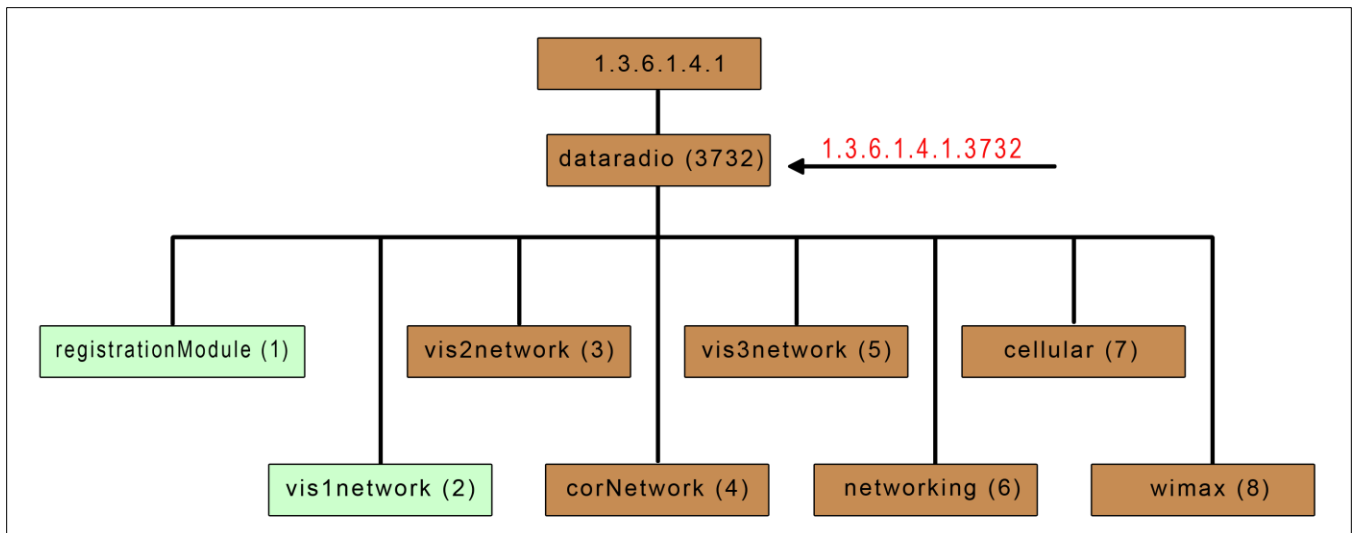
### Viper MIB Files

Each Viper firmware package is bundled with three MIB files (found inside mibs.zip file): (1) dataradio-regs.MIB contains a top level set of managed object definitions aimed at managing Dataradio products, (2) 1213.MIB contains a set of managed object definitions aimed at managing TCP/IP-based internets, and (3) VIPER.MIB contains a set of managed object definitions aimed at managing Viper radio 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 28** illustrates this tree-like structure for dataradio-regs.mib MIB, which comes bundled with every Viper SC unit package. A path to any object can be easily traced starting from the root (top of the tree). For example, object titled “dataradio” has a unique OID: 1.3.6.1.4.1.3732. The MIB associates each OID with a label (e.g. “dataradio”) 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 28 – Dataradio-REGS MIB tree**



## Viewing MIB Files

To view the hierarchy of SNMP MIB variables in the form of a tree and view additional information about each node, open each MIB files with a MIB browser. In a MIB browser, each object (or node) can be selected and its properties (including OID) can be observed. For simple networks, any MIB browser supporting SNMP v2c could be used. However, for managing complex networks, a more advanced SNMP Manager/Browser is recommended.

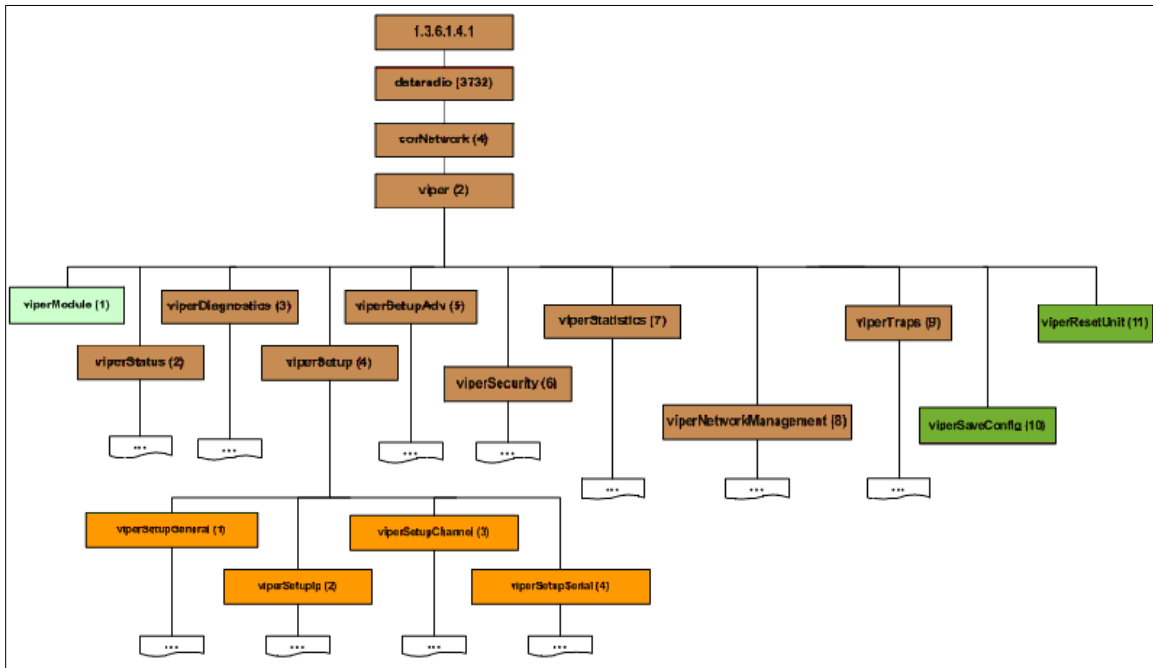
Both **Read Community** and **Read/Write Community** passwords are required to operate SNMP MIB. For all Viper SC, the same password is used for both read and read/write. This password is the same password used to access the Viper SC web pages.

**Figure 29** shows top-level objects of the Viper SC.mib file. It includes eight branches (b) and three nodes or leaves (l):

- *Viper SCModule (l)*
- *Viper SCStatus (b)*
- *Viper SCDiagnostics (b)*
- *Viper SCSetup (b)*
- *Viper SCSetupAdv (b)*
- *Viper SCStatistics (b)*
- *Viper SCSecurity(b)*
- *Viper SCNetworkManagement (b)*
- *Viper SCTraps (b)*
- *Viper SCSaveConfig (l)*
- *Viper SCResetUnit (l)*

The eight branches expand into additional branches and leaves. The last two nodes are single leaves that perform specific functions following changes to the main branches. Again, all Viper SC MIB objects can be accessed through a MIB browser.

**Figure 29 – Viper OID Tree**

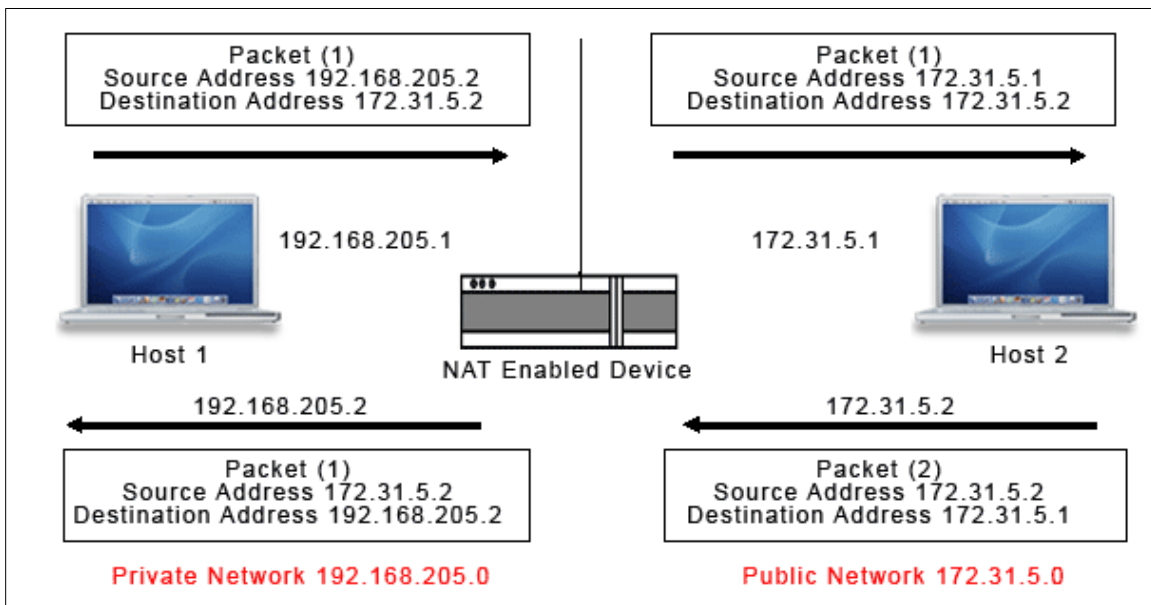


#### 4.4.2.2 NAT OVERVIEW

NAT is the process of modifying network address information in datagram (IP) packet headers while in transit across a traffic routing device for the purpose of remapping one IP address space into another. Most often, NAT is used in conjunction with network masquerading (or IP masquerading) which is a technique that hides an entire IP address space, usually consisting of private network IP addresses, behind a single IP address in another, often public address space. This mechanism is implemented in a routing device that uses stateful translation tables to map the "hidden" addresses into a single IP address and then readdresses the outgoing Internet Protocol (IP) packets on exit so that they appear to originate from the router. In the reverse communications path, responses are mapped back to the originating IP address using the rules ("state") stored in the translation tables.

As described, the method enables communication through the router only when the conversation originates in the masqueraded network, since this establishes the translation tables. For example, a web browser in the masqueraded network can browse a website outside, but a web browser outside could not browse a web site in the masqueraded network. Most NAT devices today allow the network administrator to configure translation table entries for permanent use. This feature is often referred to as "static NAT" or port forwarding and allows traffic originating in the 'outside' network to reach designated hosts in the masqueraded network.

**Figure 30 – 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 30**).

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).

#### 4.4.2.2.1 NAT ON VIPER

In a Viper SC, it is normally used on the WAN side of an IP network to hide local IP addresses from an external IP network.

The purpose of the NAT protocol is to hide a private IP network from a public network. This mechanism serves first as a firewall and second 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 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.

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

#### 4.4.2.2.1.1 ETHERNET INTERFACE PRIVATE

Figure 31 shows NAT enabled for the Ethernet interface.

Figure 31 – NAT enabled, Ethernet (Private)

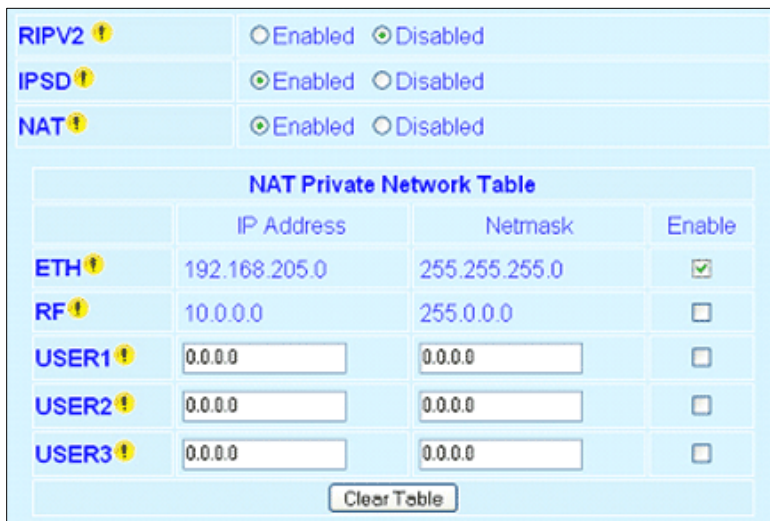
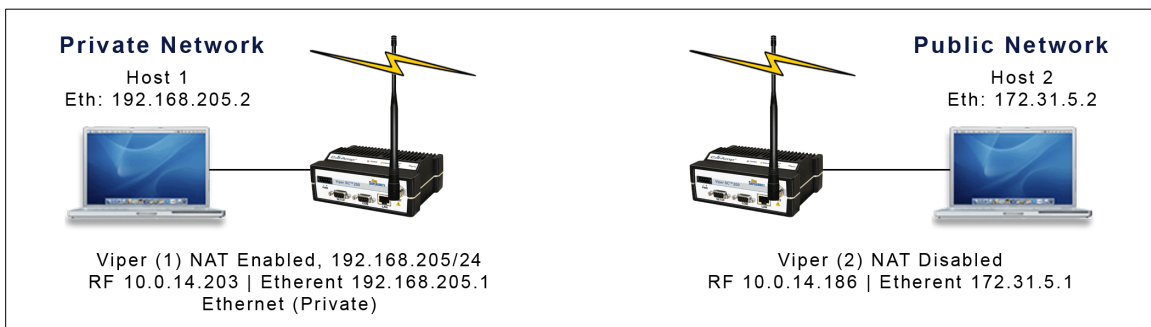


Figure 32 shows a configuration protecting Viper (1) Ethernet interface IP address from hosts located on a public network.

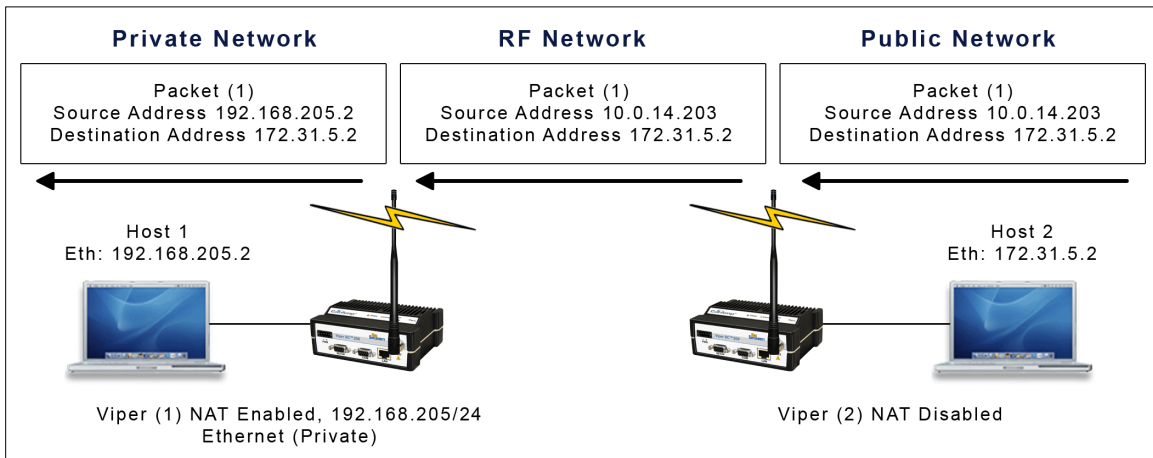
Figure 32 – NAT Enabled, Ethernet Interface (Private)



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 Viper SC(1) as shown in Figure 33.



