VIPER SC+™

Intelligent IP Router for Licensed Spectrum

USER MANUAL

NextGen
RF DESIGN

NEXTGENRF.COM

Revision History

Rev	Date	Revision Details
0	January 2008	Initial release as 001-5008-000.
1-12	2008-2012	Numerous updates driven by model additions and software changes.
A	December 2013	Added new models, Viper SC™+; all Viper SC™ models become Viper SC+ when upgraded with new Viper SC+ firmware.
B	February 2015	Added UL warnings. Corrected voltage requirements. Numerous additions and changes driven by changes/additions to configuration changes.
C	February 2016	Updated Remote Diagnostics page to add PER mode support.
D	April 2016	Updated Remote Statistics with ability to delete entry
E	August 2016	Updated Security with new Other section
F	April 2017	Updated RF Settings UI with channel selection modes.
G	August 2017	Updated 4.8.3 SNMP – Removal of key installation (no longer applicable)
H	May 2021	NextGen acquisition, Rebranding, removed obsolete models
I	Dec 2023	Remove all references to Viper 900 and Viper SC

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 or death, or loss of property. NextGen RF 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

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

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

UL Listed models only

⚠ When operating at elevated temperature extremes, the surface may exceed +70 Celsius. For user safety, the Viper should be installed in a restricted access location.

⚠ WARNING — EXPLOSION HAZARD, do not connect while circuit is live unless area is known to be non-hazardous.

For more information see APPENDIX D — UL Installation Instructions

RF Exposure Compliance Requirements

RF Exposure

Viper SC+ radios are intended for use in the Industrial Monitoring and Control and SCADA markets. Each 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.

Minimum Safety Distance	Antenna Gain		
(cm @max power)	**5 dBi**	**10 dBi**	**15 dBi**
132 MHz (VHF)	123 cm	219 cm	389 cm
215 MHz (UHF)	123 cm	219 cm	389 cm
406.1 MHz	106 cm	188 cm	334 cm

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

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

Caution: Before deploying your system, you must read and understand Section 2.5 Selecting Antenna and Lightning Arrestor combinations.

Exigences de conformité d'exposition aux Radiofréquences

Exposition aux Radiofréquences

La radio Viper SC+ est destinée à être utilisé dans les marchés contrôles industriels et SCADA. L'unité Viper SC doit être installée par un professionnel et doit assurer une distance minimale de séparation entre les sources radiantes et toute personne. Les distances sont indiquées dans le tableau ci-dessous. L'installation typique est une antenne de type fouet 1/2-longueur d'onde installée sur un poteau ou pylône.

Distance de sécurité minimum	Gain de Antenne		
(puissance cm @ max)	**5 dBi**	**10 dBi**	**15 dBi**
132 MHz (VHF)	123 cm	219 cm	389 cm
215 MHz (UHF)	123 cm	219 cm	389 cm
406.1 MHz	106 cm	188 cm	334 cm

Note: *Il est de la responsabilité de l'utilisateur de garantir le respect des règlements MPE de la FCC lorsque vous utilisez cet appareil d'une façon autre que celle décrite ci-dessus. L'installateur doit s'assurer que l'antenne est située ou orientée de façon à ne pas émettre un champ RF dépassant les limites de radiations pour la population générale établies par Santé Canada.*

La radio Viper SC+ utilise un émetteur à radiofréquence à faible puissance. L'énergie concentrée d'une antenne peut poser un risque pour la santé. On ne devrait pas être en face de l'antenne lorsque l'émetteur est en marche.

Les consignes de sécurité recommandées pour l'exposition humaine à l'énergie électromagnétiques de radiofréquences sont contenues dans le Code 6 canadien de la sécurité (disponible auprès de Santé Canada), la Commission Communications Fédéral (FCC) Bulletin 65 et la recommandation du 12 Juillet 1999 sur la limitation de l'exposition du public aux champs électromagnétiques (de 0 Hz à 300 GHz) (1999/519/CE) du Conseil de l'Union européenne.

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 or her 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.

1 TABLE OF CONTENTS

1 VIPER SC+ OVERVIEW

The 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, 406.1125-511.975 MHzfrequencies. 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 SC+ supports serial and Ethernet/IP RTUs and PLCs. 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, 406.1125-470 MHz, 450-511.975 MHz,
- 142-174 MHz, 406.1125-470 MHz, and 450-511.975 MHz frequency ranges certified for European Union (ETSI EN300 113)
- 142-174 MHz, 406.1125-470 MHz, and 450-511.975 MHz frequency ranges certified for Australia/New Zealand (ACMA AS/NZS 4925-2004 Spectrum Impact Assessment)
- User-selectable data rates – up to 256 kbps @ 100 kHz
- Wide input power range of 10 to 30 V DC
- Built-in transceiver adjustable from 1 to 10 W
- Used as an access point or an end point with each configurable in the following:
  (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

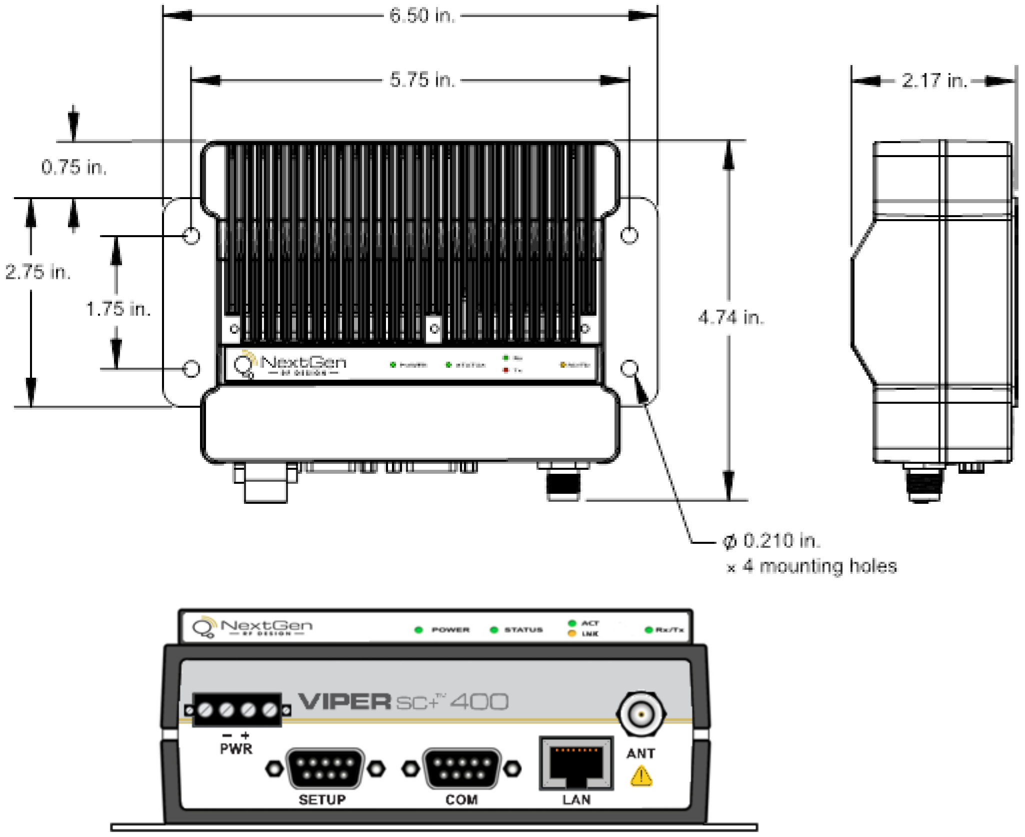
1.3. PHYSICAL DESCRIPTION

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

The following figure shows the dimensions of the Viper chassis and attached mounting plate.

Figure 1 – Viper SC+ Chassis and Mounting Plate Overall Dimensions and Mounting Hole Locations



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 in the LED panel of the Viper as shown in the following figure. Their functionality is described in the following table.

Figure 2 – Viper LED panel

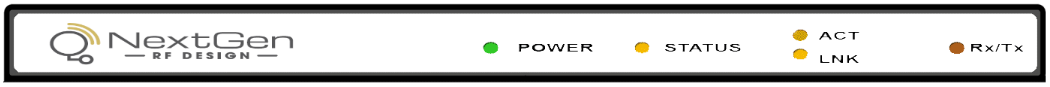


Table 1 – LED Functionality

LED	Color	Definition
POWER	Green (Solid) Green (Blinking) Red	Viper SC+ ready, normal operations Upgrade in progress Viper SC+ hardware fault
STATUS	Green Blinking Green Red Amber (Solid or Blinking)	Viper SC+ no faults, normal operations Viper SC+ scanning for neighbors Viper SC+ has a fault condition; check unit status Viper SC+ detects high background noise
ACT	Blinking Green Off	Ethernet activity detected on PHY link (RJ45 / LAN) No Ethernet activity on PHY link (RJ45 / LAN)
LNK	Amber Green Off	Ethernet connection Established, 100 Mbps (RJ45 / LAN) Ethernet connection Established, 10 Mbps (RJ45 / LAN) No Ethernet connection (RJ45 / LAN)
Rx/Tx	Green Red	Receiving data Transmitting data

1.3.3. FRONT PANEL

The front panel, shown in the following figure, has connections described in the following table.