**Figure 33 – Private to Public Packet Flow**



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.

#### 4.4.2.2.1.2 RF INTERFACE PRIVATE

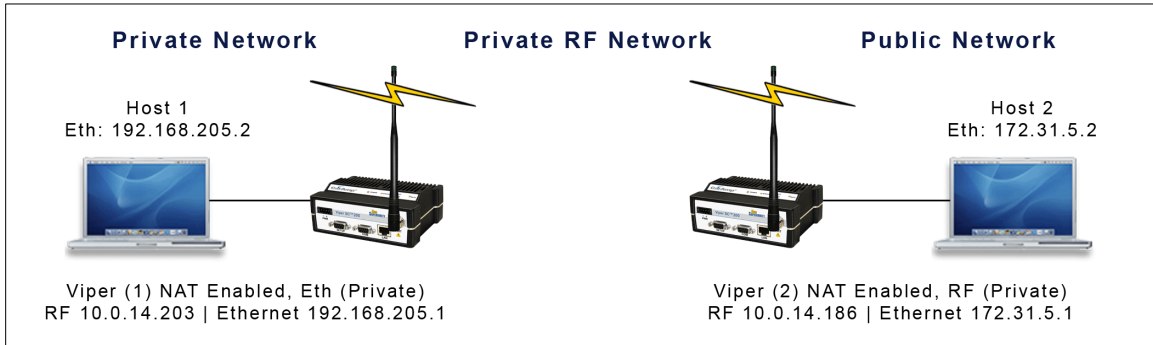
Figure 34 shows the NAT enabled for the RF interface.

**Figure 34 – NAT Enabled, RF (Private)**

RIPV2	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled		
IPSD	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled		
NAT	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled		
NAT Private Network Table			
	IP Address	Netmask	Enable
ETH	192.168.205.0	255.255.255.0	<input type="checkbox"/>
RF	10.0.0.0	255.0.0.0	<input checked="" type="checkbox"/>
USER1	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="checkbox"/>
USER2	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="checkbox"/>
USER3	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="checkbox"/>
<input type="button" value="Clear Table"/>			

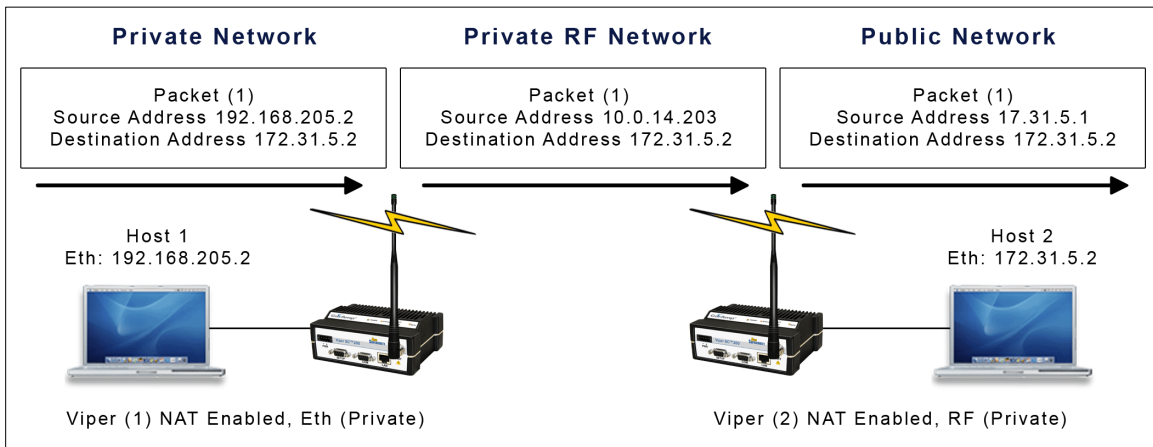
Figure 35 shows a Viper SC configuration protecting Viper SC (2) RF interface and Viper SC (1) Ethernet interface from hosts located on a public network.

**Figure 35 – NAT Enabled, RF (Private), Ethernet (Private)**



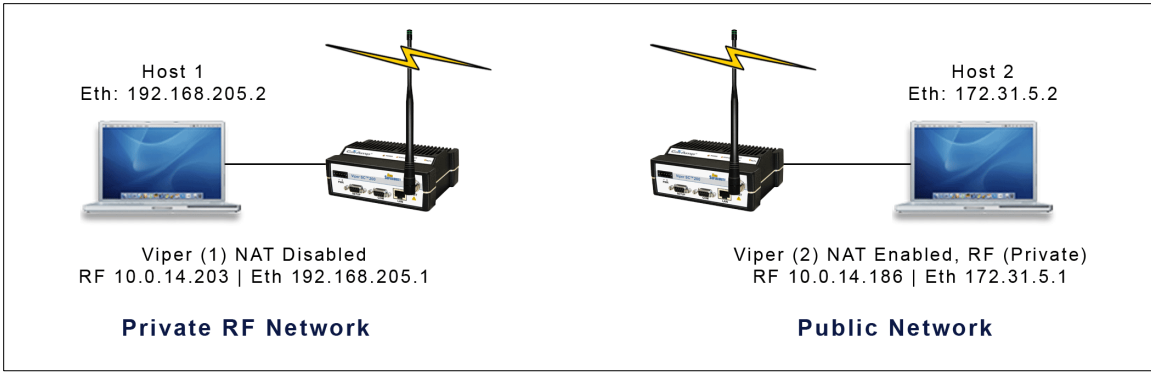
An IP packet whose source IP address originates from the RF network and is sent towards the Ethernet network will have its source IP address replaced by the Ethernet IP address of Viper (2). Notice in this configuration the Ethernet IP address for Viper (1) is considered private and the RF IP address for Viper (2) is considered private. **Figure 36** shows how the packets will be modified as the packets pass through the network.

**Figure 36 – Packet Flow: Ethernet and RF (Private)**

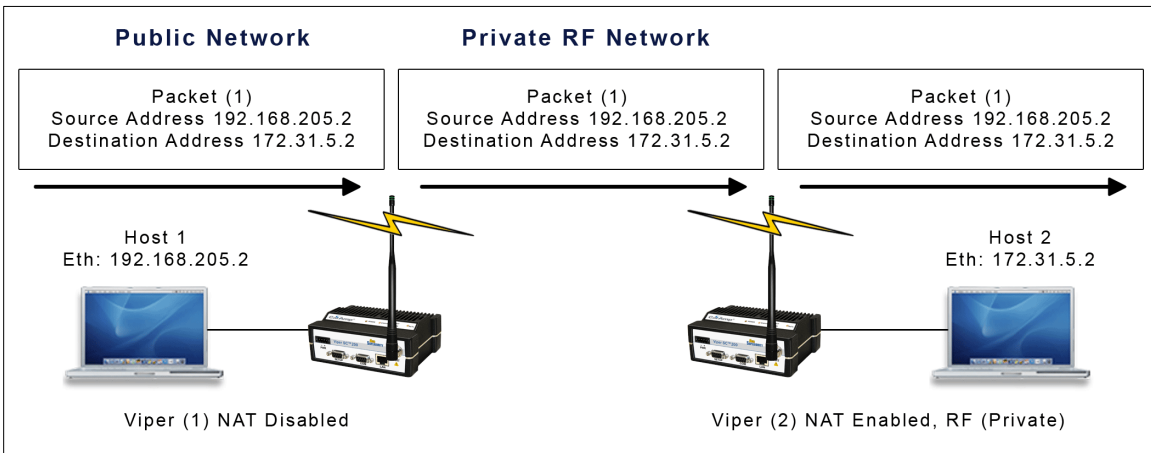


**Figure 37**, the RF interface of Viper (2) is considered private. NAT is disabled for Viper (1). Viper (1) changes the source address of the packet, making Viper (2) believe that the packet originated from the RF network.

**Figure 37 – RF Interface (Private)**



**Figure 38 – Packet Flow, RF Interface (Private)**



**Figure 38** shows when Host 1 sends a packet, the source IP address is not changed by Viper (2) because the source does not originate from the private RF network.

#### 4.4.2.3 USER NAT ENTRIES

The user can add three USER IP addresses that will be considered private.

**Figure 39** 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 Viper SC, but not added to the table, USER3 192.168.205.87 would not be considered private.

**Figure 39 – USER1 and USER2 (Private)**

<b>RIPV2</b> ⓘ	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled		
<b>IPSD</b> ⓘ	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled		
<b>NAT</b> ⓘ	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled		
<b>NAT Private Network Table</b>			
	IP Address	Netmask	Enable
<b>ETH</b> ⓘ	192.168.205.0	255.255.255.0	<input type="checkbox"/>
<b>RF</b> ⓘ	10.0.0.0	255.0.0.0	<input type="checkbox"/>
<b>USER1</b> ⓘ	<input type="text" value="192.168.205.125"/>	<input type="text" value="255.255.255.255"/>	<input checked="" type="checkbox"/>
<b>USER2</b> ⓘ	<input type="text" value="192.168.205.90"/>	<input type="text" value="255.255.255.255"/>	<input checked="" type="checkbox"/>
<b>USER3</b> ⓘ	<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>	<input type="checkbox"/>
<input type="button" value="Clear Table"/>			

#### 4.4.2.4 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.

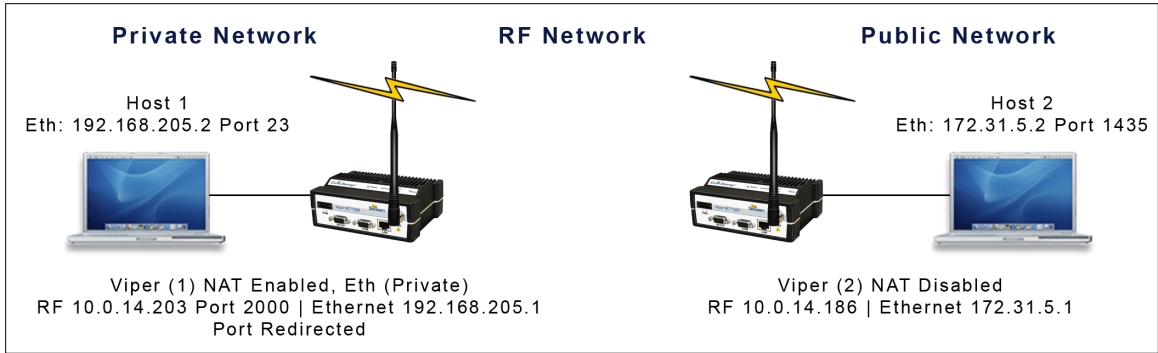
**Figure 40** shows the NAT Eth IP subnet 192.168.205.0 will be hidden from the Public Network. Any TCP packets sent to the Viper with port number 2000 will be redirected to the Private IP Address and Private Port Number entered in the NAT Port Forwarding Table.

**Figure 40 – Port 2000 is redirected to 192.168.205.125:23**

<b>ETH</b> ⓘ	192.168.205.0	255.255.255.0	<input checked="" type="checkbox"/>		
<b>RF</b> ⓘ	10.0.0.0	255.0.0.0	<input type="checkbox"/>		
<b>USER1</b> ⓘ	<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>	<input type="checkbox"/>		
<b>USER2</b> ⓘ	<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>	<input type="checkbox"/>		
<b>USER3</b> ⓘ	<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>	<input type="checkbox"/>		
<input type="button" value="Clear Table"/>					
<b>NAT Port Forwarding Table</b>					
Protocol	Public Port Number First Last		Private IP Address	Private Port Number	Enable
ⓘ TCP ▾	<input type="text" value="2000"/>	<input type="text" value="2000"/>	<input type="text" value="192.168.205.125"/>	<input type="text" value="23"/>	<input checked="" type="checkbox"/>
ⓘ ▾	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0"/>	<input type="checkbox"/>
ⓘ ▾	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0"/>	<input type="checkbox"/>
ⓘ ▾	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0"/>	<input type="checkbox"/>
ⓘ ▾	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0"/>	<input type="checkbox"/>

**Figure 41** shows the Private Network 192.168.205.0 being protected from the Public Network 172.31.5.0. Viper (1) NAT Eth interface is enabled and Viper (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, Host 172.31.5.2 thinks the IP packets are coming from 10.0.14.203.

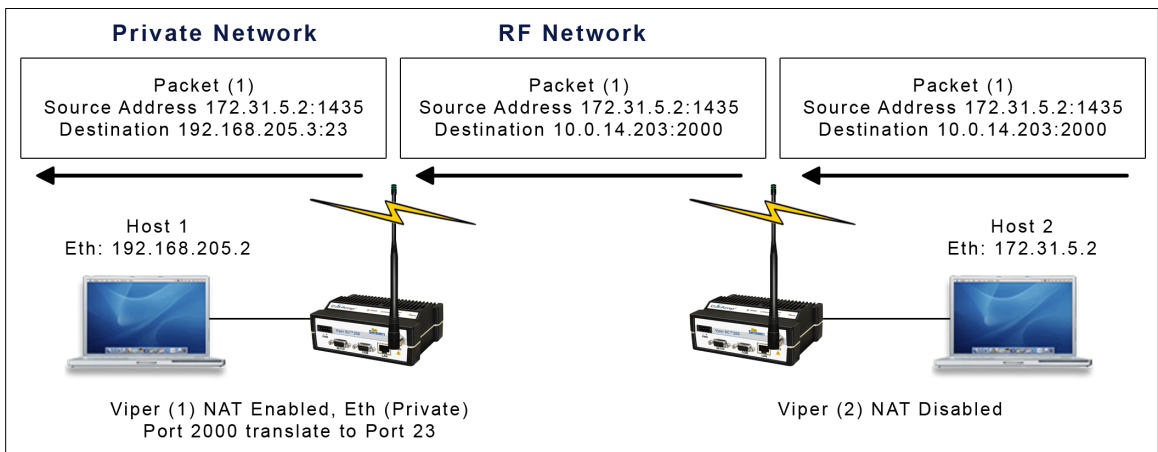
**Figure 41 – Port 2000 is redirected to 192.168.205.125:23**



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 192.168.205.2:23 (port 23) by sending the packets to 10.0.14.203:2000 (port 2000).

Figure 42 shows how the packets would be modified as they moved through the network.

Figure 42 – Packet Flow, Port Redirection



#### 4.4.3 IP ADDRESSING

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

Figure 43 – Advanced Setup/IP Addressing

Broadcast	
Directed Broadcast	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Limited Broadcast	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

Multicast		
Multicast Forwarding	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
Multicast to Broadcast (LAN to RF)	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	
Multicast to Broadcast (RF to LAN)	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	
Multicast Address List		
	First	Last
Group Range 1	<input type="text" value="239.192.0.1"/>	<input type="text" value="239.192.0.1"/>
Group Range 2	<input type="text" value="239.1.1.1"/>	<input type="text" value="239.1.1.1"/>
Group Range 3	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>
Group Range 4	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>
Group Range 5	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>

Multicast White List	
Group 1	<input type="text" value="0.0.0.0"/>
Group 2	<input type="text" value="0.0.0.0"/>
Group 3	<input type="text" value="0.0.0.0"/>
Group 4	<input type="text" value="0.0.0.0"/>
Group 5	<input type="text" value="0.0.0.0"/>

---

#### 4.4.3.1 BROADCAST

##### Directed Broadcast

This parameter controls the forwarding of directed broadcast packets from the LAN interface to the RF interface.