Figure 3 – Front Panel (Dual Port Viper SC+ 200 Shown)

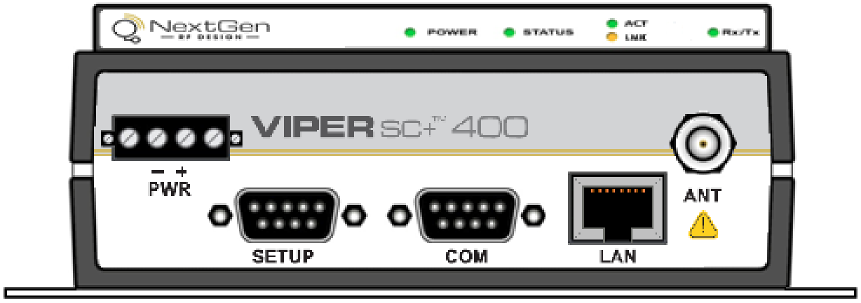


Table 2 – Front Panel Connections

Item	Description	Quantity
1	50 Ohm TNC Female Antenna connector	1
2	50 Ohm SMA Female Receive Antenna connector — **Dual-Port models only**.	1
3	Right-angle Power Connector (10-30 V DC)	1
4	DE-9F RS-232 ports: one (1) labeled Setup; one (1) labeled COM	2
5	10 Base T Auto-MDIX RJ-45 Ethernet LAN connection — **VHF/UHF models**, or	1
	10/100 Base T/Tx Auto-MDIX RJ-45 Ethernet LAN connection — **220/900 MHz models**.	1

1.3.3.1. Ethernet LAN Port

The Ethernet LAN port is an RJ-45 receptacle with a 10 Base T (or 100 Base T/Tx for 220 MHz and 290 MHz models) Ethernet connection and Auto-MDIX. Refer to the following table for pin-out descriptions and Section 4.4.6 to configure the LAN settings for this port.

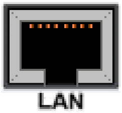
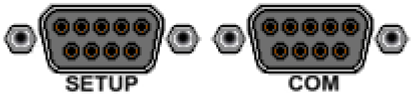


Table 3 – Pin-out for IEEE-802.3 RJ-45 Receptacle Contacts

Contact	10BaseT Signal
1	TXP[1]
2	TXN [1]
3	RXP [1]
4	SPARE
5	SPARE
6	RXN[1]
7	SPARE
8	SPARE
SHELL	Shield
[1] The name shows the default function. Given the Auto-MDIX capability of the Ethernet transceiver, Tx and Rx functions 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 the following table for pin-out descriptions and Section 4.3.4 for control line configurations of DCD, DTR, RTS, and CTS control lines.

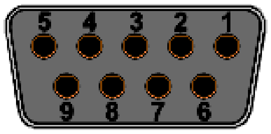


Serial port considerations:

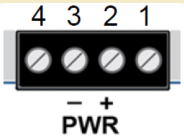
- Viper SETUP and COM ports are Data Communication Equipment (DCE) devices.
- In general, equipment connected to the Viper serial ports is Data Terminal Equipment (DTE) and a straight-through cable is recommended.

Note: If a DCE device is connected to the Viper serial ports, a null-modem cable or adapter is required.

Table 4 – Pin-Out for DCE SETUP and COM Port, 9 Contact DE-9 Connector

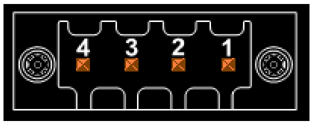
SETUP / COM port Pin-Out	Contact	Signal Name	Signal Direction	
 Contact Numbering	1	Data Carrier Detect (DCD)[1]	DTE ← DCE	
	2	Receive Data (RxD)	DTE ← DCE	
	3	Transmit Data (TxD)	DTE → DCE	
	4	Data Terminal Ready (DTR)	DTE → DCE	
	5	Signal Ground (GND)	DTE — DCE	
	6	Data Set Ready (DSR)[2]	DTE ← DCE	
	7	Ready To Send (RTS)[1]	DTE → DCE	
	8	Clear to Send (CTS)[1]	DTE ← DCE	
	9	Ring Indicator (RI)[3]	DTE — DCE	
	[1] Programmable [2] Always asserted [3] Future use			

1.3.3.3. Power Connector



Viper is supplied with a right-angle power connector (10-30 V DC). The following table shows the pin-out of the power connector.

Table 5 – Pin-Out of the Power Connector

Power Connector Pin-Out	Contact number (Left to Right)	Color	Description
	4		Fan Power Output (5V)
	3	Black	Ground
	2	Red	Positive (10-30) VDC
	1	White	Enable to Power Management — See *Note* • Power – Viper is awake. • No Power – Viper is asleep.

See Appendix B for detailed voltage and current requirements.

Note: The white Enable line must be tied to the red positive lead of the connector for the Viper to power up and 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 SC+ models have a 50-ohm TNC female antenna connector. This connection functions for both transmit and receive.

Warning: ***See Selecting Antenna and Lightning Arrestor combinations for information about types of lightning arrestors to not use and good design practices to use when selecting a lightning arrestor for use with an antenna.***

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 (50 mW).***

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.**

1.4. PART NUMBERS AND AVAILABILITY

Viper SC+™ is available in various models. Each is available with a range of features, kits, and accessories. Refer to the following table for product availability and part numbers for ordering. Refer to tables that follow for Viper SC+ accessories and for antenna options and kits.

1.4.1. VIPER SC+ RADIO

The following tables list Viper SC+ radios and kit part numbers.

NOTE: Obsolete models have been removed from the tables but are still supported through this manual.

Table 6 – Viper SC+ Radio and Kit Part Numbers

Viper SC+ 100 Series, 136 - 174 MHz

Model Number	Frequency Range	Description
140-5018-502	136 - 174 MHz	Viper SC+ 136-174 MHz 6.25-50 kHz BW
140-5018-503	136 - 174 MHz	Viper SC+ 136-174 MHz 6.25-50 kHz BW 2RFP
140-5118-502	136 - 174 MHz	Viper SC+ Std. BS 136-174 MHz 6.25-50 kHz BW
140-5318-502	136 - 174 MHz	Viper SC+ Rdnt. BS 136-174 MHz 6.25-50 kHz BW
140-5318-503	136 - 174 MHz	Viper SC+ Rdnt. BS 136-174 MHz 6.25-50 kHz BW 2RFP
250-5018-500	136 - 174 MHz	Viper SC+ 136-174 MHz Developer’s Kit (2 Vipers)
250-5018-510	136 - 174 MHz	Viper SC+ 136-174 MHz Developer’s Kit (3 Vipers)

Viper SC+ 200 Series, 215 - 240 MHz

Model Number	Frequency Range	Description
140-5028-504	215 - 240 MHz	Viper SC+ 215-240 MHz 6.25-100 kHz BW
140-5028-505	215 - 240 MHz	Viper SC+ 215-240 MHz 6.25-100 kHz BW 2RFP
140-5128-504	215 - 240 MHz	Viper SC+ Std. BS 215-240 MHz 6.25-100 kHz BW
140-5328-504	215 - 240 MHz	Viper SC+ Rdnt. BS 215-240 MHz 6.25-100 kHz BW
140-5328-505	215 - 240 MHz	Viper SC+ Rdnt. BS 215-240 MHz 6.25-100 kHz BW 2RFP
250-5028-502	215 - 240 MHz	Viper SC+ 215-240 MHz Developer’s Kit (2 Vipers)
250-5028-512	215 - 240 MHz	Viper SC+ 215-240 MHz Developer’s Kit (3 Vipers)

Key to abbreviations: BW = bandwidth, BS = Base Station, Std. = standard, Rdnt. = redundant, 2RFP = Dual RF Port.

Viper SC+ 400 Series, Range 3

Model Number	Frequency Range	Description
140-5048-302	406.1 - 470 MHz	Viper SC+ 406.1-470 MHz 6.25-50 kHz BW
140-5048-303	406.1 - 470 MHz	Viper SC+ 406.1-470 MHz 6.25-50 kHz BW 2RFP
140-5148-302	406.1 - 470 MHz	Viper SC+ Std. BS 406.1-470 MHz 6.25-50 kHz BW
140-5348-302	406.1 - 470 MHz	Viper SC+ Rdnt. BS 406.1-470 MHz 6.25-50 kHz BW
140-5348-303	406.1 - 470 MHz	Viper SC+ Rdnt. BS 406.1-470 MHz 6.25-50 kHz BW 2RFP
250-5048-300	406.1 - 470 MHz	Viper SC+ 406.1-470 MHz Developer’s Kit (2 Vipers)
250-5048-310	406.1 - 470 MHz	Viper SC+ 406.1-470 MHz Developer’s Kit (3 Vipers)

Viper SC+ 400 Series, Range 5

Model Number	Frequency Range	Description
140-5048-502	450 - 512 MHz	Viper SC+ 450-512 MHz 6.25-50 kHz BW
140-5048-503	450 - 512 MHz	Viper SC+ 450-512 MHz 6.25-50 kHz BW 2RFP
140-5148-502	450 - 512 MHz	Viper SC+ Std. BS 450-512 MHz 6.25-50 kHz BW
140-5348-502	450 - 512 MHz	Viper SC+ Rdnt. BS 450-512 MHz 6.25-50 kHz BW
140-5348-505	450 - 512 MHz	Viper SC+ Rdnt. BS 450-512 MHz 6.25-50 kHz BW 2RFP
250-5048-500	450 - 512 MHz	Viper SC+ 450-512 MHz Developer’s Kit (2 Vipers)
250-5048-510	450 - 512 MHz	Viper SC+ 450-512 MHz Developer’s Kit (3 Vipers)

Key to abbreviations: BW = bandwidth, BS = Base Station, Std. = standard, Rdnt. = redundant, 2RFP = Dual RF Port.

EN 300 113 ETSI Compliant and AS/NZ Compliant Models

Table 7 – Viper SC+ EN 300 113 ETSI Compliant and AS/NZ Compliant Radio and Kit Part Numbers

Viper SC+ 100 Series, 142 – 174 MHz

Model Number	Frequency Range	Description
140-5018-600	142 - 174 MHz	Viper SC+ 142-174 MHz 12.5-25 kHz BW ETSI AS/NZ
140-5018-601	142 - 174 MHz	Viper SC+ 142-174 MHz 12.5-25 kHz BW ETSI AS/NZ 2RFP
140-5118-600	142 - 174 MHz	Viper SC+ Std. BS 136-174 MHz 12.5-25 kHz BW ETSI AS/NZ
140-5118-601	142 - 174 MHz	Viper SC+ Std. BS 136-174 MHz 12.5-25 kHz BW ETSI AS/NZ 2RFP
140-5318-600	142 - 174 MHz	Viper SC+ Rdnt. BS 142-174 MHz 12.5-25 kHz BW ETSI AS/NZ
140-5318-601	142 - 174 MHz	Viper SC+ Rdnt. BS 142-174 MHz 12.5-25 kHz BW ETSI AS/NZ 2RFP

Viper SC+ 400 Series, Range 3

Model Number	Frequency Range	Description
140-5048-400	406.1 - 470 MHz	Viper SC+ 406.1-470 MHz 12.5-25 kHz BW ETSI AS/NZ
140-5048-401	406.1 - 470 MHz	Viper SC+ 406.1-470 MHz 12.5-25 kHz BW ETSI AS/NZ 2RFP
140-5148-400	406.1 - 470 MHz	Viper SC+ Std. BS 406.1-470 MHz 12.5-25 kHz BW ETSI AS/NZ
140-5148-401	406.1 - 470 MHz	Viper SC+ Std. BS 406.1-470 MHz 12.5-25 kHz BW ETSI AS/NZ 2RFP
140-5348-400	406.1 - 470 MHz	Viper SC+ Rdnt. BS 406.1-470 MHz 12.5-25 kHz BW ETSI AS/NZ
140-5348-401	406.1 - 470 MHz	Viper SC+ Rdnt. BS 406.1-470 MHz 12.5-25 kHz BW ETSI AS/NZ 2RFP

Viper SC+ 400 Series, Range 5

Model Number	Frequency Range	Description
140-5048-600	450 - 512 MHz	Viper SC+ 450-512 MHz 12.5-25 kHz BW ETSI AS/NZ
140-5048-601	450 - 512 MHz	Viper SC+ 450-512 MHz 12.5-25 kHz BW ETSI AS/NZ 2RFP
140-5148-600	450 - 512 MHz	Viper SC+ Std. BS 450-512 MHz 12.5-25 kHz BW ETSI AS/NZ
140-5148-601	450 - 512 MHz	Viper SC+ Std. BS 450-512 MHz 12.5-25 kHz BW ETSI AS/NZ 2RFP
140-5348-600	450 - 512 MHz	Viper SC+ Rdnt. BS 450-512 MHz 12.5-25 kHz BW ETSI AS/NZ
140-5348-601	450 - 512 MHz	Viper SC+ Rdnt. BS 450-512 MHz 12.5-25 kHz BW ETSI AS/NZ 2RFP

Key to abbreviations: BW = bandwidth, BS = Base Station, Std. = Standard, Rdnt. = Redundant, 2RFP = Dual RF Port.

1.4.2. FAN KITS AND CABLES

The following tables list standard fan kits and cables available for use with the Viper SC+™.

Table 8 – Viper SC+ Fan Kits

Description	Part Number
Fan Kit, Viper SC+, Factory Installed	150-5008-001
Fan Kit, Viper SC+, Field Installed	150-5008-002

Table 9 – Viper SC+™ Power Cable

Description	Part Number
Power Cable, Viper SC+	897-5008-010

Table 10 – Coaxial Adapter Cables

Length	Connectors	Type	Part Number
18 inches	TNC-Male to N-Male	RG-400	140-5018-502
48 inches	TNC-Male to N-Male	RG-400	140-5018-503
72 inches	TNC-Male to N-Male	RG-400	250-5018-502
18 inches	TNC-Male to N-Female	RG-400	140-5118-502

1.5. COMPONENTS

1.5.1. BASIC UNIT

The following items are included with the Viper SC+ basic unit.

Description	Item
Viper SC+ IP Router	
60 in. Cat 5 Ethernet Cable	
Power Cable	

1.5.2. TWO- AND THREE-PIECE KIT ADDITIONAL ITEMS

The following items are included with two- and three-piece Viper SC+™ Developer Kits.

Description	Item
SMA Male to BNC Female Connector	
SMA Female to BNC Male Connector	
TNC Male to BNC Female Connector	
Mini Circuits 5 W 20 dB Attenuator	
Flex Rubber Duck Antenna (VHF, UHF, or 900 MHz)	
120 VAC to 13.8 VDC 4 A Power Supply	

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 SC+ 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+ can 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 an RS232

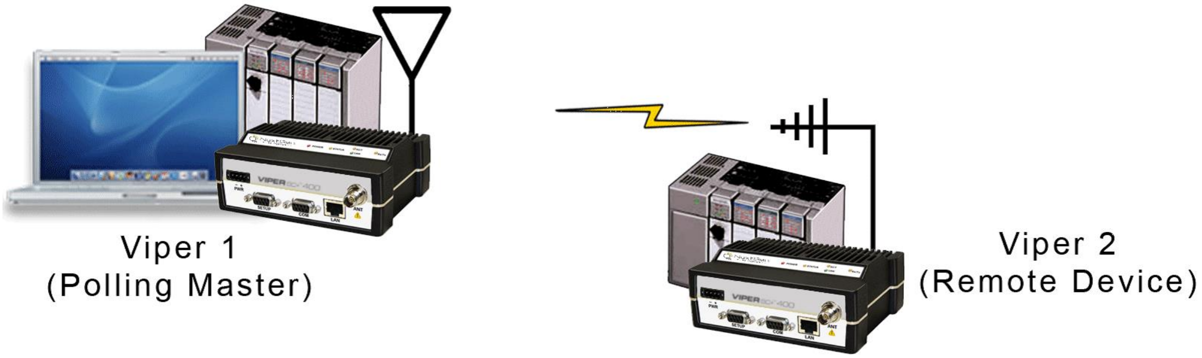
polling message, which may or may not be generated by the same HMI/PLC. NextGen RF recommends the user program the polling sequence in each protocol with logic that interacts with the other’s protocol “Done” and “Error” bits. The Ethernet polling protocol would not be allowed to send a message until 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 NETWORK

A point-to-point network is the simplest type of network and may be used for connecting a pair of PCs, a host computer and a terminal, a SCADA polling master and one remote, or a wide variety of other networking applications.

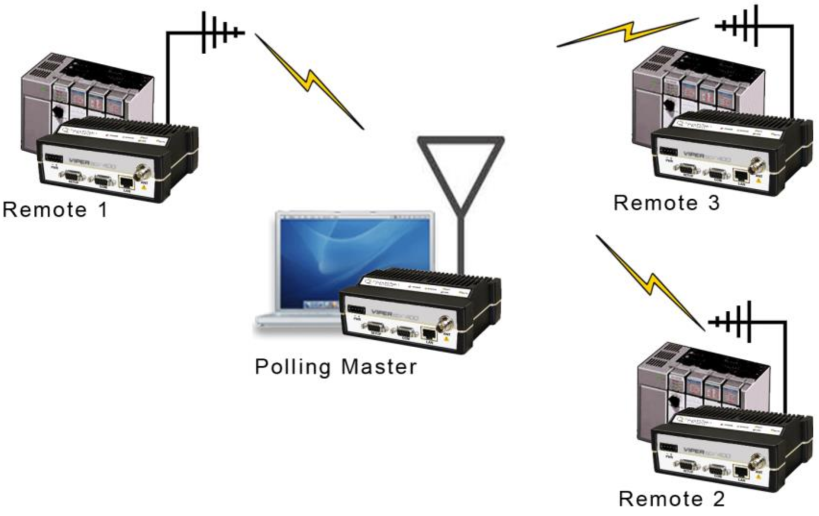
Figure 4 – Point-to-Point Network

2.1.2. POINT-TO-MULTIPOINT NETWORK



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 5 – Point-to-Multipoint Network