- Enabled** - Forwarding of directed broadcast packets is enabled (default).
- Disabled** - Forwarding of directed broadcast packets is disabled.

##### Limited Broadcast

This parameter controls the forwarding of limited broadcast packets from the LAN interface to the RF interface.

- Enabled** - Forwarding of limited broadcast packets is enabled.
- Disabled** - Forwarding of limited broadcast packets is disabled (default).

---

#### 4.4.3.2 MULTICAST

### Multicast Forwarding

This parameter controls the forwarding of multicast packets between the LAN interface and the RF interface. The packets forwarded from the LAN to the RF interface are identified by the "Multicast Address List" (all other multicast packets are dropped). The "Multicast White List" controls which multicast packets are forwarded from the RF interface to the LAN interface. When the "Multicast White List" is empty, all multicast packets received from the RF interface are forwarded to the LAN interface; otherwise, only the multicast packets identified in the white list are forwarded to the LAN.

- Enabled** - Forwarding of multicast packets is enabled (default).
- Disabled** - Forwarding of multicast packets is disabled.

### Multicast to Broadcast (LAN to RF)

When a multicast packet is forwarded from the LAN interface to the RF interface, the destination IP address can be changed to the broadcast IP address (255.255.255.255)

- Enabled** - Conversion of the destination IP address from multicast to broadcast is enabled.
- Disabled** - Conversion of the destination IP address from multicast to broadcast is disabled (default).

### Multicast to Broadcast (RF to LAN)

When a multicast packet is forwarded from the RF interface to the LAN interface, the destination IP address can be changed to the broadcast IP address (255.255.255.255)

- Enabled** - Conversion of the destination IP address from multicast to broadcast is enabled.
- Disabled** - Conversion of the destination IP address from multicast to broadcast is disabled (default).

## 4.4.3.2.1 MULTICAST ADDRESS LIST

---

All packets received from the LAN interface with a multicast destination IP address matching one of the multicast address identified in this list will be forwarded from the LAN interface to the RF interface.

## 4.4.3.2.2 MULTICAST WHITE LIST

---

All packets received from the RF interface with a multicast destination IP address matching one of the multicast address identified in this list will be forwarded from the RF interface to the LAN interface. If this list is empty, any packet received from the RF interface with a multicast destination IP address will be passed over the LAN. If this list is non-empty, any packet received from the RF interface with a multicast destination IP address that does not match an entry in this list will be dropped.

---

## 4.4.4 IP OPTIMIZATION



IP Optimization is only available in router mode.

**Figure 44 – IP Optimization (& Tuning)**

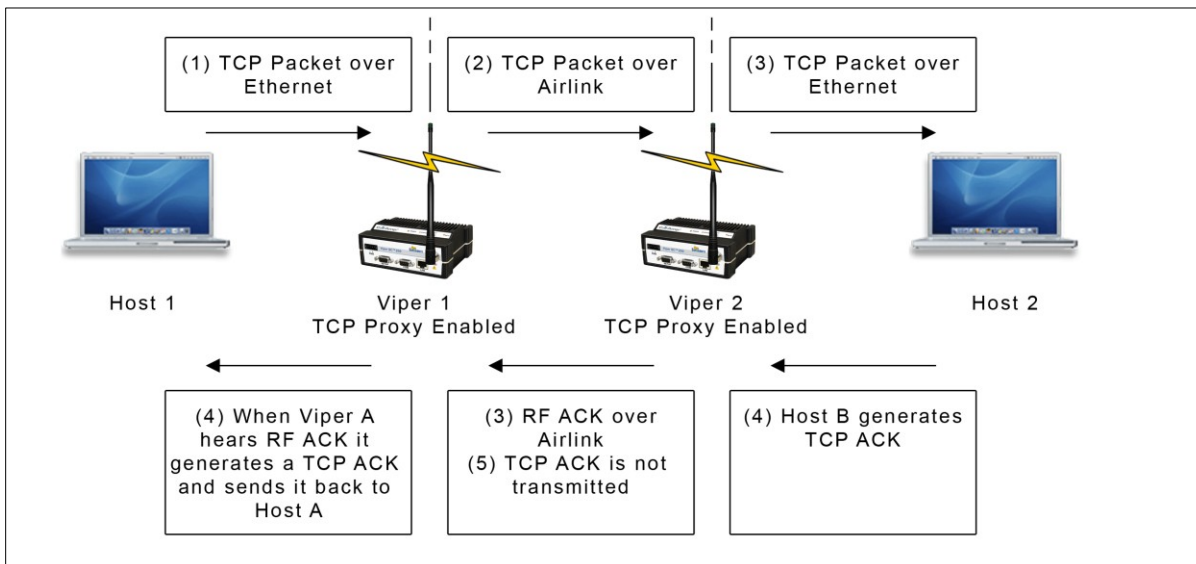
<b>OIP</b>	
<b>RF ACK</b> ⚠	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
<b>TCP Proxy</b> ⚠	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
<b>OIP Retries</b> ⚠	<input type="text" value="5"/>
<b>Duplicate Packet Removal</b>	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
<b>Quality Of Service (QoS)</b>	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

— **RF ACK (RF Acknowledgements)**. Select **Enabled/Disabled**. *Default = Disabled*. If **enabled**, the receiving Viper will reply with an acknowledgement message to the sending Viper to indicate that it has received the packet successfully. If the sending Viper does not receive the acknowledgement, it assumes the message was lost and resends the message. This number of retries is specified using MAC Retries (**Section 4.4.1**) and OIP Retries (below).

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.

— **TCP Proxy**. The TCP proxy optimizes the throughput of a TCP connection by removing some of the TCP packets from the Airlink. A Viper SC receiving a TCP packet over the air sends an RF acknowledgement to the sending unit. If the sending Viper SC 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 Viper SC 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 Viper SC and is not sent over the Airlink.

**Figure 45 – TCP Proxy**



In this example, the following events occur in this order:

- 1) Host A sends TCP data packet to Viper SC A.
  - 2) Viper SC A transmits packet over the air to Viper SC B.
  - 3) Viper SC B immediately responds with an RF acknowledgment and sends the TCP data packet to Host B.
  - 4) Viper SC A hears an RF acknowledgment from Viper SC 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) Viper SC B receives the TCP ACK but does not send it over the air saving bandwidth on the Airlink
- **OIP Retries.** Enter a value to specify the number of retries that the OIP layer will attempt if acknowledgement is not received from the destination Viper. *Default = 2*. Retries are only enabled if Router mode is selected and RF ACK is turned on. The number of retries should be increased if there is a marginal RF path to another unit.
  - **Duplicate Packet Removal.** Enables or disables the duplicate packet removal algorithm (by default it is disabled to preserve compatibility with older versions of the firmware). This algorithm detects duplicate packets that might appear through the system as a result of retransmissions.
  - **Quality of Service (QoS).** Enables or disables the RF Quality of Service algorithm. Enabled by default, this algorithm classifies data according to the local physical interface by which it enters the Viper to ensure that each interface obtains a fair share of the RF bandwidth. When QoS is enabled, the "Setup Port" and "Data Port" are assigned 25% each of the RF bandwidth; the "Ethernet Port" is assigned 50% of the RF bandwidth. When a port is not using its share of the bandwidth, that portion is assigned to the other ports.

When QoS is disabled, the packets are transmitted over the RF interface on a first come, first served basis.

---

#### 4.4.5 IP ROUTING

##### Figure 46 – IP Routing

- **Routing Table.** Displays the table of active IP routes. The routing table will be populated by the Neighbor Discovery process (described in **Section XXX**) and/or by manual entry as shown in **Section XXX**.
  - **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 Viper SC) of the destination gateway.
  - **Type.** There are three different types of routes. **Connected** (direct physical connection on the Ethernet port), **Static** (user-defined routes), and **Proprietary** (routes learned by the Viper SC unit that point to over-the-air destinations).
  - **Routing Entries.** This section allows the user to manually enter new routes or delete existing routes.

---

#### 4.4.6 TIME SOURCE

Figure 47 – Time Source

SNTP	
Client	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Server Address	<input type="text" value="0.0.0.0"/>
Period	<input type="text" value="64"/> Secs
SNTP UTC Time	<input type="text" value="0"/>

Time Zone	
TimeZone	<input type="text" value="(GMT) Greenwich Mean Time"/>
Daylight Saving	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

---

#### 4.4.6.1 SNTP

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

- **Client.** Select: **Enabled/Disabled**. Default = Disabled
- **Server Address.** Enter the IP Address of the SNTP Server in dot decimal format. Default = **0.0.0.0**
- **Period.** Enter the period of time (in seconds) at which the SNTP Server is polled. Default = **64**.
- **SNTP UTC Time.** Displays the last update received from the SNTP Server (in seconds). Default = **0**.

---

#### 4.4.6.2 TIME ZONE

Select Local Time Zone (**from list**). Default = **(GMT) Greenwich Mean Time**.

**Daylight Saving.** Select **Enabled/Disabled**. Default = **Disabled**.

---

#### 4.4.7 ALARM REPORTING/DIAGNOSTIC SETTINGS

Viper can be enabled to report several different types of alarms using the SNMP protocol. If SNMP is enabled (refer to Section 0) and reporting is enabled for a specific alarm, Viper will send an SNMP Trap to each of the IP addresses listed in the Trap IP List (refer to Section 0) whenever an alarm occurs.

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

Figure 48 – Alarm Reporting/Diagnostic Settings

Alarm Reporting	
Forward Power Alarm & Notification	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Reverse Power Alarm & Notification	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
PA Power Alarm & Notification	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

- **Forward Power Alarm & Notification.** Select **Enabled/Disabled**. *Default = Enabled*. 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 Viper SC 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.
- **Reverse Power Alarm & Notification.** Select **Enabled/Disabled**. *Default = Enabled*. 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 Viper SC 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.
- **PA Power Alarm & Notification.** Select **Enabled/Disabled**. *Default = Enabled*. 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 Viper SC 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 Viper SC 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 Viper SC will resume transmitting at full power and the PA Power Notification SNMP Trap will be generated to indicate that the Viper SC is operating at full power again.

---

#### 4.4.8 USER SETTINGS

**Figure 49 – User Settings**

Temperature Display	<input checked="" type="radio"/> Celsius <input type="radio"/> Fahrenheit
---------------------	--

---

##### 4.4.8.1 TEMPERATURE DISPLAY

Select **Celsius/Fahrenheit**. Default = **Celsius**.

## 4.5 SECURITY

From the navigation frame, select **Security** to configure passwords, encryption and access control.

### 4.5.1 PASSWORD AND ENCRYPTION

Figure 50 – Security Settings/Pass Control

The screenshot shows two configuration panels. The top panel, titled 'User', has four input fields: 'User ID', 'Old Password', 'New Password', and 'New Password (Confirm)'. Below these fields are 'Apply' and 'Cancel' buttons. The bottom panel, titled 'Encryption', has a radio button group with 'Enabled' and 'Disabled' (selected), an 'Encryption Pass Phrase' field containing 'Dataradio', and an 'Encryption Key' field containing the hexadecimal string 'b3 35 b0 7b ba 8d eb 5d 44 66 3c 3a a7 16 f1 80'. Below these fields are 'Apply' and 'Cancel' buttons.

#### 4.5.1.1 USER

- **User ID.** Enter a string up to 15 alphanumeric characters.
- **Old Password.** Default = ADMINISTRATOR.
- **New Password.** Enter a new password. Passwords are case sensitive and must be 8-15 characters in length.

#### 4.5.1.2 ENCRYPTION

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

- **Encryption.** Select: **Enabled/Disabled**. Default = **Enabled**.
- **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.** Example: **b3 35 b0 7b ba 8d eb 5d 44 66 3c 3a a7 16 f1 80**. The encryption key generated is for display only and does not need to be recorded.
- 

### 4.5.2 RADIUS

Viper uses **RADIUS** (Remote Authentication Dial in User Service) for authentication and authorization. RADIUS is a networking protocol that provides centralized authentication, authorization and accounting management for computers and devices to connect and use a network service.

RADIUS in the Viper is used for two authentication scenarios: **User Authentication** (see **Section 4.5.2.1.1**) and **Device Authentication** (see **Section 4.5.2.1.2**).

- RADIUS is used to authenticate users who wish to connect to a unit through the Viper SC Web Interface, the FTP server, or the command shell.
- RADIUS can also be used to authenticate devices based on their MAC addresses. Unauthorized devices will not be able to establish a VPN secure tunnel with an access point.

To use RADIUS within a Viper network, an external RADIUS server must be set up with a proper device database (identified by MAC addresses) and a user database. RADIUS transactions are encoded with an encryption key that is only known to the RADIUS server and each Viper device.

**Figure 51 – Security → Radius (Configuration)**

<b>General</b>	
<b>User Authentication</b>	
<b>Command Shell</b>	<input checked="" type="radio"/> Local <input type="radio"/> Radius&Local <input type="radio"/> Radius
<b>HTTP Server</b>	<input checked="" type="radio"/> Local <input type="radio"/> Radius&Local <input type="radio"/> Radius
<b>FTP Server</b>	<input checked="" type="radio"/> Local <input type="radio"/> Radius&Local <input type="radio"/> Radius
<b>Device Authentication</b>	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

<b>Client</b>	
<b>RADIUS Server IP</b>	<input type="text" value="0.0.0.0"/>
<b>RADIUS Server Port</b>	<input type="text" value="1812"/> (1-65535)
<b>RADIUS Secret</b>	<input type="text" value="dataradio"/>
<b>RADIUS Timeout</b>	<input type="text" value="3"/> Secs
<b>RADIUS Retries</b>	<input type="text" value="3"/> Times
<b>Delay Between Retries</b>	<input type="text" value="1"/> Secs

---

#### 4.5.2.1 GENERAL

RADIUS authentication can only be configured if your Viper is operating in router mode.

##### 4.5.2.1.1 USER AUTHENTICATION

---

User access can be configured independently for Command Shell and HTTP and FTP Servers. In the following descriptions, the HTTP interface is used as an example but they also apply to the FTP and command shell interfaces.

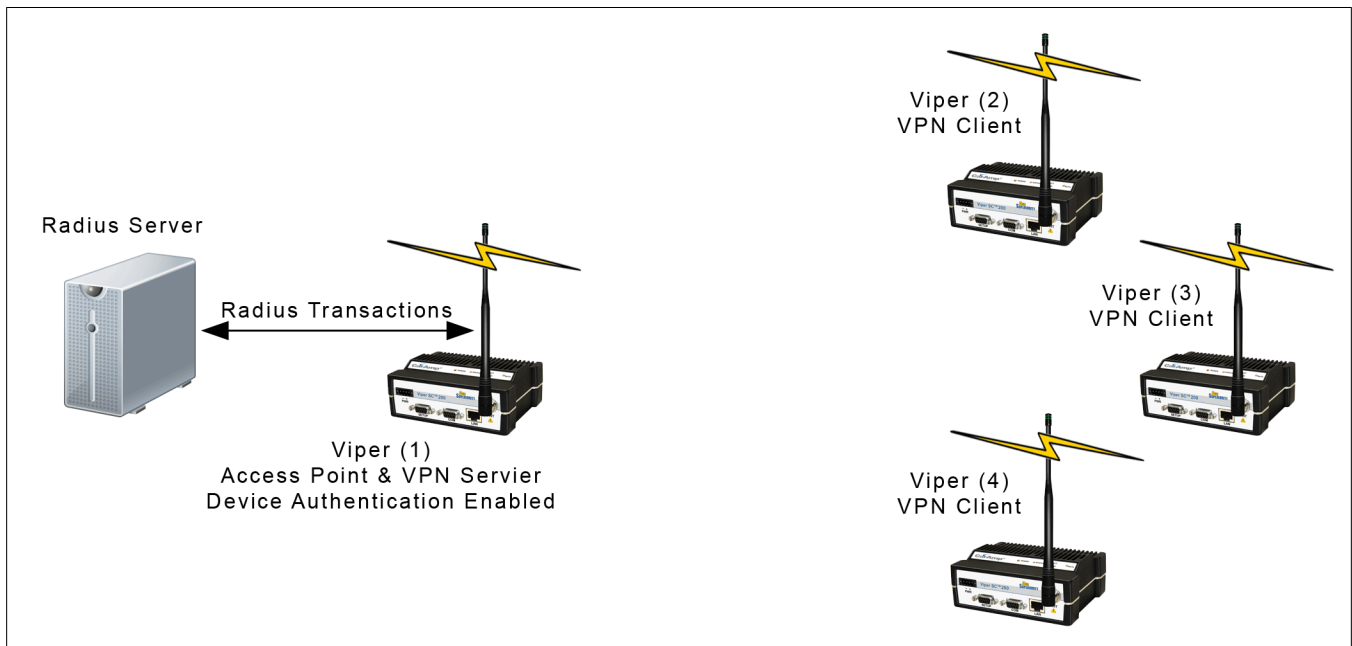
- **Local.** Authentication is done locally, i.e. within the Viper device. Example: when accessing the HTTP server, check the user credentials against username and password stored in the unit. The user will not be able to access the HTTP server unless proper credentials are provided. Local authentication is currently performed on the password only.
- **Radius & Local.** When accessing the HTTP server, check the user credentials against username and password stored in the unit. If the username and password fail to match local credentials, check for a match against the RADIUS server credential database.
- **RADIUS.** When accessing the HTTP server, check the user credentials against the RADIUS server. If the user credentials fail to match with the RADIUS server, access to the HTTP server is denied.

In order for Radius authentication to work, Client settings must be properly configured.

#### 4.5.2.1.2 DEVICE AUTHENTICATION

**Figure 52** illustrates device authentication using Radius with a Viper Network. In this example, VPN Client 2 requests a secure tunnel. The VPN server initiates a RADIUS transaction to authenticate Client 2 using its MAC address as a username and password. The tunnel is created only if the RADIUS server responds with an authentication grant.

**Figure 52 – Device Authentication**



To utilize Device Authentication, your network must use the following configuration parameters: The master device (Viper 1) must have **Device Authentication: Enabled**, and must be configured as Access Point (4.3.1) and VPN Server (Security ⇒ VPN). All remote devices (Vipers 2-4) must have **VPN Module: Enabled** and be configured as VPN Clients. (Security ⇒ VPN).

#### 4.5.2.2 CLIENT

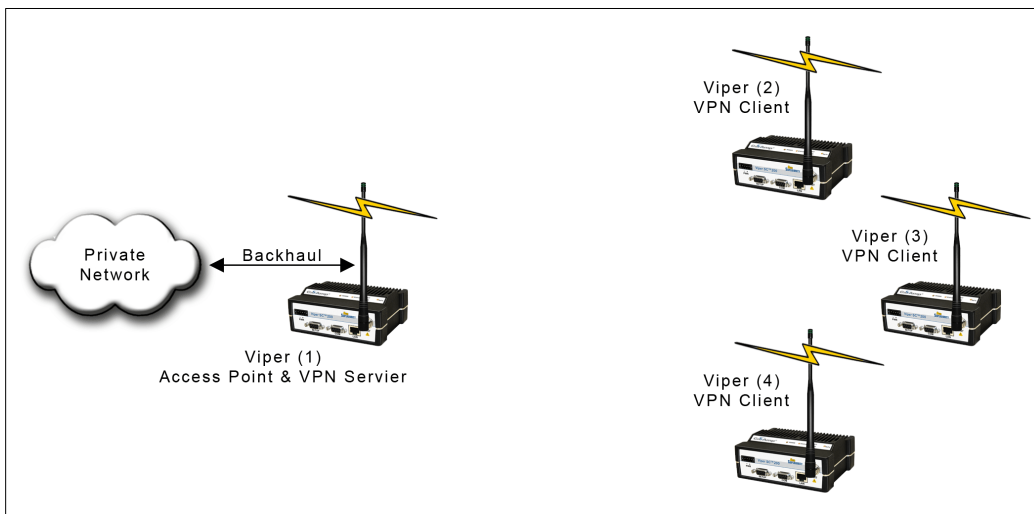
- **RADIUS Server IP.** User entered Server IP address.
- **RADIUS Server Port.** User entered port can be used but most common values are 1812 or 1645. ***These are the only values supported for RADIUS login on a non-access point device that uses the VPN feature.***
- **RADIUS Secret.** Request encryption key. The same value must be set in the RADIUS server.
- **RADIUS Timeout.** Timeout (in seconds) on the RADIUS' server reply before a new request is generated. Default = 5.
- **RADIUS Retries.** Number of retries before declaring a RADIUS fault. Default = 5.
- **Delay between retries.** Delay (in seconds) between retries. Default = 3.

### 4.5.3 VPN

From the navigation frame, select **Security → VPN (Virtual Private Network)**. A VPN provides a secure connection between two points, over an insecure network, for example, the Internet. This secure connection is called a VPN Tunnel. Viper units feature a firewall-friendly, proprietary VPN implementation optimized for radio communications. This VPN implementation uses cryptography designed for FIPS 140 certification. VPN is available in router mode only.

**Figure 53** illustrates a VPN network with one Viper programmed as a VPN server and three remotes set as VPN clients. In this example, a secure connection is established between all Viper remotes and the Access Point. Only Viper configured as an Access Point can operate as a VPN server.

**Figure 53 – Viper VPN Network**



This example can be further extended to include a relay point which allows a unit to relay data from one RF coverage area to another RF coverage area. In

**Figure 54**, Viper (3), configured as a Relay Point, must be configured as a VPN client.



Figure 54 – Viper VPN Network with Relay Point

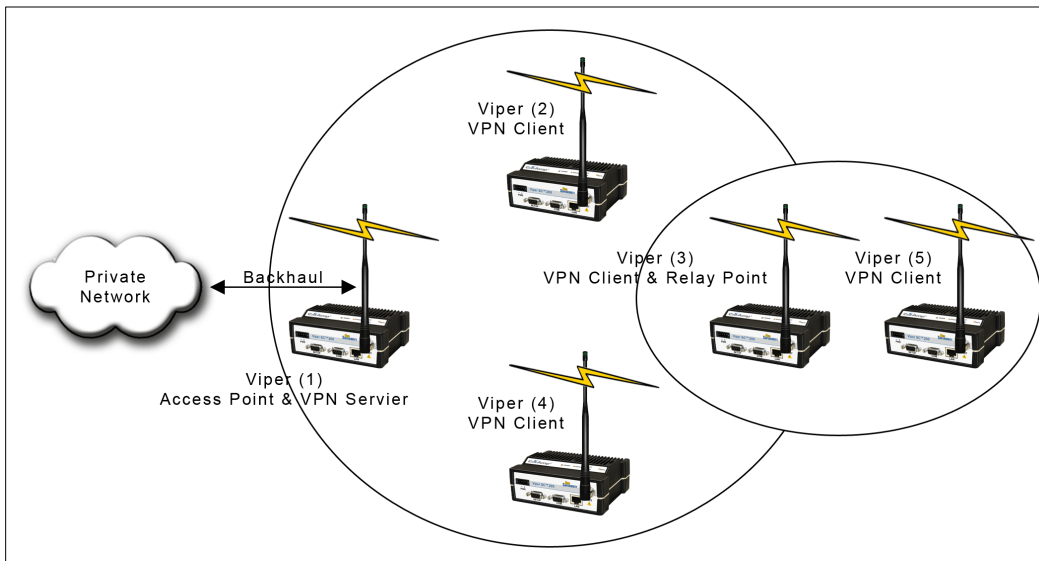


Figure 55 – Security→VPN Settings

## VPN Configuration

### Access To Settings

VPN Password	<input type="text"/>	Login
Clear VPN Password and Master Key		

### Service Control

Enable VPN	Disable VPN
Enable VPN Clients	Disable VPN Clients

### Status and Statistics

Operating mode: Server	
Status: Ready	
Number Of Tunnels	33
Tunnels Ready	31
Tunnels In Key Exchange	1
Packets Sent	516071
Packets Received	567947
Packets Received In Error	0
Refresh Clear	

#### 4.5.3.1 ACCESS TO SETTINGS

- **VPN Password.** The VPN configuration login password must be at least 8 characters long and contain at least three of the following character types: (1) uppercase letters, (2) lowercase letters, (3) numbers, and (4) special characters.
- **Key Strength.** Enter **128/192/256**. *Default = 128*. This value represents the strength (in bits) of the master key used by the VPN client and the VPN server. **Enter 128** for a Master Key that is 16 bytes (16 characters). **Enter 192** for a Master Key that is 24 bytes (24 characters). **Enter 256** for a Master Key that is 32 bytes (32 characters). This Key Strength is the same for all VPN keys. The Master Key Strength must be the same for the VPN server and all its clients.
- **Master Key.** Since hexadecimal (numeric) characters contain 8 bits (compared to binary-numeric characters which contain 7 bits) and permit the user to enter the equivalent of non-printable characters, they provide stronger security. A hexadecimal value can be entered if started with "0x". Example for a 128 bit Master Key (2+32 characters): 0x00112233445566778899aabbccddeeff. If spaces are used, the master key must be entered inside the quotation marks as shown: a\_16-byte\_string, or "a 16-byte string". The Master Key Strength and the Master Key have to be the same for a VPN server and all its clients.

#### 4.5.3.2 SERVICE CONTROL

## Enable/Disable VPN

Select **Enable VPN/Disable VPN**. Click to manually enable/disable the device's VPN service.

## Enable/Disable VPN Clients

(Available on VPN servers only)

The VPN server sends a 'VPN enable service' or 'VPN disable service' command to all of its clients when the user clicks the Enable- or Disable- VPN Clients button.

Note: The command is broadcast a few times using the 'Network Latency' VPN setting as the delay (in seconds) between each broadcast. Clicking this button again before the command-transmit sequence is completed will result in an error message.

**Warning:** VPN clients cannot process commands from the VPN server while a user is accessing the VPN configuration settings.

---

### 4.5.3.3 STATUS AND STATISTICS

- **Number of Tunnels.** VPN statistics are displayed for all tunnels. This value represents the total number of active tunnels terminating in the unit. The maximum number of key-exchanging tunnels is currently limited to 128 on a VPN server and 1 on a VPN client. A "Shared" tunnel is included in this statistic. It is used for special types of traffic such as broadcast and multicast packets. The tunnel is always keyed, so the minimum Number of Tunnels shown is 1 when VPN is enabled on the device.
- **Tunnels Ready.** Indicates the number of tunnels that are accepting traffic. Tunnels that are not ready block all traffic passing through them.
- **Tunnels in Key Exchange.** Indicates the number of tunnels in key exchange. A key-exchanging tunnel is considered to be "Not Ready".
- **Packets Sent.** Number of packets sent across all tunnels.
- **Packets Received.** Number of packets received across all tunnels
- **Packets Received in Error.** Number of packets received in error by the device from all VPN tunnels, possible causes include:
  - \* Reception of non-VPN packets when 'Block non-VPN packets' is enabled.

\* Decryption errors due to network congestion, or packet corruption. **Figure 56 – VPN Configuration**

## VPN Configuration

VPN Password and Master Key	
VPN Password	<input type="text"/> <input type="button" value="Set Password"/>
Key Strength	<input type="text" value="256"/> 128, 192, or 256 bits <input type="button" value="Set Strength"/>
Master Key	<input type="text" value="....."/> <input type="button" value="Set Key"/>
<input type="button" value="Clear VPN Password and Master Key"/>	

General Settings	
<input type="button" value="Set Server Defaults"/> <input type="button" value="Set Client Defaults"/>	
Operating Mode	<input checked="" type="radio"/> Server <input type="radio"/> Client
Automatic Start	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Server Settings	
Block non-VPN Traffic	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Status Frequency	<input type="text" value="10"/> seconds
Idle Timeout	<input type="text" value="3"/> minutes
Idle Probes	<input type="text" value="3"/>
Key Timeout	<input type="text" value="0"/> hours
Network Latency	<input type="text" value="30"/> seconds
Packet Filter Settings	
Source Filter	
IP address	<input type="text" value="0.0.0.0"/>
IP netmask	<input type="text" value="255.255.255.255"/>
Port Range	<input type="text" value="0"/> to <input type="text" value="0"/>
Destination Filter	
IP address	<input type="text" value="0.0.0.0"/>
IP netmask	<input type="text" value="255.255.255.255"/>
Port Range	<input type="text" value="0"/> to <input type="text" value="0"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

### 4.5.3.4 GENERAL SETTINGS

- **Operating Mode.** Select **Server/Client**. *Default = Client.*
- **Automatic Start.** Select **Enabled/Disabled**. *Default = Enabled.* If **enabled**, VPN service starts automatically when Viper is powered on.

### 4.5.3.5 SERVER SETTINGS

- **Block non-VPN Traffic.** Select **Enabled/Disabled**. *Default = Enabled.* If **enabled**, the VPN service blocks all packets from the RF link which were not sent via a VPN tunnel. This is especially useful to block devices not configured for VPN operation from sending packets into the corporate network.

- **Status Frequency** (Available on VPN servers only). The delay (in seconds) between server-status advertisements sent to VPN clients. An advertisement consists of a few packets sent at an interval determined by the Network Latency setting. A server's status includes its VPN service state (enabled/disabled) and load (0-100% tunnel capacity in use). A non-zero value permits VPN clients to 'discover' servers (e.g. they do not need to be pre-configured with server IP addresses). Clients that are aware of more than one server can select one based on its advertised load.

Note: Regardless of the Status Frequency setting, a VPN server always sends a status to its clients upon its VPN service changing state (becoming enabled or disabled).

Note: To minimize RF traffic, Server-status packets are broadcast over radio link; devices acting as radio-relays must therefore explicitly enable station relay mode to forward VPN server-status packets.