2.1.3. REPORT BY EXCEPTION CONFIGURATION

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

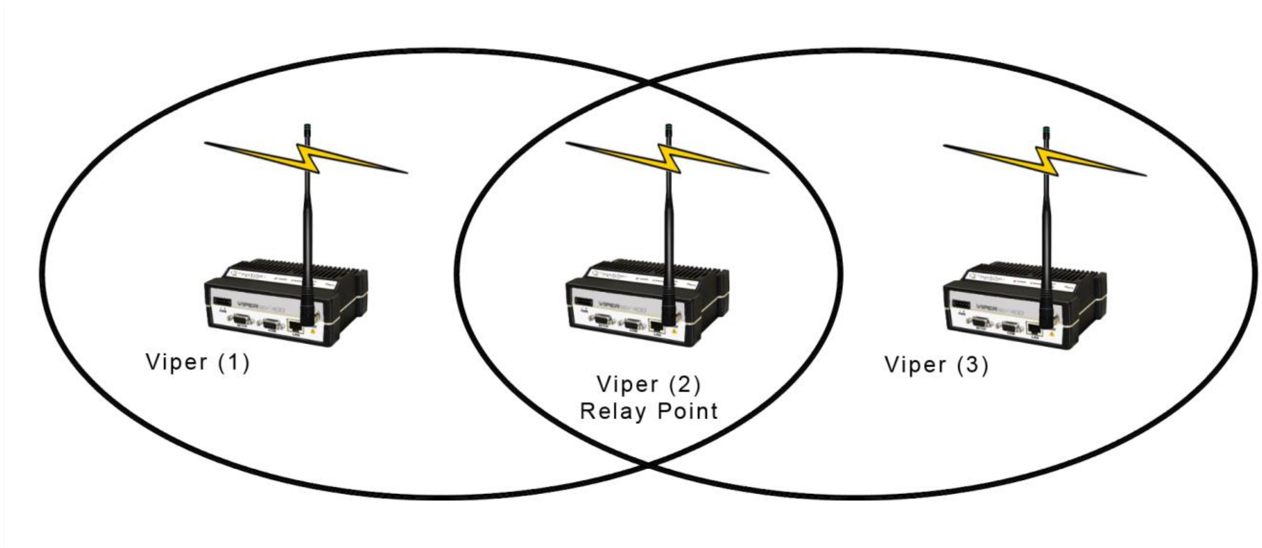
A Viper can be configured as a Relay Point (see the following figure). Relay Points provide store and forward repeating of necessary information from one coverage area to the next. In Bridge mode all traffic is forwarded. In Router mode, only Broadcast Packets and address specific packets are forwarded. There may be multiple Relay Points to extend coverage over several hops.

Note: Multiple relay points in a single network may slow the flow of data traffic.

Serial data is always sent out as a broadcast message. A broadcast message cannot take advantage of IP routing mode so it must use relay points to move from one RF coverage area to another. However, it may be possible to configure the Viper SC+ so that it may be able to take advantage of the router mode feature and collision avoidance features of the router mode.

An option to configure the Viper SC+ as a relay point is in the first step of the Viper Setup Wizard or later in the RF Network tab of the RF Network Settings page. Instructions for completing the Viper Setup Wizard and for configuration options in the Viper Web Interface tabbed pages are provided later in this User Manual.

Figure 6 – Extending coverage areas by configuring the Viper SC+ as a relay point



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 a packet will pass through several gateways or routers to get to its destination.

The Viper SC+ has two different modes of operation:

- Bridge Mode – Bridge mode is for quick setup of units all on the same network.
- Router Mode — Router mode is for advanced networks.

Both modes are explained in the sections that follow.

2.1.5. 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

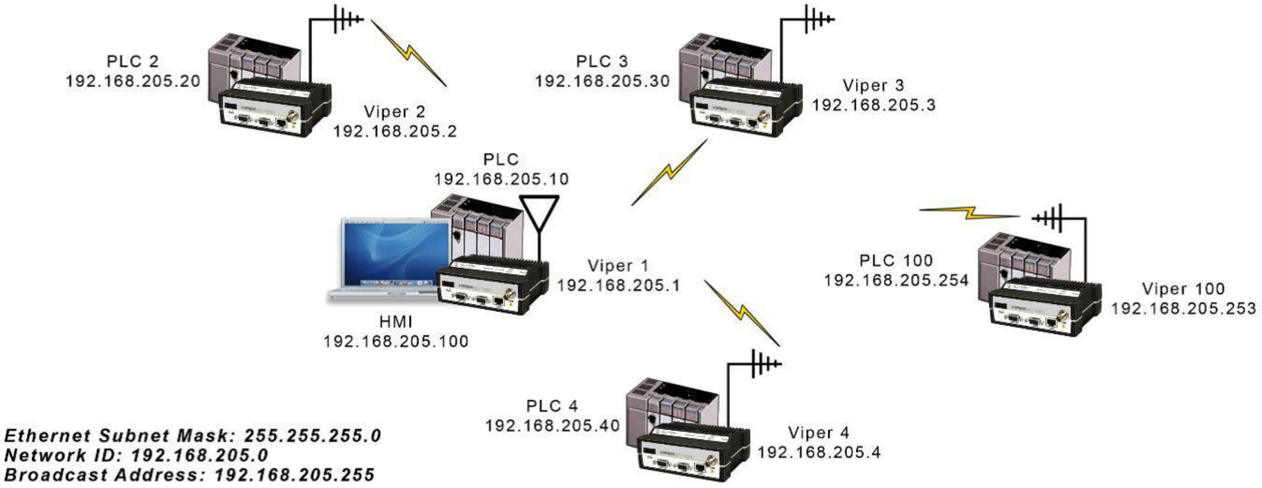
This example illustrates a sample Viper network. The subnet consists of IP addresses ranging from 192.168.205.0 to 192.168.205.255. The subnet mask is 255.255.255.0. This subnet is sometimes indicated as 192.168.205.1/24 since the subnet mask 255.255.255.0 contains 24 ones (followed by 8 zeros) when 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.

Ethernet Subnet Mask	255.255.255.0
Network ID	192.168.205.0
Broadcast Address	192.168.205.255

Viper #1	192.168.205.1/24	**Viper #2**	192.168.205.2/24
PLC/RTU #1	192.168.205.10/24	PLC/RTU #2	192.168.205.20/24
Computer #1	192.168.205.100/24		
Viper #3	192.168.205.3/24	**Viper #4**	192.168.205.4/24
PLC/RTU #3	192.168.205.30/24	PLC/RTU #4	192.168.205.40/24
…		**Viper #100**:	192.168.205.253/24
		PLC/RTU #100:	192.168.205.254/24

Figure 7 – 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 (followed by 16 zeros) when converted to binary.

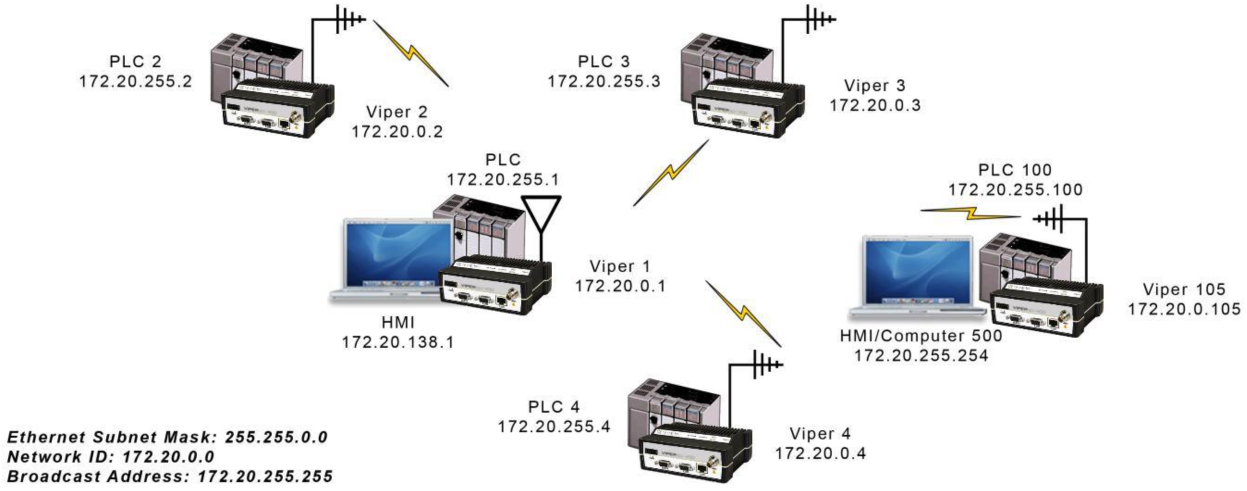
- The first address 172.20.0.0 is reserved for the Network ID.
- The last address 172.20.255.255 is reserved for the broadcast address.
- There are 65534 valid IP addresses available to be assigned to hosts on the network.

Ethernet Subnet Mask	255.255.255.0
Network ID	172.20.0.0
Broadcast Address	172.20.255.255

Viper #1	172.20.0.1/16	**PLC/RTU #1**	172.20.255.1/16
Viper #2	172.20.0.2/16	**PLC/RTU #2**	172.20.255.2/16
Viper #3	172.20.0.3/16	**PLC/RTU #3**	172.20.255.3/16
…		…	
Viper #105	172.20.0.015/16	**PLC/RTU #250**	172.20.255.250/16

Computer #1	172.20.138.1/16
…	
Computer #500	172.20.255.254/ 16

8 – Bridge Mode Example 2



2.1.6. ROUTER MODE

Router mode allows greater network configuration flexibility, allows the use of a variety of protocols, and adds RF diagnostics capability to Viper networks. Diagnostics can be retrieved through the Ethernet port of the Viper. More information about Viper RF diagnostics is provided in section 4.6 .

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 into the network.

In Router mode, each Viper uses two IP addresses:

- An Ethernet IP Address
- An 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.

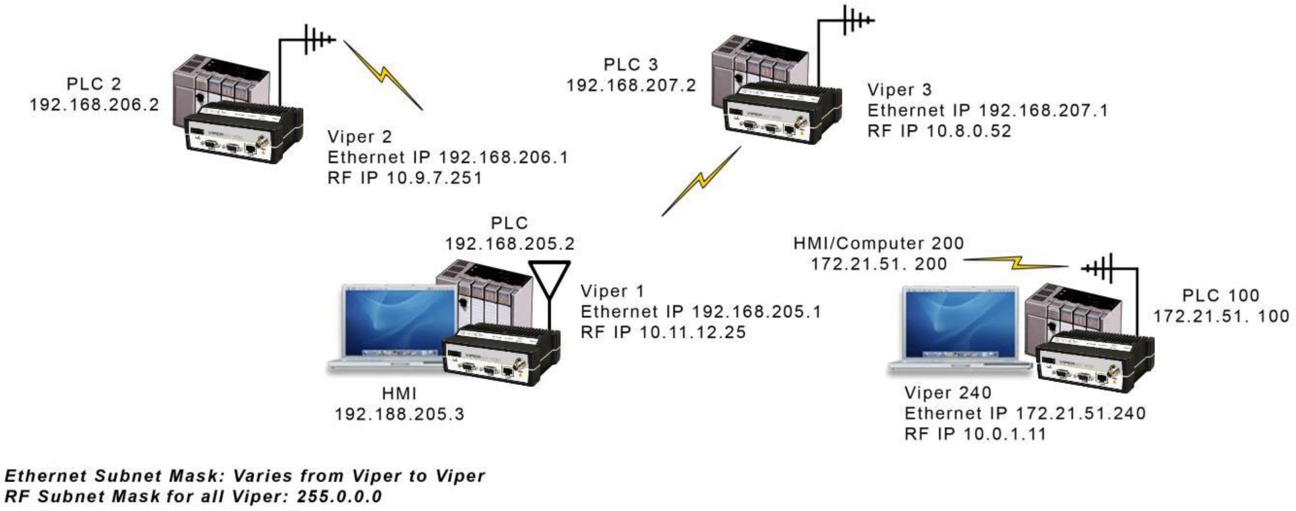
Note 2 All the Viper Ethernet IP addresses are on different networks.

Note 3 Computers, PLCs, RTUs, or other Ethernet capable devices can be connected 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 relates to.

Ethernet Subnet Mask Varies from Viper to Viper.
RF Subnet Mask is the same for all units: 255.0.0.0 (hence /8 shown for all RF IP Addresses; 8 ones (24 zeros) binary.)
HMI/PLC/RTU Default Gateway points to the Viper that the HMI/PLC/RTU is connected to.

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	Default Gateway:	192.168.205.1
	Computer/HMI #1:	192.168.205.3/24	Default Gateway:	192.168.205.1
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	Default Gateway	192.168.206.1
Viper #3:	Ethernet IP Address:	192.168.207.1/24	RF IP Address:	10.8.0.52/8
	PLC #3:	192.168.207.2/24	Default Gateway:	192.168.207.1
	Computer #3:	192.168.207.3/24	Default Gateway:	192.168.207.1
Viper #4:	Ethernet IP Address:	172.21.51.105/16	RF IP Address:	10.0.1. 11/8
	PLC #4:	172.21.51.106/16	Default Gateway	172.21.51.106

Figure 9 – Router Mode Example 1



Router Mode Example 2

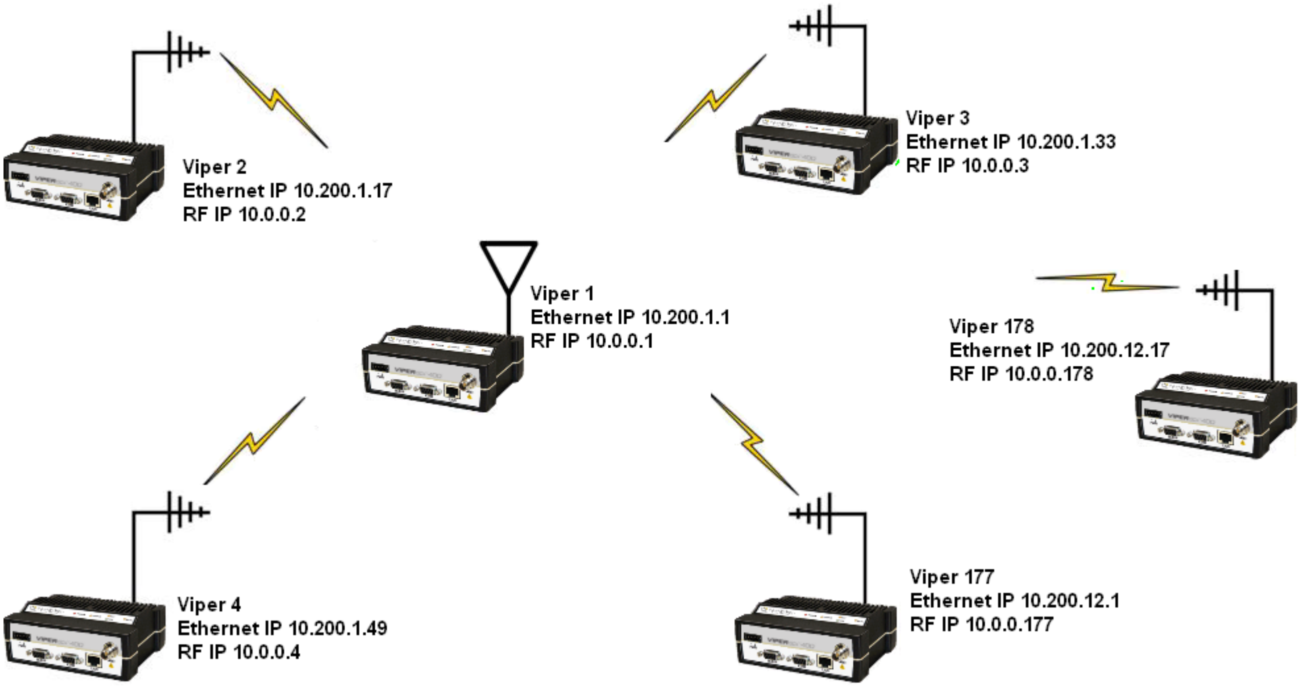
Each Viper has an Ethernet IP address on a unique network.

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.

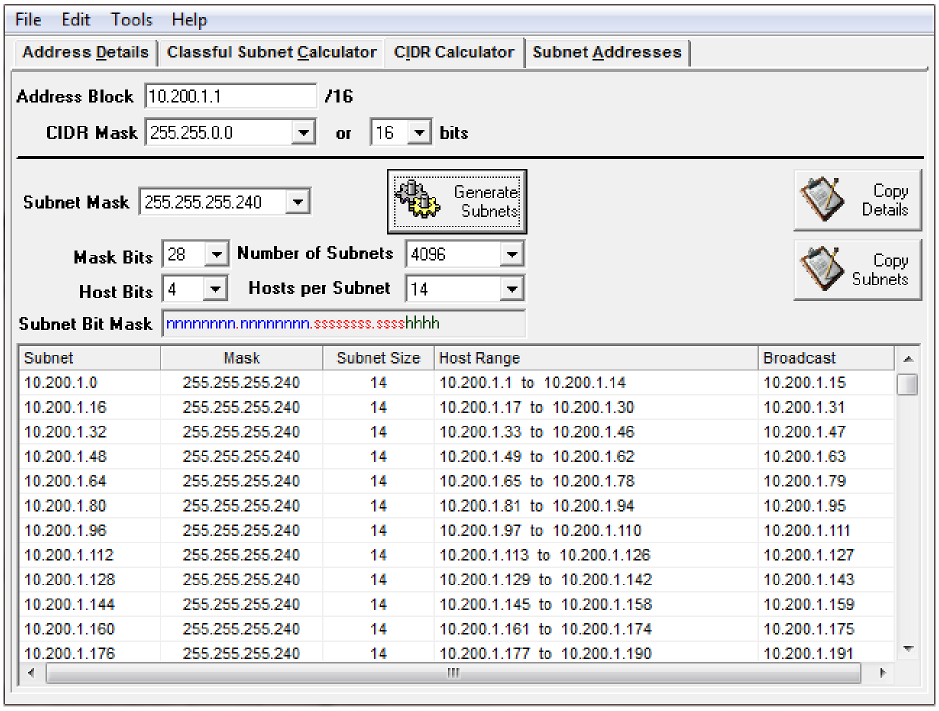
Viper #1:	Ethernet IP Address:	10.200.1.1/28	RF IP Address:	10.0.0.1/16
Viper #2:	Ethernet IP Address:	10.200.1.17/28	RF IP Address:	10.0.0.2/16
Viper #3:	Ethernet IP Address:	10.200.1.33/28	RF IP Address:	10.0.0.3/16
Viper #4:	Ethernet IP Address:	10.200.1.49/28	RF IP Address:	10.0.0. 4/16
…				
Viper #177:	Ethernet IP Address:	10.200.12.1/28	RF IP Address:	10.0.0.177/16
Viper #178:	Ethernet IP Address:	10.200.12.17/28	RF IP Address:	10.0.0. 178/16

Figure 10 – Router Mode Example 2



Solarwinds™ Advanced Subnet Calculator (available as a free download from the Solarwinds website at www.solarwinds.com) can be used to help calculate subnets as used in this example. The Advanced Subnet Calculator will calculate and display the range of host IP addresses that can be used, as shown in the following figure.