Default: 10 seconds

Minimum: 5 seconds (0 = disabled)





Maximum: 60 seconds

- **Idle Timeout.** *Default = 15 minutes.* **Enter 0** to disable. Enter a value to represent the number of minutes the device can go with no traffic on the tunnel before it will attempt the Idle Probe and/or Key Exchange. This value affects the time it takes for VPN clients to re-establish their tunnels after a VPN server (access point) is restarted.
- **Idle Probes.** *Default = 3.* **Enter 0** to disable. Enter a value to configure the number of Idle Probes to attempt without receiving a reply back after the Idle Timeout. An Idle Probe attempt consists of a 100 byte UDP packet that is sent or received via a VPN tunnel. If reply is received, no action is taken. If no reply is received after the specified number of attempts, the Key Exchange is started immediately. The retry frequency of each probe attempt is affected by the Network Latency setting. For a Network Latency of 10, the probe frequency is 10 seconds. Idle Probes will not be sent if the Idle Timeout is set to 0.
- **Key Timeout.** Enter a value to represent the maximum duration of VPN tunnel security keys (in hours). *Default = 6.* For security reasons, the VPN protocol requires all endpoints on the VPN network to re-key periodically. Key Exchange consists of approximately 12 (80-100) byte long TCP packets (~1 kilobyte), which may take several seconds or more when retries required. The retry frequency of each key exchange attempt is affected by the Network Latency setting. For a Network Latency of 10, the key exchange attempt frequency is 10-80 seconds.
- **Network Latency.** *Default =10.* This parameter is a multiplier factor for tuning VPN management operations, and affects the frequency of Idle Probes and Key Exchange attempts. Only change this value by small increments (1-5). Values should be larger if key exchanges do not complete (refer to the Status and Statistics **Section 4.5.3.3**). Refer to the Idle Probe and Key Timeout for the impact of Network Latency.

---

#### 4.5.3.6 CLIENT SETTINGS

When the operating mode is set to 'Client', the 'Server Settings' part of Figure 56 above is replaced with:

Client Settings	
Server IP addresses	
Server 1 	<input type="text" value="0.0.0.0"/>
Server 2 	<input type="text" value="0.0.0.0"/>
Server 3 	<input type="text" value="0.0.0.0"/>
Server 4 	<input type="text" value="0.0.0.0"/>

Enter the RF IP address of the VPN server(s). You may enter up to 4 VPN servers. The unit will attempt to establish a VPN tunnel connection with the first server on the list. If unsuccessful, it will continue down the list in a round-robin manner.

#### 4.5.3.7 VPN FILTERS

The VPN filters provide criteria used to select which packets are sent through VPN tunnels. Packets passing through VPN tunnels are protected with strong encryption. Traffic not matching these filters is discarded provided that the 'Block non-VPN Traffic' setting is enabled on the endpoints of a VPN tunnel (default). Note: If "Block non-VPN Traffic" is disabled, the traffic is forwarded in the clear.

VPN filters fields can be configured to limit the traffic going through the VPN tunnel. Depending on system requirements, they may be set automatically using the Set to Defaults button or manually as shown in the examples below.

- **Set to Defaults.** Click to set the VPN filters based on the device's current Ethernet IP configuration. Filters are set to forward all local traffic from Ethernet and the device itself via the VPN. **Set to Defaults** also changes the General VPN Settings to the default parameters.

For VPN servers, it is recommended to set the source IP address to 0.0.0.0 (disable source IP address filter) to allow stations anywhere on the core network to access to remote Vipers via the VPN.

#### Example 1

Filters	
Source IP address	<input type="text" value="172.30.51.3"/>
Source IP netmask	<input type="text" value="255.255.255.5"/>
Destination IP address	<input type="text" value="192.138.90.50"/>
Destination IP netmask	<input type="text" value="255.255.255.0"/>
Source Port	start <input type="text" value="5555"/> end <input type="text" value="6000"/>
Destination Port	start <input type="text" value="0"/> end <input type="text" value="0"/>

In this example the source netmask is 255.255.255.255 so only messages originating from the source IP address 172.30.51.3 will be passed through the VPN tunnel. The destination netmask is 255.255.255.0 so messages destined to IP addresses: 192.138.90.1-192.138.90.254 will be passed through the VPN tunnel.

The source port range is from 5555 to 6000 so only traffic from these ports will be allowed through the VPN tunnel. Destination ports 0 to 0 allow packets to be passed through the VPN tunnel to any port on 192.138.90.1 to 192.138.90.254

Both the IP and port filter information are used to select which packets are sent via the VPN tunnel.

## Example 2

Filters	
Source IP address	<input type="text" value="172.30.51.3"/>
Source IP netmask	<input type="text" value="255.255.255.0"/>
Destination IP address	<input type="text" value="0.0.0.0"/>
Destination IP netmask	<input type="text" value="255.255.255.0"/>
Source Port	start <input type="text" value="5555"/> end <input type="text" value="6000"/>
Destination Port	start <input type="text" value="0"/> end <input type="text" value="0"/>

In this example the source netmask is 255.255.255.0, so messages originating from source IP addresses: 172.30.51.1-172.30.51.254 and from ports: 5555-6000 will be passed through the VPN tunnel. All other messages will be blocked (assuming that “Block non-VPN Traffic” is enabled).

The destination IP address is 0.0.0.0 and the destination port range is 0 to 0. So messages destined to any IP address and any destination port will be passed through the VPN tunnel.

## 4.6 STATISTICS

From the navigation frame select **Statistics** to view statistics reporting the amount of traffic sent and received by each of the three interfaces. This page also reports statistics gathered from the Airlink that can indicate the quality of the RF links.

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.

**Figure 57 – Statistics**

Ethernet			
<b>LAN</b>			
RX Pkts	1428		
TX Pkts	445		
Serial			
<b>Setup</b>		<b>COM</b>	
RX Bytes	0	RX Bytes	0
TX Bytes	0	TX Bytes	0
RX Pkts	0	RX Pkts	0
TX Pkts	0	TX Pkts	0
RF			
<b>OIP Sublayer</b>		<b>Airlink Sublayer</b>	
RX Pkts	0	RX Ctrl Pkts	0
TX Pkts	1584	RX Data Pkts	0
		TX Ctrl Pkts	0
		TX Data Pkts	0
Airlink Error Detection			
Reliable Service Msg Success Count	0		
Reliable Service Msg Failure Count	0		
Total Retry Count	0		
Noise Detected Count	3164		
Rx Total "Other" Count	0		

---

#### 4.6.1 ETHERNET INTERFACE

Ethernet statistics gathered from the LAN port include:

- **RX Pkts.** 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.

---

#### 4.6.2 SERIAL INTERFACE

Serial statistics are gathered from both the Setup and COM ports. These include:

- **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.

---

#### 4.6.3 RF INTERFACE

RF statistics include those from the OIP and the Airlink sublayers.

---

##### 4.6.3.1 OIP SUBLAYER

- **RX Pkts.** The total number of input packets received by RF-OIP interface.
- **TX Pkts.** The total number of output packets transmitted by RF-OIP interface.

---

##### 4.6.3.2 AIRLINK SUBLAYER



- **RX Ctrl Pkts.** The total number of control packets received over-the-air. These packets may be RTS/CTS messages or RF Acknowledgements.
- **RX Data Pkts.** The total number of input data packets received over-the-air.
- **TX Ctrl Pkts.** The total number of output control packets transmitted over-the-air. These packets may be RTS/CTS messages or RF Acknowledgements.
- **TX Data Pkts.** The total number of output data packets transmitted over-the-air.

#### 4.6.3.2.1 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 Viper SC 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 Viper SC overheard that were intended for another station. These messages are discarded.

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

#### 4.6.3.3 STATISTICS/REMOTES

**Figure 58 – Statistics/Remotes**

This Unit 80:0D:3D									
Remote Units	Packet Type	Received Packets			Transmitted Packets			RSSI (dBm)	SNR (dB)
		Good	Failed	PER	Good	Failed	PER		
*80:18:0A	unicast	0	0	?	0	0	?	N/A	N/A
	broadcast	0	0	?	4	0	?		
80:18:07	unicast	4	0	0.00%	4	0	0.00%	-80.05	38.03
	broadcast	0	0	?	4	0	?		

**Remote Units.** The RF MAC address of a neighboring remote unit. This table is updated every time the Viper sends (or receives) data to (or from) that unit. When the RF MAC address is prefixed by an asterisk (\*), the Viper learned about this unit through a Relay Point (RP) (e.g., this unit is more than 1 RF hop away).

**Received Packets.** The number of IP packets sent by the remote unit to this unit. A packet is bad (failed) if at least one of the following is incorrect: the CRC, the length, the system identifier or it was simply not received at all by this unit (as evidenced by a gap in the packet stream sequence numbers). The receive Packet Error Rate (PER) is calculated with this formula:  $per = (bad / (bad + good)) * 100$

A PER value shows a question mark ("?") when the unit cannot compute it. This can be due to no packets being received or to the received packets not including a sequence number. The later is due to the "OIP duplicate packet removal" feature being disabled.

**Transmitted Packets.** The number of IP packets transmitted on the RF interface (good and bad packets) to the remote unit (unicast or broadcast). A packet is bad (failed) if we did not receive a notification from the remote unit of the arrival of the packet. The transmit Packet Error Rate (PER) is calculated with the this formula:  $per = (bad/(bad+good))*100$

A PER value shows a question mark ("?") when the unit cannot compute it, either due to the "RF ACK" feature being disabled on this unit or to the fact that no packet has yet been transmitted.

**RSSI.** The last Received Signal Strength Indicator (RSSI) from the given remote unit. Each time a new packet is received from the remote unit, the RSSI in this table is calculated and updated.

**SNR.** The last Signal to Noise Ratio (SNR) from the given remote unit. Each time a new packet is received from the remote unit, the SNR in this table is calculated and updated.

## 4.7 MAINTENANCE

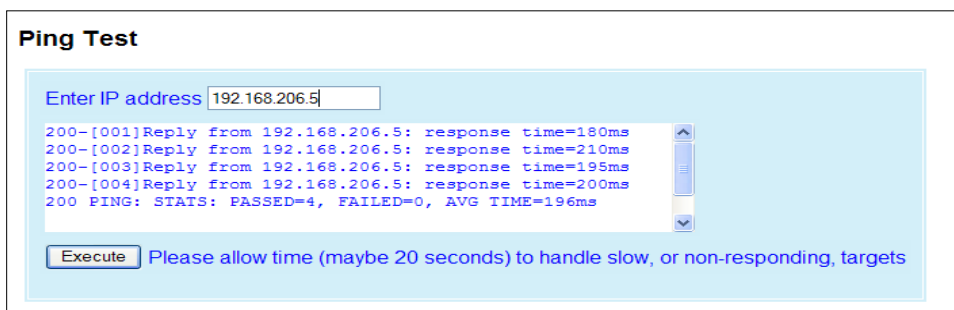
From the navigation frame, select **Maintenance** to access:

- Ping Test (see Section 4.7.1)
- Config Control (see Section 4.7.2)
- Package Control (see Section 4.7.3)
- Net Tests (see Section 4.7.4)
- RF Tests (see Section 4.7.5)
- Feature Options (see Section 4.7.7)

### 4.7.1 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. **Enter IP Address** and press **EXECUTE**. Allow up to 20 seconds to handle slow or non-responding targets.

**Figure 59 – Maintenance/Ping Test**

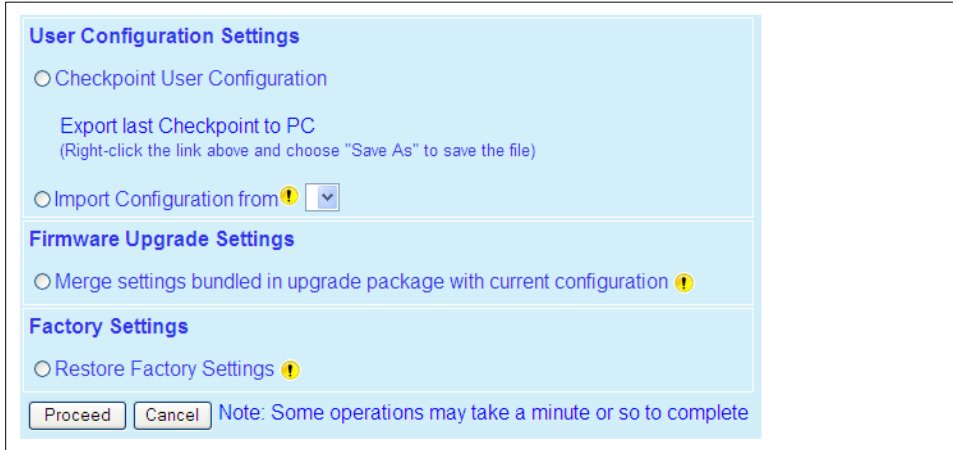


---

## 4.7.2 CONFIG CONTROL

The **Config Control** page grants access to User Configuration, Firmware Upgrade and Factory Settings.

**Figure 60 – Maintenance/Unit Configuration Control**



---

### 4.7.2.1 USER CONFIGURATION SETTINGS

Select **Checkpoint User Configuration** to create a checkpoint of all the user configurable settings in the Viper. Click **Proceed** to save these settings into the configuration file (UserCFG\_*macaddress*.drp, where *macaddress* is equal to the Ethernet MAC Address of the Viper). 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.

Additionally, portions of the Routing Table and the Neighbor Table are saved into the configuration file as described below.

#### 4.7.2.1.1 NEIGHBOR TABLE

- **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.

#### 4.7.2.1.2 ROUTING TABLE

- **Connected Route.** Not Saved. These routes point to a direct physical connection on the Ethernet port and are created dynamically based on the Viper SC'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 Viper SC 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 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 Viper SC or into another Viper SC by using an FTP client program. Do not load more than 5 separate configuration files into a single Viper SC. Loading many configuration files into a Viper SC may use up an excessive amount of memory causing the Viper to malfunction. After saving the configuration file back into the Viper SC 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 Viper SC. 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.

---

#### 4.7.2.2 FIRMWARE UPGRADE SETTINGS

- **Merge settings bundled in upgrade package with current configuration.** Select to merge upgraded settings with the current configuration. To complete the merge process, click **Proceed**, click **Save Config** and then click **Reset Unit**. The firmware upgrade process will replace the existing configuration with the firmware bundled with the upgrade package.

---

#### 4.7.2.3 FACTORY SETTINGS

Review your record of the Viper factory settings before proceeding with this command. Select to **Restore Factory Settings** to restore all settings to the default factory configuration.

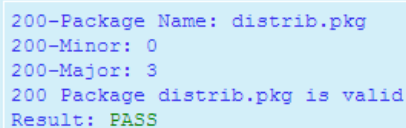
---

#### 4.7.3 PACKAGE CONTROL

Package Control is used to verify a field upgrade of the Viper 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 and/or corrupt.

The Package Validation window is for reference only.

**Figure 61 – Maintenance/Package Validation**



```
200-Package Name: distrib.pkg
200-Minor: 0
200-Major: 3
200 Package distrib.pkg is valid
Result: PASS
```

---

#### 4.7.4 NET TESTS

From the navigation frame, select **Maintenance → Net Tests** to test the reliability of the RF link. Test packets are generated and transmitted with a special test bit set in the package header to identify the packet as a test packet. The receiving Viper counts the number of test packets received successfully. Test results are viewed on the receiving Viper.

Figure 62 – Maintenance/Net Tests

Net Test Setup		
Destination RF MAC address	<input type="text" value="0xFFFFFFFF"/>	Default: 0xFFFFFFFF Range: [1 - 0x00FFFFFF]
Number of Packets To Transmit	<input type="text" value="1"/>	Default: 1
Delay Between Packets	<input type="text" value="0"/>	Default: 0 [msec]
Packet Data Pattern	<input checked="" type="radio"/> Fixed <input type="radio"/> Random	
Packet Data Type	<input checked="" type="radio"/> ASCII <input type="radio"/> Binary	
Length of Data Payload	<input type="text" value="2"/>	Default: 2 Range: [2 - 1500]
Lock PTT Between Packets	<input type="radio"/> ON <input checked="" type="radio"/> OFF	
!!! Warning !!! The test mode cannot be enabled (active) for more than 15 minutes !!!		
Test Mode	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	
<input type="button" value="Start Test"/> <input type="button" value="Stop Test"/> <input type="button" value="Show Stats"/> <input type="button" value="Clear Stats"/>		

- **Destination RF MAC address.** User entered RF MAC address of the Viper unit they wish to connect to (Format 0x0000FD4). Default = 0xFFFFFFFF) Send a broadcast packet to all Viper listening for the test packets.
  - **Number of packets to transmit.** The total number of packets transmitted during the test. Default = 1.
  - **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.** Select **Fixed/Random** Fixed data is highly compressible; random data is not; Viper SC utilizes a data compression algorithm to compress data before transmitting.
  - **Packet data type.** Select **ASCII/Binary**. Hex formats. ASCII data is highly compressible. 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 Viper SC unit.
  - **Lock PTT between packets.** If the "Off" option is chosen and enough delay has been added between packets, the Viper SC will stop transmitting between packets. If "On" is selected the Viper SC will continuously transmit between packets.
  - **Test Mode.** Select **Enable/Disable**. If Enabled, Viper listens for test packets being transmitted from a remote unit.
- Start Test/Stop Test.** Click to **start/stop** transmitting test packets. Test packets received are stored and can be used by selecting **Show Stats**. Select **Clear Stats** to clear test results.

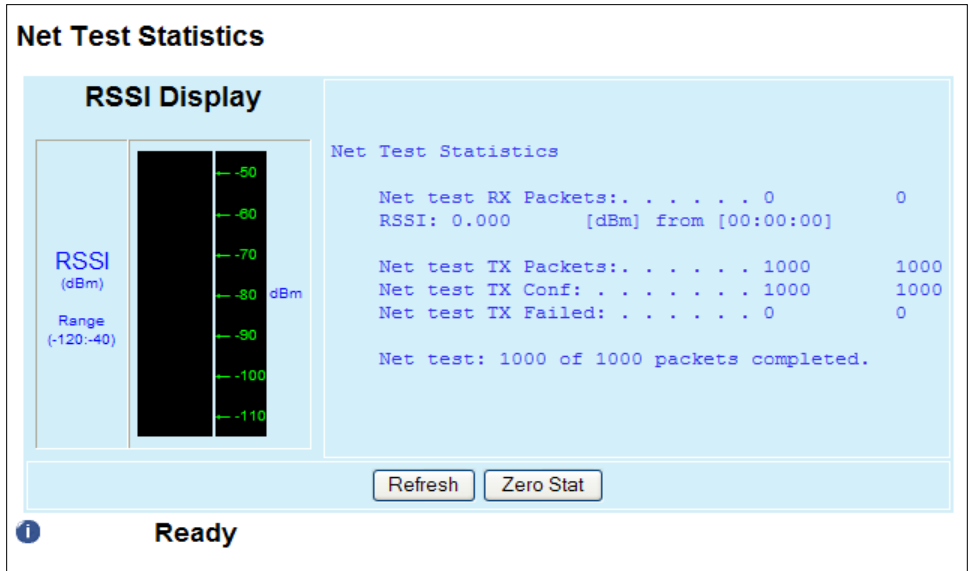
**Warning!** When Viper is in test mode, it will not respond to RF activity from other Viper units. Test mode cannot be Enabled (active) for more than 15 minutes. After 15 minutes, test mode will be automatically disabled and normal communications will resume.

Open window to display 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.

Net Test Results

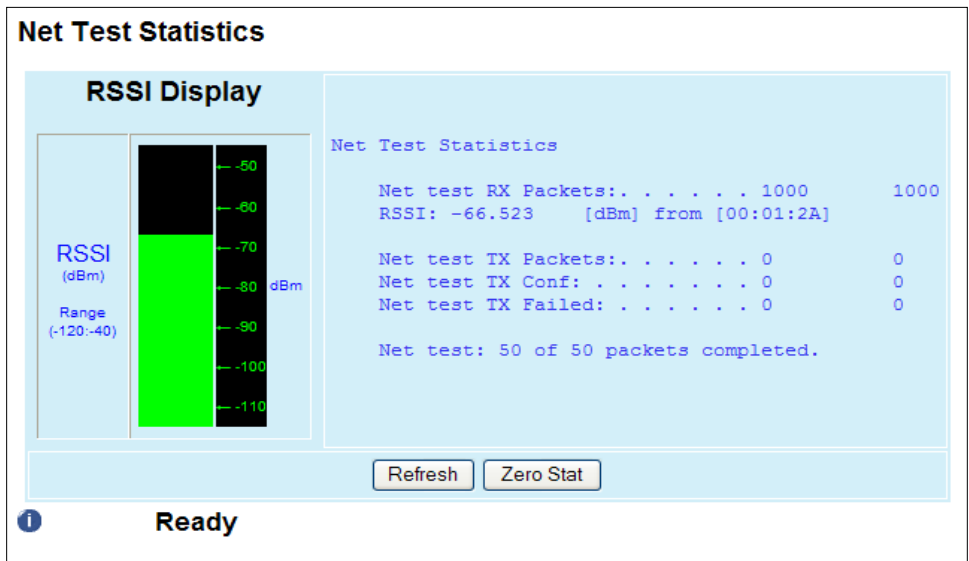
Click **Show Stats** to display the test results. A typical results page from the transmitting Viper is shown in **Figure 63**.

**Figure 63 – Net Test Statistics (From the Transmitting device)**



The left column lists current results. The right column shows results from the last time the stats were refreshed. In this example, 1000 of 1000 packets were successfully transmitted. To see how many packets were successfully received, check the stats on the receiving Viper.

**Figure 64 – Net Test Statistics (From the Receiving device)**



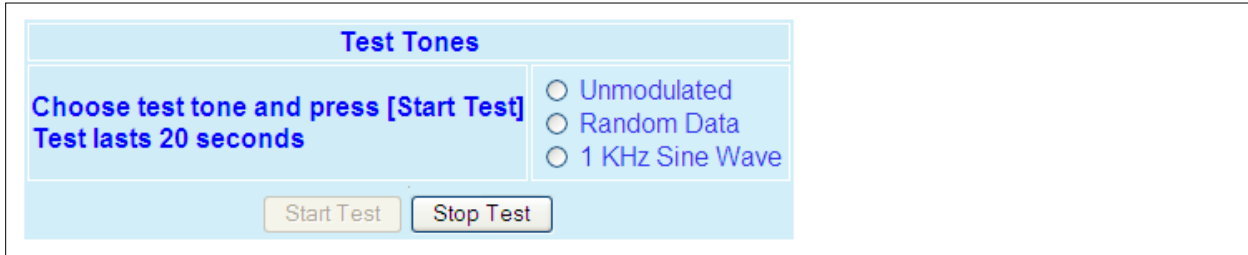
In this example, 1000 test packets were successfully received from Viper 00:01:2A with an RSSI value of -66.523 dBm.

---

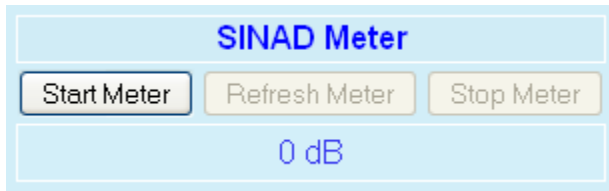
#### 4.7.5 RF TESTS

Select **Unmodulated/Random Data/1 KHz Sine Wave** to indicate the type of test tone to be transmitted. Click **Start Test** to transmit a test tone for 20 seconds. Other Viper in the network may stop transmitting for the duration of this test. Click **Stop Test** to end the test tone immediately.

**Figure 65 – Maintenance/RF Tests**



**Figure 66 – SINAD Meter**



**SINAD Meter.** Display readings from the SINAD meter. SINAD is a measure of signal degradation by unwanted or extraneous signals including noise and distortion. The higher the figure for SINAD, the better the quality of the received signal. The SINAD figure is expressed in decibels (dB) and can be determined from the simple formula:

$$\text{SINAD} = 10\text{Log} (\text{SND}/\text{ND})$$

Where:

**SND = combined Signal + Noise + Distortion power level**

**ND = combined Noise + Distortion power level**

**0dB <= SINAD < 50dB**

The receiver must be fed a 1KHz tone.

---

#### 4.7.6 WING COMMANDER

While the Viper can be upgraded (locally or over-the-air) in a one-to-one fashion using the standard FTP protocol, the CalAmp Wing Commander Protocol (WCP) allows a Wing Commander Server (WCS) to efficiently and reliably upgrade OTA (over-the-air) a field of Vipers in a one-to-many fashion, using multicast UDP/IP.

A typical upgrade scenario using the Wing Commander Protocol is as follows. The WCS splits the firmware upgrade archive into small numbered blocks, which it then multicasts to the Vipers. The WCS next polls the Viper units to assess which blocks need to be re-sent. The Viper stores the received blocks in non-volatile memory as they are received, maintaining the proper logical order even for blocks received out of order. When the WCS establishes that the prescribed number of

Vipers in the deployment have received all the blocks, it directs the Vipers to install the image received and perform a station reset. As a last step, the WCS verifies that all Vipers have successfully applied the firmware upgrade.

**Figure 67 – Maintenance → Wing Commander**

WCP Settings							
Unit ID	123456789012345						
Group ID #1	aA0#\$\$&()[]^_@						
Group ID #2	n/a						
Group ID #3	n/a						
Group ID #4	n/a						

IP Settings	
Multicast Group <span style="color: yellow;">!</span>	239.192.0.1

Queued Files							
Server	Filename	Size (bytes)	Handle	Blocks		Completed (%)	Cmd
				Total	Written		
172.28.50.200	301200.zip	1413026	7	1380	93	6	Send Block

Most of the WCP settings (intrusive or transparent packet pacing, addressing options, retries etc.) are controlled from the WCS, leaving only a few settings to be specified on the Viper unit.

The WCS can select from a rich array of addressing options to target Viper unit(s) for software upgrade. Amongst these addressing options are an arbitrary unit ID an up to four arbitrary group IDs.

Since the WCP reduces OTA traffic by using multicast IPv4 UDP/IP datagrams whenever possible, the Viper units must first be provisioned with the multicast address to use. By default, WCP uses a multicast address taken from the IPv4 Organization Local Scope Multicast Pool (from which an organization should allocate sub-ranges when defining scopes for private use). Note that while private backhalls can be configured to forward traffic to addresses in that pool, public routing fabrics will not forward multicast datagrams destined to addresses in that range. Consult your network administrator to obtain an IANA-compliant routable multicast address before using WCP across public networks.

**WCP Settings**

- Unit ID                      Unique identifier representing this unit.
- Group ID #1                Group identifier number 1 to whom this unit belongs to
- Group ID #2                Group identifier number 2 to whom this unit belongs to
- Group ID #3                Group identifier number 3 to whom this unit belongs to
- Group ID #4                Group identifier number 4 to whom this unit belongs to



Each ID is an arbitrary 15 character long case-sensitive string. The following characters are allowed:

a-z	ASCII: 0x61 – 0x7A
A-Z	ASCII: 0x41 – 0x5A
0-9	ASCII: 0x30 – 0x39
#	ASCII: 0x23
\$	ASCII: 0x24
%	ASCII: 0x25
#	ASCII: 0x23
\$	ASCII: 0x24
%	ASCII: 0x25
&	ASCII: 0x26
(	ASCII: 0x28
)	ASCII: 0x29
*	ASCII: 0x2a
-	ASCII: 0x2d
@	ASCII: 0x40
[	ASCII: 0x5b
^	ASCII: 0x5e
_	ASCII: 0x5f

The default value (“n/a”) does not result in an ID comparison match when used.

**IP Settings. Multicast Group** Multicast IP address used by the Wing Commander Protocol Server. Default value is 239.192.0.1

**Queued Files.** The Viper WCP client supports of to five (5) concurrent WCP streams. Each stream is identified by the following information:

Server

IP address of the WCP server performing the file transfer

Filename

Name of the file being downloaded. Only the rightmost 10 characters are displayed, however the Viper keeps track of the full filename.

Size (bytes)

Size of the file being downloaded, in bytes

Handle

Arbitrary handle associated to the filename with the WCP server. The server uses this handle to perform all operations related to that specific WCP stream.

### Blocks Total

The WCP server sends the filename in small blocks. This number represents the number of blocks the server divided the file into.

### Block Written

Number of blocks that have been successfully written into the Viper non-volatile memory

### Completed (%)

Completion ratio (blocks written over total number of blocks)

### Cmd

The last WCP command received by the client

**Contact your authorized CalAmp representative for availability and details on the Wing Commander Server.**

---

## 4.7.7 FEATURE OPTIONS

The Feature Option page shows the available features and shows which features are currently installed in the Viper SC.

**Table 12 – Available Feature Options**

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

## 4.8 NETWORK MANAGEMENT/NEIGHBOR TABLE

Each unit is equipped with a powerful neighbor discovery module. The purpose is to detect all units in the RF network and add all necessary IP routes required to reach neighboring units. Vipers discover other Viper by sending and receiving neighbor discovery control messages.

From the navigation frame, select **Network Management** to access Viper Neighbor Management options. This page also displays information about local status, discovered neighbors, and control operations.

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).

Neighbor discovery is only operational in router mode.

Figure 68 – Network Management→Neighbor Table

**Neighbor Discovery**

Manual-Scan
  Auto-Scan
  Disabled

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

**Local Status**

Scanning For Neighbors
**Neighboring ViPRs found** 2
**Discovery Duration** 00:00:34

**Discovered ViPR Neighbors**

Information on Neighboring ViPR				Route to Neighboring ViPR			
RF MAC Address	RF IP Address	Ethernet IP Address	RSSI <small>dBm</small>	Hop Count	Next Hop	Entry Type	Connectivity Status
00:0F:E0	10.0.15.224/8	192.168.206.2/24	-52.34	1	00:0F:E0	Dynamic	Reachable
00:0F:D8	10.0.15.216/8	192.168.207.1/24		2	00:0F:E0	Static	Reachable

**Control Operations**

#### 4.8.1 NEIGHBOR DISCOVERY

Select **Manual/Auto/Disabled**. Default = **Manual-Scan**. There are three modes of operation. This mode must be configured the same for every Viper in the network.

- **Manual-SCAN.** Viper 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 Viper SC 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. This mode is recommended for most projects.
  