Figure 11 – Router Mode Example 2 Subnet Calculations


File Edit Tools Help
Address Details | Classful Subnet Calculator | CIDR Calculator | Subnet Addresses
Generate Subnets
Copy Details
Copy Subnets

Address Block 10.200.1.1 /16

CIDR Mask 255.255.0.0 or 16 bits

Subnet Mask 255.255.255.240

Mask Bits 28 Number of Subnets 4096

Host Bits 4 Hosts per Subnet 14

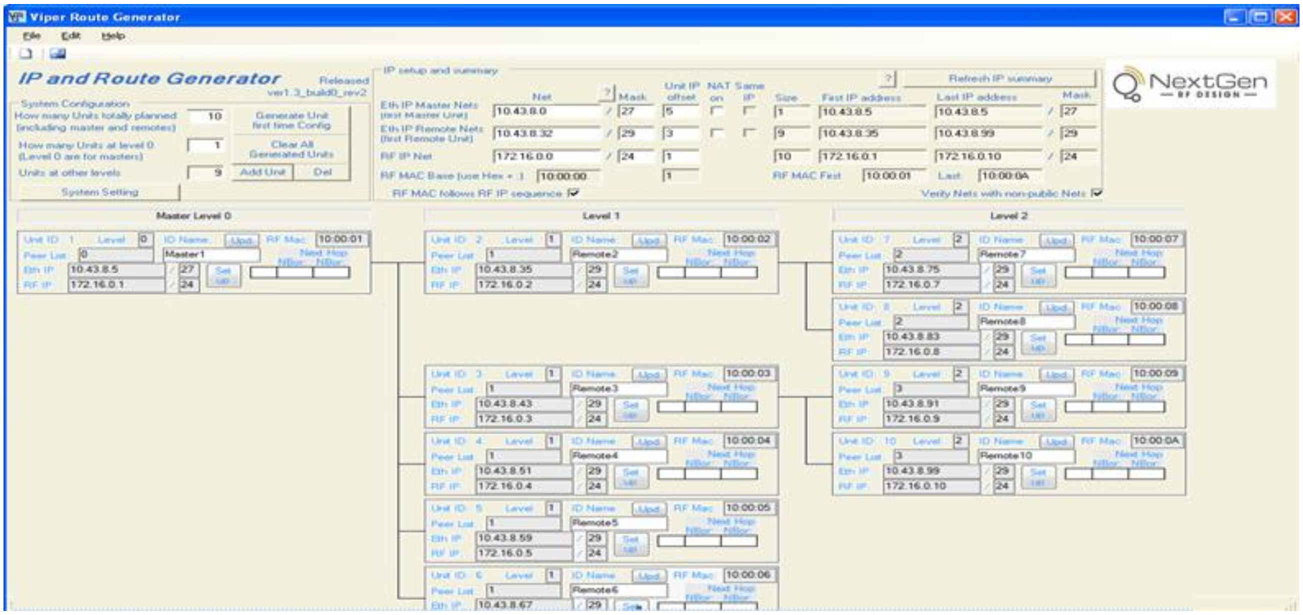
Subnet Bit Mask nnnnnnnn.nnnnnnnn.ssssssss.sssshhhh

Subnet	Mask	Subnet Size	Host Range	Broadcast
10.200.1.0	255.255.255.240	14	10.200.1.1 to 10.200.1.14	10.200.1.15
10.200.1.16	255.255.255.240	14	10.200.1.17 to 10.200.1.30	10.200.1.31
10.200.1.32	255.255.255.240	14	10.200.1.33 to 10.200.1.46	10.200.1.47
10.200.1.48	255.255.255.240	14	10.200.1.49 to 10.200.1.62	10.200.1.63
10.200.1.64	255.255.255.240	14	10.200.1.65 to 10.200.1.78	10.200.1.79
10.200.1.80	255.255.255.240	14	10.200.1.81 to 10.200.1.94	10.200.1.95
10.200.1.96	255.255.255.240	14	10.200.1.97 to 10.200.1.110	10.200.1.111
10.200.1.112	255.255.255.240	14	10.200.1.113 to 10.200.1.126	10.200.1.127
10.200.1.128	255.255.255.240	14	10.200.1.129 to 10.200.1.142	10.200.1.143
10.200.1.144	255.255.255.240	14	10.200.1.145 to 10.200.1.158	10.200.1.159
10.200.1.160	255.255.255.240	14	10.200.1.161 to 10.200.1.174	10.200.1.175
10.200.1.176	255.255.255.240	14	10.200.1.177 to 10.200.1.190	10.200.1.191

2.1.7. VIPER ROUTER GENERATOR (VRG) PROGRAM

NextGen RF has developed a Viper Route Generator (VRG) application that assists in generating the Viper's neighbor or router tables and generates the configuration files for all the radios in your project within minutes.

Figure 12 – Viper Route Generator tool



System Configuration

How many Units totally planned (including master and remotes) 10

How many Units at level 0 (Level 0 are for masters) 1

Units at other levels 9

IP setup and summary

	Net	Mask	Unit IP offset	NAT on	Same IP	Size	First IP address	Last IP address	Mask
Eth IP Master Nets (first Master Unit)	10.43.8.0	/ 27	5	☐	☐	1	10.43.8.5	10.43.8.5	/ 27
Eth IP Remote Nets (first Remote Unit)	10.43.8.32	/ 29	3	☐	☐	9	10.43.8.35	10.43.8.99	/ 29
RF IP Net	172.16.0.0	/ 24	1			10	172.16.0.1	172.16.0.10	/ 24

RF MAC Base (use Hex + :) 10:00:00 1 RF MAC First 10:00:01 Last 10:00:0A

RF MAC follows RF IP sequence ☑ Verify Nets with non-public Nets ☑

Unit ID	Level	ID Name	RF Mac	Peer List	Eth IP		RF IP	
1	0	Master1	10:00:01	0	10.43.8.5	/ 27	172.16.0.1	/ 24
2	1	Remote2	10:00:02	1	10.43.8.35	/ 29	172.16.0.2	/ 24
3	1	Remote3	10:00:03	1	10.43.8.43	/ 29	172.16.0.3	/ 24
4	1	Remote4	10:00:04	1	10.43.8.51	/ 29	172.16.0.4	/ 24
5	1	Remote5	10:00:05	1	10.43.8.59	/ 29	172.16.0.5	/ 24
6	1	Remote6	10:00:06	1	10.43.8.67	/ 29		
7	2	Remote7	10:00:07	2	10.43.8.75	/ 29	172.16.0.7	/ 24
8	2	Remote8	10:00:08	2	10.43.8.83	/ 29	172.16.0.8	/ 24
9	2	Remote9	10:00:09	3	10.43.8.91	/ 29	172.16.0.9	/ 24
10	2	Remote10	10:00:0A	3	10.43.8.99	/ 29	172.16.0.10	/ 24

You should try to choose an IP addressing scheme so that the master Viper's address is always first in a sequence and then the remote IP addresses to follow in that sequence.

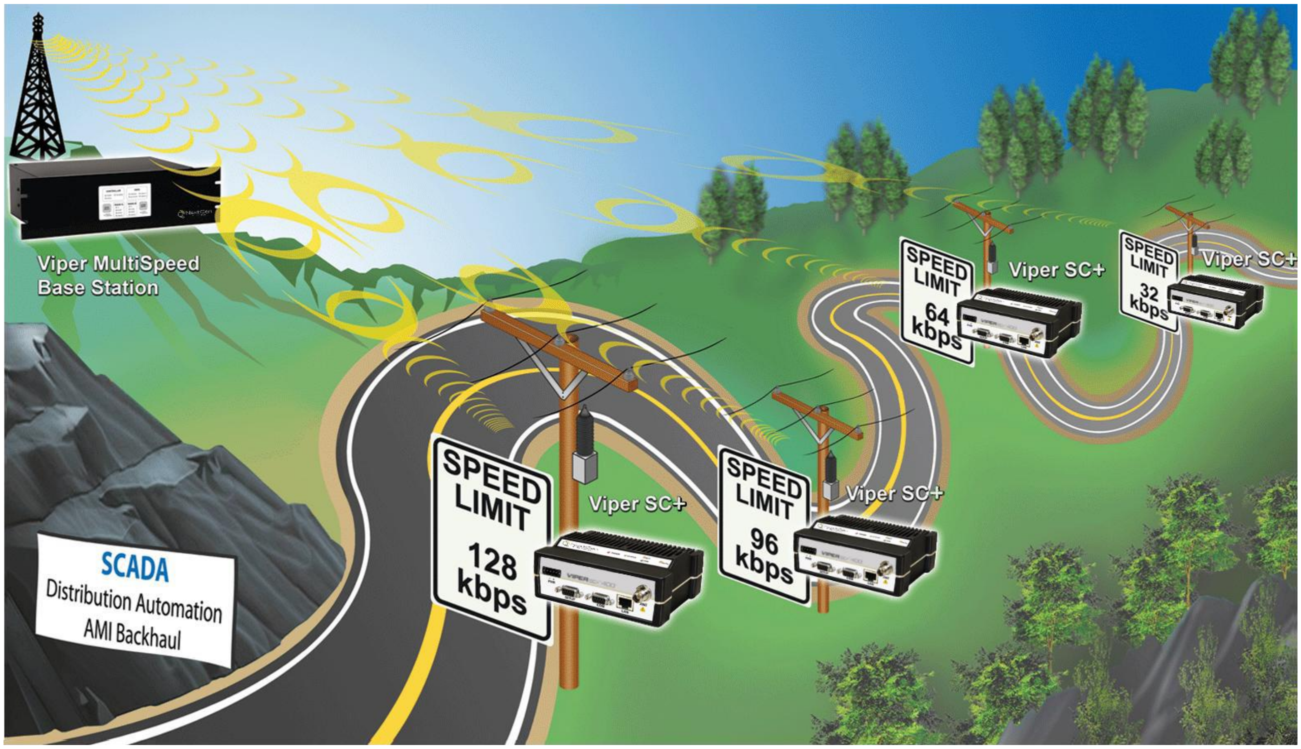
The VRG application can be downloaded from NextGen RF. Contact NextGen RF Technical Support to obtain the VRG application and instructions for its use.