- **Auto-SCAN.** Viper begins "Scanning for Neighbors". In the "Scanning for Neighbors" state, Viper discovers other Viper units in the network and other Viper SC units learn about the Viper SC initiating the scan. Viper goes from "Scanning for Neighbors" state to "Ready" state when it doesn't discover another Viper SC for a given amount of time. In "Ready" state, Viper SC will generate a "keep alive" packet periodically. In "Ready" state, Viper SC performs broken link detection. Viper SC is monitoring the "keep alive" packets of other Viper SCs (1 hop away). Viper SC knows the interval period for other Viper SCs generating their "keep alive" packets. If Viper SC (A) fails to receive four "keep alive" packets in a row from Viper SC (B), Viper SC (A) removes Viper SC (B) from its neighbor table and goes into the "Scanning for Neighbors" state. If a user presses the "Force Scan" button, Viper SC goes into the "Scanning for Neighbors" state. If other Viper SCs are in the "Scanning for Neighbors" state, Viper SC 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 Viper SC

network. Auto-Scan mode could generate a large number of neighbor discovery control messages in a large Viper SC network. CalAmp recommends Auto-Scan be limited to Viper SC networks of two to ten units. If Auto-Scan mode is used, be aware that 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.

- **Disabled.** In the disabled state, Viper does not send neighbor discovery packets nor does it process neighbor discovery packets generated by other Vipers. The user can enter static entries in the Neighbor Table. Disabled is recommended in projects where the customer does not want RF paths to deviate from RF engineered, or site survey completed paths.

---

#### 4.8.1.1 LOCAL STATUS

Discovery Mode represents the mode of operation of the remote device. There are five states of operations reported in the local status display: Ready, Scanning for Neighbors, Disabled, Saving Neighbor Table, and Testing Connectivity.

- **Ready.** The neighbor discovery module is in a “Ready” state when it is not scanning for other units. If the Viper SC is operating in Manual-Scan, it does nothing. If the Viper SC 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 Viper SC 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 Viper SC 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.

Local Status also reports the number of **Neighboring Vipers Found** and the **Discovery Duration**, which is the time it took for the Viper unit to complete the neighbor discovery learning process.

---

#### 4.8.1.2 DISCOVERED VIPER NEIGHBORS

Each entry in the Table represents a remote Viper. The table displays information about the remote device and information about the route to each remote device.

##### 4.8.1.2.1 INFORMATION ON NEIGHBORING VIPER

---

- **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.

#### 4.8.1.2.2 ROUTE TO NEIGHBORING VIPER

- **Hop Count/Next Hop.** Indicates the route the remote Viper SC 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 through another Viper SC as identified by the Next Hop field.

#### 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.

#### 4.8.1.3 CONTROL OPERATIONS

- **Clear List.** Select to clear 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 Viper in the list to ensure an RF path between the units.
- **Add Static Entry.** Click to open a popup window where the user can add a new static neighbor entry. To create the new neighbor, completely fill in all the information. The requested fields are described below. Finally, the user must press **Apply** and **Save Config** 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.
- **Delete Entry.**

Add static neighbor entry			
RF MAC Address	<input type="text" value="80:01:0A"/>		
RF IP Address	<input type="text" value="10.128.1.10"/>	RF netmask	<input type="text" value="255.0.0.0"/>
Ethernet IP Address	<input type="text" value="192.168.206.1"/>	Ethernet netmask	<input type="text" value="255.255.255.0"/>
Hop Count	<input type="text" value="1"/>		
Next Hop	<input type="text" value="80:01:0A"/>		
Description	<input type="text" value="ViPR #2"/>		
Attributes	<input type="checkbox"/> Access Point <input type="checkbox"/> Relay Point <input type="checkbox"/> TCP Proxy <input type="checkbox"/> NAT		
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

- **RF MAC Address.** Default = the last six digits of the Ethernet MAC that is found on the label on the bottom of your Viper. Also you can verify the current RF MAC that is being used in the remote radio by checking the Basic Setup ⇒ IP Settings web page of the remote unit. Enter the current RF MAC address of the remote radio into this field.
- **RF IP address, RF netmask, Ethernet IP Address, and Ethernet netmask** of the remote Viper. These can all be obtained from the Basic Setup → IP Settings web page of the remote Viper.
- **Hop Count.** Enter the number of RF hops required to reach the remote Viper SC.
- **Next Hop.** Enter the RF MAC address of the next Viper SC that data packets must first go to before being repeated on to the remote Viper SC. If the Viper SC you are adding is only one hop away, enter the RF MAC address of the Viper SC you are adding. If you are setting up a system with multiple hops (with relay/repeater points), you must first enter remote Viper SCs into the neighbor table that are 1 hop away before adding Viper SCs that are 2 or more hops away. This insures that the Viper SC will recognize the RF MAC address of the “Next Hop” Viper SC as you setup routes to Viper SCs that are 2 or more hops away.
- **Description.** Enter the Station Name of the remote Viper SC. 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 Viper SC has enabled: Access Point, Relay Point, TCP Proxy, and/or NAT (Network Address Translation).

NOTES:

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

---

#### 4.8.1.4 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 Viper SC’s Routing Table when entries are added or deleted from the Neighbor Table.

---

#### 4.8.1.5 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.

<b>Description</b>	Sedna 2
<b>RF MAC Address</b>	00:01:B8
<b>RF IP Address</b>	10.0.1.185/8
<b>Ethernet IP Address</b>	172.31.19.100/16
<b>Attributes</b>	N/A
<b>Discovery Mode</b>	Automatic
<b>Primary Route</b>	
Hop Count	<input type="text" value="1"/> Next Hop <input type="text" value="00:01:B8"/> (Active)
<b>Backup Route</b>	
Hop Count	<input type="text" value="2"/> Next Hop <input type="text" value="00:01:01"/> (Inactive)
<input type="button" value="Toggle Primary/Backup Routes"/> <input type="button" value="Apply"/>	

The Neighbor Discovery module will keep track of two routes determined by the shortest hop count to any given Viper SC - 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 Viper SC #1 to Viper SC #3 goes through Viper SC #2. The route selected must be edited in Viper SC #1 and Viper SC #3. The routing path must use the same Viper SCs 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.***

## 4.8.2 STATUS

Figure 69 – Network Management → Status

Network Status			
RF-MAC Address	Station Status	ND Mode	Command Status
No command in progress			
<input type="button" value="Refresh"/>			

## 4.8.3 MAINTENANCE

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

Figure 70 – Network Management → Maintenance

<input type="radio"/> Delete Station	RF-MAC Address <input type="text"/>	<input type="checkbox"/> Save Configuration After Remote Operation	
<input type="radio"/> Replace Station	Old RF-MAC Address <input type="text"/>	New RF-MAC Address <input type="text"/>	<input type="checkbox"/> Save Configuration After Remote Operation
<input type="radio"/> Change ND mode	<input type="radio"/> Manual-Scan <input type="radio"/> Auto-Scan <input type="radio"/> Disabled	<input type="checkbox"/> Save Configuration After Remote Operation	
<input type="radio"/> Save Configuration			
<input type="radio"/> Get Status			
	<input type="checkbox"/> Single Station <input type="text"/>		
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

- **Delete Station.** User entered RF MAC Address of the station to be deleted from the Neighbor Table of all Viper SCs in the network.
- **Replace Station.** User entered RF MAC Address of the Viper to be replaced and the new RF MAC Address (that will replace the old Viper SC). This will update the Neighbor Table of all Viper in the network.
- **Change ND mode.** Select to change the Neighbor Discovery mode of all Viper in the network to Manual-Scan, Auto-Scan, or Disable. Refer to **Section 4.8.1** for a description of Neighbor Discovery modes.
- **Save Configuration.** Click to send a save configuration command to all Viper in the network.
- **Get Status.** Click to send a command to all Vipers in the network. Command results are displayed on the Network Management → Status page.
- **Single Station.** Check to enter the single RF MAC Address of the Viper SC module commands will be sent to. If this option is selected, the command will be sent to an individual Viper SC instead of being sent to all Viper SCs in the Network.



## 5 NETWORK OPTIMIZATION

### 5.1 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. Viper SC 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 Viper SC 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.

### 5.2 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.

#### 5.2.1 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 Viper units, but is well worth the increase in link stability over the simple Bridge mode.

RF Acknowledgements can be enabled on Viper web pages under Setup (Advanced) ⇒ IP Optimization. RF Acknowledgements must be enabled or disabled on all Vipers in the network.

Vipers 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.

#### 5.2.2 REDUCE RF NETWORK BIT RATE

Viper has up to four speeds of operation available for each of the four channel bandwidths. The fastest speeds utilize 16-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. When the received RF signal level is strong, the system is able to utilize the faster bit rates. However, if the system has a low RF signal level or the RF signal levels are close to an elevated noise floor level, you can run at a slower over-the-air speed for the system's bandwidth. It may result in better overall performance.

---

### 5.2.3 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 Viper's web pages under Setup (Advanced) ⇒ RF Optimizations. The number of OIP retries can be configured under Setup (Advanced) ⇒ IP Optimization.

## 6 UPGRADING YOUR FIRMWARE

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

There are two sets of code in the Viper SC Radio. The first set of code is the Modem Firmware and must be updated every time a software upgrade is needed. The second set of code is the Radio Firmware. This firmware resides on the Viper SC 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 Viper SC. Do this by following the steps outlined in section 6.1. The Modem Firmware package will contain the new Radio Firmware file (Viper SC\_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 Viper SC's CLI (command line interface) and executing the upgrade command as outlined in section 6.2.

### 6.1 UPGRADE PROCEDURE (MODEM)

#### **WARNING:**

**Firmware version 3.0 and greater must NOT be loaded into Viper SC units currently running V1.x firmware. The Viper SC will not boot and will be unrecoverable due to higher memory usage requirements of the added features. To verify your current firmware version, navigate to Unit Identification and Status webpage.**

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 Viper SC files. Failure to follow the recommended procedure as detailed above may result in unit becoming unresponsive.
4. Once the file transfer is complete, cycle power and allow the unit to boot. The Viper SC should return to its pre-update state. 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.

### 6.2 UPGRADE PROCEDURE (RADIO)

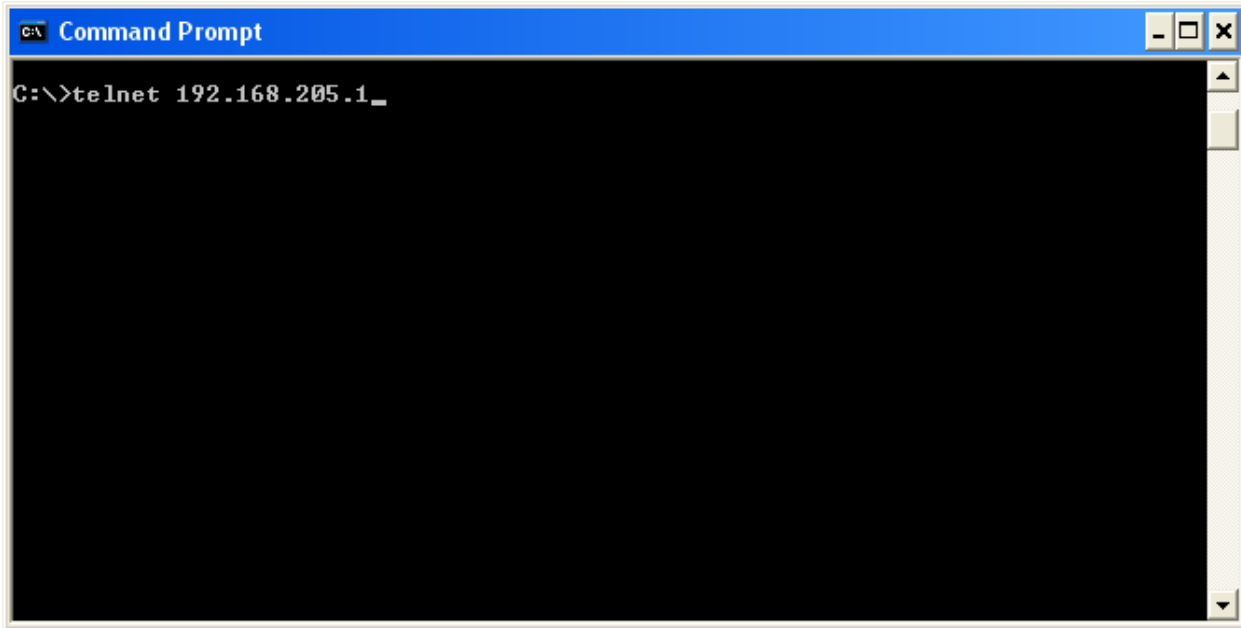
If the radio firmware revision has been upgraded in the new package, follow these steps to complete the upgrade process.

1. First upgrade the Viper SC Modem Firmware as outlined in section 6.1
2. Telnet into the Viper SC 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 Viper\_SC\_ip\_address*