2.1.8. MULTISPEED NETWORKING

When using the Viper SC+ with a Viper SC+ multi-speed base station, it is possible to configure the network for multispeed operation. With the base station enabled as the *rate controller*, the remote device becomes a *rate follower*. The rate controller (base station) 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 using the Base Station configuration interface 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 for the same bandwidth.

An option to configure the Viper SC+ for multispeed networking is in the first step of the Viper Setup Wizard or later in the RF Network tab of the RF Network Settings page. Instructions for completing the Viper Setup Wizard and for configuration options in the Viper Web Interface tabbed pages are provided later in this User Manual.

Figure 13 – Viper SC+ Base Station with remote Vipers configured with different OTA data rates



2.2. 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 indicator of strength of signal energy received by the receiver is called the Received Signal Strength Indication (RSSI) and is expressed in dBm.

A radio modem requires minimum amount of received RF signal to operate reliably and provide adequate data throughput. This is the radio receiver’s sensitivity. In most cases, spectrum regulators will define or limit the amount of signal that can be transmitted, and it will be noted in 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. SITE SELECTION AND SITE SURVEY

2.3.1. SITE SELECTION

For a successful installation, careful thought must be given to selecting the site for each radio. These requirements can be quickly determined in most cases. 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.

2.3.2. SITE SURVEY

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

2.4. SELECTING ANTENNA AND LIGHTNING ARRESTOR COMBINATIONS

Very Important! Before you deploy your system, you must read and understand this section.

RF engineers and installers have seen many types of radio installations over the years, and they know there are certain details that must not be overlooked at any installation. Most radio installations contain some form of lightning protection. However, the wrong combination of antenna and lightning arrestor can create high voltage transients on the radio’s antenna port having devastating impacts on the life and reliability of modern-day radio equipment.

2.4.1. LIGHTNING ARRESTOR OVERVIEW

Lightning arrestors can take many forms. But some of the most common lightning arrestors use gas discharge tubes that turn on when the voltage across their terminals exceeds the specified threshold. Under normal conditions, these devices have extremely high impedance and no current flows through the device. When the turn on voltage threshold is exceeded, the gas discharge tube turns on instantaneously and becomes a short.

This functionality works well to limit the magnitude of a transient from a nearby lightning discharge. However, it can have extremely negative consequences if a gas discharge lightning arrestor is used with the wrong antenna.

2.4.2. ANTENNA OVERVIEW

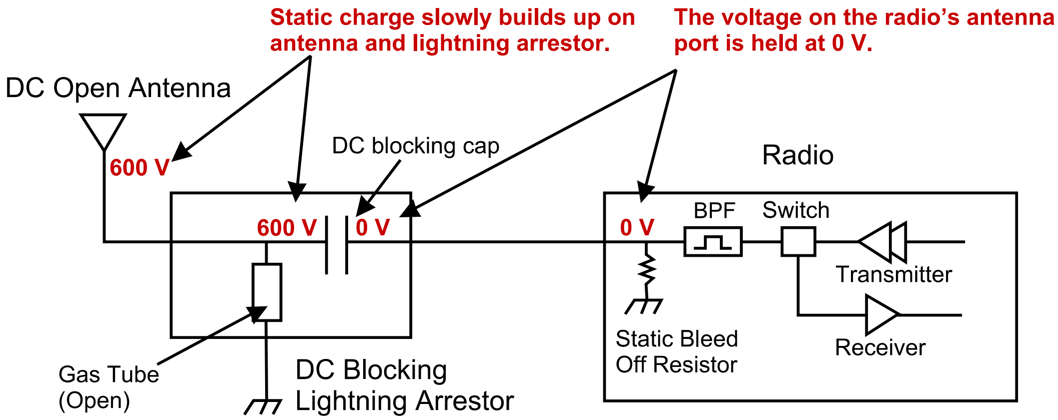
Antennas can come in just about any shape or size. However, there is one parameter that the system designer should not overlook, especially if the radio installation uses gas discharge tube lightning arrestors. The parameter is the DC grounding of the active element in the antenna.

A DC grounded antenna will measure 0 ohms from the active element to ground when tested with an ohmmeter. One way to test this is to connect the ohmmeter from the center conductor to ground of the RF cable that is attached directly to the antenna. This will read as a short for a DC grounded antenna, and as an open for a non-DC grounded antenna. Note: Some antenna datasheets are misleading and will indicate the antenna is DC grounded. However, the datasheet may be referring to the body of the antenna and not necessarily the active element. For this reason, it is best to measure the antenna you plan to use to verify the active element is DC grounded.

2.4.3. THE WRONG COMBINATION

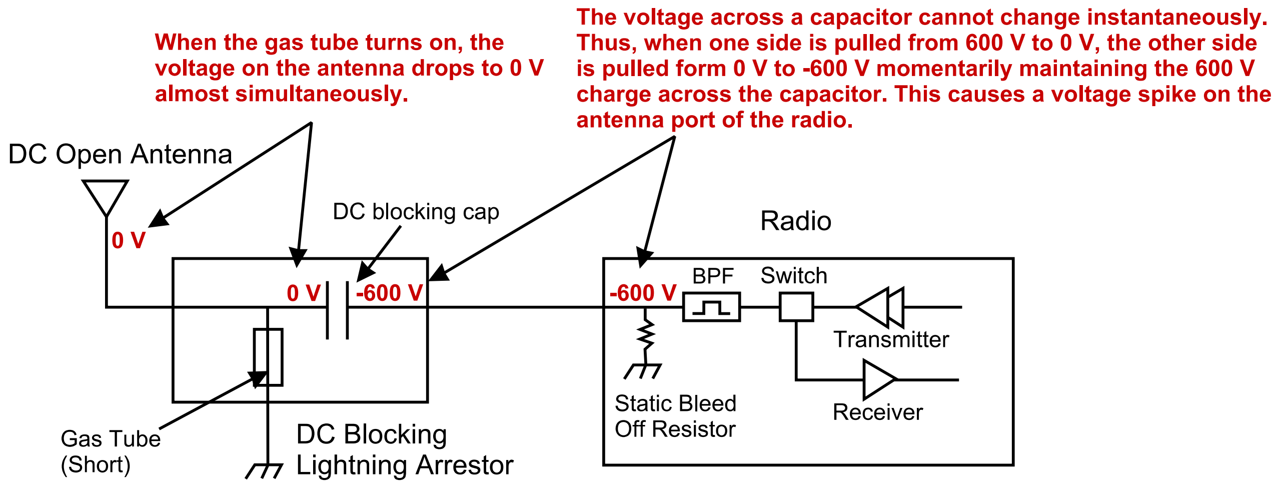
The combination of a DC open antenna and a DC blocked gas discharge tube lightning arrestor creates a situation where static charge can build up slowly on the active element of the antenna. Static charge can be created by wind blowing across the antenna, precipitation hitting the active element, or other environmental causes. As static charge builds up on the antenna’s active element, over a period of minutes or even hours, the DC blocking capacitor inside the lightning arrestor is charged.

Figure 14 – Voltage buildup due to static


Static charge slowly builds up on antenna and lightning arrestor.
The voltage on the radio’s antenna port is held at 0 V.
DC Open Antenna
600 V
DC blocking cap
Radio
600 V
0 V
0 V
BPF
Switch
Transmitter
Receiver
Static Bleed Off Resistor
Gas Tube (Open)
DC Blocking Lightning Arrestor

When the voltage exceeds 600V (the breakdown voltage for IS-B50LN series PolyPhasers), the gas discharge tube turns on and the antenna side of the DC blocking capacitor is immediately pulled from 600V to 0V. Since the lighting arrestor’s capacitor was charged to 600V, that charge must dissipate through the radio. As the capacitor discharges, a large negative transient is created on the antenna port of the radio. Positive transients can also be created if the static charge buildup on the antenna has a negative polarity.

Figure 15 – Voltage transient immediately after the gas tube turns on



When the gas tube turns on, the voltage on the antenna drops to 0 V almost simultaneously.

The voltage across a capacitor cannot change instantaneously. Thus, when one side is pulled from 600 V to 0 V, the other side is pulled form 0 V to -600 V momentarily maintaining the 600 V charge across the capacitor. This causes a voltage spike on the antenna port of the radio.

During testing, transients were measured on the antenna port of NextGen RF’s Viper at voltage levels up to +/-280V. These voltage transients often have high frequency content that can easily pass through any filtering in the radio and damage components in the transmitter and receiver circuitry.

2.4.4. GOOD DESIGN PRACTICES

There are two relatively easy ways to avoid creating large transients due to static buildup on an antenna and the subsequent firing of the gas discharge tube in the lightning arrestor. Following either or both recommendations below will eliminate this potential problem.

1. Use antennas with a DC grounded active element. Antennas can easily be tested, by using an ohm meter, to measure the resistance from the center conductor to the ground of the RF cable that is directly attached to the antenna. The ohmmeter should indicate a short. (Some antenna designs, such as folded dipole or folded dipole Yagi antennas, inherently have a DC ground on the active element due to the nature of the antenna design.)