**Figure 71 – Use Windows Command Prompt to Telnet to Viper SC 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: . . . . Nov 05 2009  
200-Build Time: . . . . 07:47:45  
200-Copyright:. . . . Copyright 2008 DRL
```

200-Firmware Version: . FIRM-03\_10-R  
200-ASD Data Map: . . . 2.0  
200-Radio Circuit Board: 0.10  
200-Radio Serial Number: 405163  
200 Radio Model Number: 823-5028-452

Check that the “Firmware Version:” shows the latest firmware revision.

Figure 72 – Using Windows Command Prompt to upgrade Radio Firmware

pre>
C:\> Telnet 192.168.206.1
Login: username
Password: \*\*\*\*\*
200 Login successful

>radio.upload.firmware.binary -v -f vipr\_radio.bin
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

>radio.version
200-Radio Information
200-Build Date: . . . . Nov 05 2009
200-Build Time: . . . . 07:47:45
200-Copyright: . . . . Copyright 2008 DRL
200-Firmware Version: . FIRM-03\_10-R
200-ASD Data Map: . . . . 2.0
200-Radio Circuit Board: 0.10
200-Radio Serial Number: 405163
200 Radio Model Number: 823-5028-452

>\_

5. Restart the Viper SC. You can restart the Viper SC by typing “stationreset” in the CLI then pressing enter.

### 6.3 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.**

## APPENDIX A – SPECIFICATIONS

These specifications are typical and subject to change without notice.

GENERAL				
	Model Numbers	Frequency Range	Channel Bandwidths Available	
Model Numbers, Frequency Range and Bandwidth	140-5018-502	136 – 174 MHz	6.25 kHz, 12.5 kHz, 25 kHz, 50 kHz	
	140-5018-600	136 – 174 MHz	6.25 kHz, 12.5 kHz, 25 kHz, 50 kHz	
	140-5028-502	215 – 240 MHz	6.25 kHz, 12.5 kHz, 25 kHz, 50 kHz	
	140-5028-504	215 – 240 MHz	6.25 kHz, 12.5 kHz, 25 kHz, 50 kHz, 100kHz	
	140-5048-302	406.125 – 470.000 MHz,	6.25 kHz, 12.5 kHz, 25 kHz, 50 kHz	
	140-5048-400	406.125 – 470.000 MHz,	12.5kHz, 25kHz (ETSI, AS/NZ)	
	140-5048-502	450.000 - 511.975 MHz	6.25 kHz, 12.5 kHz, 25 kHz, 50 kHz	
	140-5048-600	450.000 - 511.975 MHz	12.5kHz, 25kHz (ETSI, AS/NZ)	
	140-5098-304	880 – 902 MHz	12.5 kHz, 25 kHz, 50 kHz, 100 kHz	
	140-5098-502	928 – 960 MHz	12.5 kHz, 25 kHz, 50 kHz	
140-5098-504	928 – 960 MHz	12.5 kHz, 25 kHz, 50 kHz, 100 kHz		
Frequency Stability	1.0 ppm			
Modes of Operation	Simplex, Half-Duplex			
Frequency Increment	1.25 kHz			
Power Source	VDC, Negative GND The Viper is UL approved when powered with a listed Class 2 power supply.			
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) 450 mA (typ)	270 mA (max) 240 mA (typ)	190 mA (max) 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) 3.6 A (typ)	2.5 A (max) 1.8 A (typ)	1.6 A (max) 1.2 A (typ)
	30 dBm (1W)	1.6 A (max) 1.2 A (typ)	0.8 A (max) 0.6 A (typ)	0.6 A (max) 0.4 A (typ)
Cold start	35 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 142-174 MHz 215 – 240 MHz	406.125 – 470.000 MHz, 450.000 - 511.975 MHz	880 - 902 MHz 928 - 960 MHz
Carrier Output Power	1-10 Watts Adjustable	1-10 Watts Adjustable	1-8 Watts Adjustable
Duty Cycle	100% (Power Foldback Allowed for High Temperatures)		
Radiated Spurious Emissions	Per FCC/Regulatory		
Conducted Spurious Emissions	Per FCC/Regulatory		
Transmitter Stability into VSWR:	> 10:1 (Power Foldback Allowed)		
RX to TX Time	< 2 ms 4 ms (ETSI Versions)		
Channel Switching Time	< 15 ms (Band-End to Band-End)		



RECEIVER						
	Bandwidth Bit Rate	140-5018-50x	140-5028-50x	140-5048-30x 140-5048-50x	140-5098-x0x	Units
RX Frequencies		136 - 174	215 - 240	406.125 – 470.000 450.000 - 511.975	880 – 902 928 - 960	MHz MHz
Data Sensitivity @ 10 <sup>-6</sup> Bit Error Rate (BER)  Typical / Max	<b>6.25 kHz</b>					
	4 kbps	-115 / -112	-115 / -112	-115 / -112	--	dBm
	8 kbps	-106 / -103	-106 / -103	-106 / -103	--	dBm
	12 kbps	-100 / -95	-100 / -95	--	--	dBm
	<b>12.5 kHz</b>					
	8 kbps	-116 / -114	-116 / -114	-116 / -114	-112 / -109	dBm
	16 kbps	-109 / -106	-109 / -106	-109 / -106	-106 / -103	dBm
	24 kbps	-102 / -98	-102 / -98	-102 / -98	-99 / -95	dBm
	32 kbps	-95 / -91	-95 / -91	-95 / -91	-90 / -86	dBm
	<b>25 kHz</b>					
	16 kbps	-114 / -111	-114 / -111	-114 / -111	-111 / -108	dBm
	32 kbps	-106 / -103	-106 / -103	-106 / -103	-104 / -101	dBm
	48 kbps	-100 / -96	-100 / -96	-100 / -96	-97 / -93	dBm
	64 kbps	-92 / -88	-92 / -88	-92 / -88	-89 / -85	dBm
	<b>50 kHz</b>					
	32kbps	-111 / -108	-111 / -108	-111 / -108	-108 / -105	dBm
	64 kbps	-104 / -101	-104 / -101	-104 / -101	-101 / -98	dBm
	96 kbps	-97 / -94	-97 / -94	-97 / -94	-94 / -91	dBm
	128 kbps	-88 / -85	-88 / -85	-88 / -85	-85 / -82	dBm
	<b>100 kHz</b>					
32kbps		-111 / -108	-111 / -108	-108 / -105	dBm	
64 kbps		-104 / -101	-104 / -101	-101 / -98	dBm	
96 kbps		-97 / -94	-97 / -94	-94 / -91	dBm	
128 kbps		-88 / -85	-88 / -85	-85 / -82	dBm	
256 kbps		82 / -79		-79 / -76	dBm	

	<b>Bandwidth</b> Bit Rate	<b>140-5018-60x</b>		<b>140-5048-40x</b> <b>140-5048-60x</b>		
RX Frequencies		142 - 174		406.125 – 470.000 450.000 - 511.975		MHz MHz
ETSI Mode Useable Sensitivity @ 10 <sup>-2</sup> Bit Error Rate (BER)  Typical / <b>Max</b>	<b>12.5 kHz (ETSI)</b> 8 kbps 16 kbps 24 kbps	-111 / <b>-108</b> -104 / <b>-101</b> -96 / <b>-92</b>		-111 / <b>-108</b> -104 / <b>-101</b> -96 / <b>-92</b>		dBm dBm dBm
	<b>25kHz (ETSI)</b> 16 kbps 32 kbps 48kbps	-110 / <b>-107</b> -103 / <b>-100</b> -96 / <b>-92</b>		-110 / <b>-107</b> -103 / <b>-100</b> -96 / <b>-92</b>		dBm dBm dBm
Adjacent Channel Rejection (min)	6.25 kHz	45	45	45	--	dB
	12.5 kHz	60	60	60	60	dB
	25 kHz	70	70	70	70	dB
	50 kHz	75	75	75	75	dB
Spurious Response Rejection	All	> 75 dB				dB
Intermodulation Rejection	All	> 75 dB				dB
TX to RX Time	All	< 1 ms 5 ms (ETSI Versions)				ms
Channel Switching Time	All	< 15ms (Band-End to Band-End)				ms
Receive Input Power	All	17 dBm (50mW) max.				dBm

<b>Connectors</b>		
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	<b>Power Header</b>	<b>Power Plug</b>
	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

MODEM/LOGIC							
	Model	6.25 kHz	12.5 kHz	25 kHz	50 kHz	100 kHz	
Data Rate (Selectable)	<b>Viper 100</b> 140-5018-500 140-5018-501 <b>Viper 400</b> 140-5048-300 140-5048-301 140-5048-500 140-5048-501	4 kbps 8 kbps	8 kbps 16 kbps	16 kbps 32 kbps			
	<b>Viper 900</b> 140-5098-500 140-5098-501		8 kbps 16 kbps	16 kbps 32 kbps			
	<b>Viper SC 100</b> 140-5018-502 140-5018-503 <b>Viper SC 200</b> 140-5028-502 140-5028-503	4 kbps 8 kbps 12 kbps	8 kbps 16 kbps 24 kbps 32 kbps	16 kbps 32 kbps 48 kbps 64 kbps	32 kbps 64 kbps 96 kbps 128 kbps		
	<b>Viper SC+ 200</b> 140-5028-504	4 kbps 8 kbps 12 kbps	8 kbps 16 kbps 24 kbps 32 kbps	16 kbps 32 kbps 48 kbps 64 kbps	32 kbps 64 kbps 96 kbps 128 kbps	64 kbps 96 kbps 128 kbps 256 kbps	
	<b>Viper SC 400</b> 140-5048-302 140-5048-303 140-5048-502 140-5048-503	4 kbps 8 kbps	8 kbps 16 kbps 24 kbps 32 kbps	16 kbps 32 kbps 48 kbps 64 kbps	32 kbps 64 kbps 96 kbps 128 kbps		
	<b>Viper SC 900</b> 140-5098-502 140-5098-503		8 kbps 16 kbps 24 kbps 32 kbps	16 kbps 32 kbps 48 kbps 64 kbps	32 kbps 64 kbps 96 kbps 128 kbps		
	<b>Viper SC+ 900</b> 140-5098-304 140-5098-504		8 kbps 16 kbps 24 kbps 32 kbps	16 kbps 32 kbps 48 kbps 64 kbps	32 kbps 64 kbps 96 kbps 128 kbps	64 kbps 96 kbps 128 kbps 256 kbps	
	<b>Viper SC 100 (ETSI AS/NZ)</b> 140-5018-600 140-5018-601 <b>Viper SC 400 (ETSI AS/NZ)</b> 140-5048-400 140-5048-401 140-5048-600 140-5048-601		8 kbps 16 kbps 24 kbps	16 kbps 32 kbps 48 kbps			
	Modulation Type	2FSK, 4FSK, 8FSK, 16FSK					
	Addressing	IP					

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

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

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

## APPENDIX B – REGULATORY CERTIFICATIONS

Domestic and International Certifications					
Model Number	Frequency Range	FCC	IC (DOC)	European Union EN 300 113	Australia/New Zealand
140-5018-500 140-5018-501 140-5018-502 140-5018-503	136 – 174 MHz	NP4-5018-500	773B-5018500		
140-5018-600 140-5018-601	142 – 174 MHz			<b>CE1588</b> ⓘ	ACMA AS/NZS 4925-2004 (Spectrum Impact Assessment)
140-5028-502 140-5028-503	215 – 240 MHz	NP4-5028-502	773B-5028502		
140-5028-504	215 – 240 MHz	NP45028504	773B-5028504		
140-5048-300 140-5048-301 140-5048-302 140-5048-303	406.1 - 470 MHz	NP4-5048-300	773B-5048300		
140-5048-400 140-5048-401	406.1 - 470 MHz			<b>CE1588</b> ⓘ	ACMA AS/NZS 4925-2004 (Spectrum Impact Assessment)
140-5048-500 140-5048-501 140-5048-502 140-5048-503	450 - 512 MHz	NP4-5048-300	773B-5048300		
140-5048-600 140-5048-601	450 - 512 MHz			<b>CE1588</b> ⓘ	ACMA AS/NZS 4925-2004 (Spectrum Impact Assessment)
140-5098-304	880 - 902 MHz	NP45098304	773B-5098304		
140-5098-500 140-5098-501 140-5098-502 140-5098-503	928 - 960 MHz	NP4-5098-500	773B-5098500		
140-5098-504	928 - 960 MHz	NP45098504	773B-5098504		
UL Certification	All models UL approved when powered with a listed Class 2 source. This device is suitable for use in Class I, Division 2, Groups A, B, C, and D or non-hazardous locations only.				
Installation	This device is intended for installation only in a RESTRICTED ACCESS LOCATION per EN60950-1:2006.				

## DECLARATION OF CONFORMITY FOR MODELS # 140-5018-60x, 140-5048-40x, and 140-5048-60x

The Viper radio is tested to and conforms with the essential requirements for protection of health and the safety of the user and any other person and Electromagnetic Compatibility, as included in following standards:














Standard	Issue Date
EN 60950-1	2006 (with Amendment A11: 2009 + A1: 2010)
EN 301 489-1	2008-04
EN 301 489-5	2002-08









and is tested to and conforms with the essential radio test suites so that it effectively uses the frequency spectrum allocated to terrestrial/space radio communication and orbital resources so to as to avoid harmful interference, as included in following standards:

Standard	Issue Date
EN 300 113-1/-2	2009-11

and therefore complies with the essential requirements and provisions of the **Directive 1999/5/EC** of the European Parliament and of the council of March 9, 1999 on Radio equipment and Telecommunications Terminal Equipment and the mutual recognition of their conformity and with the provisions of Annex IV (Conformity Assessment procedure referred to in article 10).

This device is a data transceiver intended for commercial and industrial use in all EU and EFTA member states.

 Český [Czech]	CalAmp tímto prohlašuje, že tento rádio je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
 Dansk [Danish]	Undertegnede CalAmp erklærer herved, at følgende udstyr radio overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
 Deutsch [German]	Hiermit erkläre CalAmp, dass sich das Gerät radio in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
 Eesti [Estonian]	Käesolevaga kinnitab CalAmp seadme raadio vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
 English	Hereby, CalAmp, declares that this radio is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
 Español [Spanish]	Por medio de la presente CalAmp declara que el radio cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
 Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ CalAmp ΔΗΛΩΝΕΙ ΟΤΙ ΡΑΔΙΟΦΩΝΟ ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
 Français [French]	Par la présente CalAmp déclare que l'appareil radio est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
 Italiano [Italian]	Con la presente CalAmp dichiara che questo radio è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
 Latviski [Latvian]	Ar šo CalAmp deklarē, ka radio atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
 Lietuvių [Lithuanian]	Šiuo CalAmp deklaruoja, kad šis radijo atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
 Nederlands [Dutch]	Hierbij verklaart CalAmp dat het toestel radio in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
 Malti [Maltese]	Hawnhekk, CalAmp, jiddikjara li dan tar-radju jikkonforma mal-ħtiġijiet essenzjali u ma

	provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
 Magyar [Hungarian]	Alulírott, CalAmp nyilatkozom, hogy a rádió megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
 Polski [Polish]	Niniejszym CalAmp oświadcza, że radio jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
 Português [Portuguese]	CalAmp declara que este rádio está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
 Slovensko [Slovenian]	CalAmp izjavlja, da je ta radio v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
 Slovenský [Slovak]	CalAmp týmto vyhlasuje, že rádio spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
 Suomi [Finnish]	CalAmp vakuuttaa täten että radio tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
 Svenska [Swedish]	Härmed intygar CalAmp att denna radio står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Íslenska [Icelandic]	Hér með lýsir CalAmp yfir því að útlit er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
 Norsk [Norwegian]	CalAmp erklærer herved at utstyret radio er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

#### EU and EFTA Member States' Acceptable Frequency Table

Country	Acceptable Frequencies	Prohibited Frequencies
<b>Belgium</b>	146-174, 406.1-430 or 440-470 450-470	470-512
<b>Bulgaria</b>	None	All
<b>Denmark</b>	406.125-470, 450-511.975	136-174
<b>Estonia</b>	None	All
<b>France</b>	Contact Authority	Contact Authority
<b>Germany</b>	Contact Authority	Contact Authority
<b>Greece</b>	142-174 421-449	406.1250-420 450-511.975
<b>Hungary</b>	142-174 406.125-470 450-511.975	Contact Authority
<b>Italy</b>	142-174	Contact Authority
<b>Latvia</b>	142-174 406.125-470	450-470 470-511.975
<b>Lithuania</b>	406.125-430 440-470	136-146 430-440 470-512
<b>Luxembourg</b>	146-156.5125 156.5375-156.7625 156.8375-169.4 169.825-174 406.1-430 440-470	142-145 431-439 471-511.975

<b>Malta</b>	Contact Authority	Contact Authority
<b>Slovak Republic</b>	146-174 410-448	142-145 406.25-409, 449-470 450-511.975
<b>Slovenia</b>	146-174 401.6-410, 440-470 450-470	142-145 411-439 471-511.975
<b>Spain</b>	147-174 406.1-470	430-440
<b>All other EU and EFTA Member States</b>	142-174 406.125 – 512	

The countries not listed above did not reply to the notification, which means the country authority did not have any question or problem with the notification information, however it will still be necessary to obtain a license and/or authorization from the appropriate country authority, and to operate the device in accordance with the frequency, power and other conditions set forth in the authorization.



## APPENDIX C – PRODUCT WARRANTY

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, one (1) year 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 IS 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

THIRTY DAY. Tuning and adjustment of telemetry radios  
NO WARRANTY: Fuses, lamps and other expendable parts

Effective 1/2008

## APPENDIX D – DEFINITIONS

**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 Viper SC 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

**RADIUS (Remote Authentication Dial In User Service).** A networking protocol that provides centralized authentication, authorization, and accounting management for computers to connect and use a network service

**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

**SNMP (Simple Network Management Protocol).** A protocol used by network management systems to manage and monitor network-attached devices.

**SNTP (Simple Network Time Protocol).** A 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

**VPN (Virtual Private Network).** A computer network that uses a public network (example: the Internet) to transmit private data. VPN users can exchange data as if inside an internal network even if they are not directly interconnected.