2. Use a lightning arrestor that does not have a gas discharge tube. PolyPhaser® makes several DC-blocked lightning arrestors that have an inductor to ground instead of a gas tube. These lightning arrestors will not allow the static to build up on the antenna, and there is no gas tube that can trigger causing a transient into the antenna port of the radio. The following lightning arrestors, manufactured by PolyPhaser, have inductors to ground instead of gas tubes:

   a. PolyPhaser® Part Number: VHF50HN Frequency Range: 100MHz - 512MHz, 750W

   b. PolyPhaser® Part Number: TSX-NFF Frequency Range: 700MHz - 2.7GHz, 750W

Tip: Lightning arrestors that use gas tubes will normally specify a “Turn-On Voltage” in the data sheet. If you see this specification in the datasheet, it is very likely that the lightning arrestor has a gas discharge tube. If you are still unsure, contact the manufacturer.

2.5. SELECTING ANTENNA AND FEEDLINE

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

2.5.1. ANTENNA GAIN

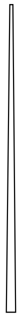
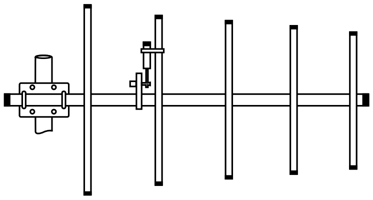
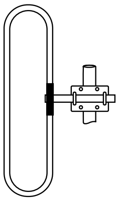
Antenna gain is usually measured in comparison to a dipole. A dipole acts much like the filament of a flashlight bulb: it radiates energy in almost all directions. One bulb like this would provide very dim room lighting. Add a reflector capable of concentrating all the energy into a narrow angle of radiation 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.

2.5.2. TYPES OF ANTENNAS

Several FCC-approved antennas have been tested for use with the Viper. Similar antenna types from other manufacturers may be equally acceptable. It is important to follow the manufacturer's recommended installation procedures and instructions when mounting any antenna.

Table 11 Antenna Types

Omni (Vertical Collinear)	Yagi	Vertical Dipole
		

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 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 three or four, 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.

2.5.3. 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 the following table for feedline recommendations

Table 12 Transmission Loss (per 100 Feet)

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

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

2.5.4. RF EXPOSURE COMPLIANCE REQUIREMENTS

RF Exposure

Viper SC+ radios are intended for use in the Industrial Monitoring and Control and SCADA markets. Each 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.

Minimum Safety Distance	Antenna Gain		
(cm @max power)	**5 dBi**	**10 dBi**	**15 dBi**
132 MHz (VHF)	123 cm	219 cm	389 cm
215 MHz (UHF)	122 cm	218 cm	388 cm
406.1 MHz	106 cm	188 cm	334 cm

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

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

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.

Exigences de conformité d'exposition aux Radiofréquences

Exposition aux Radiofréquences

La radio Viper SC+ est destinée à être utilisé dans les marchés contrôles industriels et SCADA. L'unité Viper SC+ doit être installée par un professionnel et doit assurer une distance minimale de séparation entre les sources radiantes et toute personne. Les distances sont indiquées dans le tableau ci-dessous. L'installation typique est une antenne de type fouet 1/2-longueur d'onde installée sur un poteau ou pylône.

Distance de sécurité minimum	Gain de Antenne		
(puissance cm @ max)	**5 dBi**	**10 dBi**	**15 dBi**
132 MHz (VHF)	123 cm	219 cm	389 cm
215 MHz (UHF)	123 cm	219 cm	389 cm
406.1 MHz	106 cm	188 cm	334 cm

Note: *Il est de la responsabilité de l'utilisateur de garantir le respect des règlements MPE de la FCC lorsque vous utilisez cet appareil d'une façon autre que celle décrite ci-dessus. L'installateur doit s'assurer que l'antenne est située ou orientée de façon à ne pas émettre un champ RF dépassant les limites de radiations pour la population générale établies par Santé Canada.*

La radio Viper SC+ utilise un émetteur à radiofréquence à faible puissance. L'énergie concentrée d'une antenne peut poser un risque pour la santé. On ne devrait pas être en face de l'antenne lorsque l'émetteur est en marche.

Les consignes de sécurité recommandées pour l'exposition humaine à l'énergie électromagnétiques de radiofréquences sont contenues dans le Code 6 canadien de la sécurité (disponible auprès de Santé Canada), la Commission Communications Fédéral (FCC) Bulletin 65 et la recommandation du 12 Juillet 1999 sur la limitation de l'exposition du public aux champs électromagnétiques (de 0 Hz à 300 GHz) (1999/519/CE) du Conseil de l'Union européenne.

2.6. 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. NextGen RF recommends a 20 dB fade margin for most projects. The following table shows the RSSI versus Reliability.

Table 13 RSSI Reliability

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

2.7. 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 considered 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 NextGen RF sales representative or NextGen RF Technical Services for additional options. The Technical Services group has qualified personnel to help resolve your RF issues.

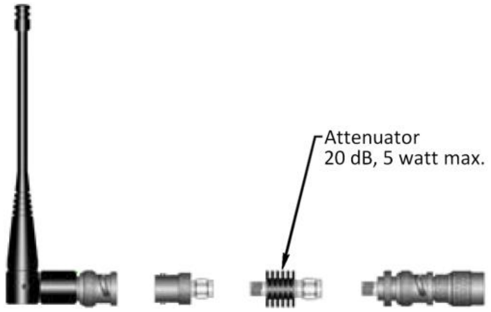
3. GETTING STARTED: QUICK SETUP AND INITIAL CONFIGURATION

These instructions allow you to setup a Viper SC+ so you will be able to verify basic unit operation and experiment with network designs and configurations. To eliminate unnecessary disruption of traffic on the existing network while you become familiar with the Viper SC+, you should use a network IP subnet address that does not overlap with subnets currently in use in your test area.

3.1. INSTALL THE ANTENNA

An Rx/Tx antenna is required for basic operation. For demo units only, connect the antennas as shown in the following figure to provide stable radio communications between demo devices.

Figure – 16 Demo Antenna Assembly



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

3.2. MEASURE PRIMARY POWER

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

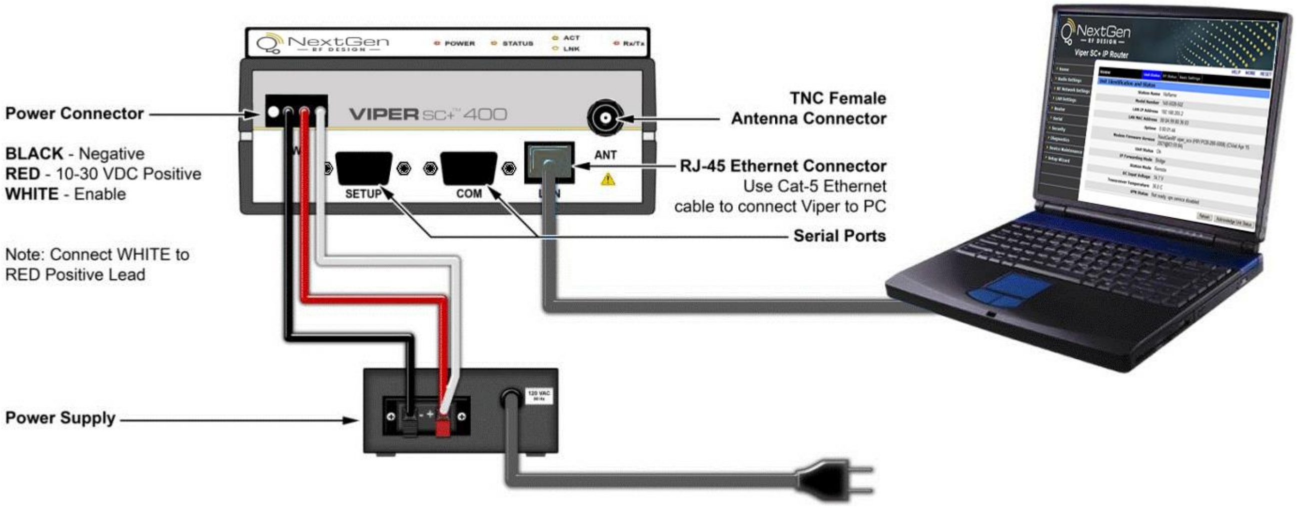
- 10 W supply for Tx at 1 W
- 40 W supply for Tx at 5 W, or
- 60 W supply for Tx at 10 W

Viper SC+ Demo kits include a power supply with spring terminals. Observe proper polarity when connecting the cables to the power supply. *The white wire must be connected to the red wire or B+ supply.* See the following figure.

3.3. CONNECT THE VIPER SC+ TO PROGRAMMING PC

Connect an Ethernet cable into the LAN port of the Viper SC+ and plug the other end into the Ethernet port of your PC.

Figure 17 – Viper SC+ cable connections

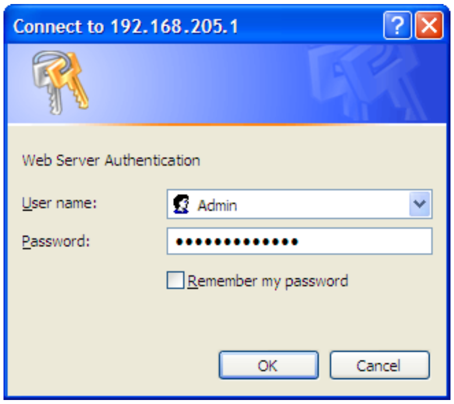


3.4. LAN CONFIGURATION

The Viper SC+ contains a DHCP server which will automatically assign an IP address to your computer, however in some cases it may be necessary to change the network settings on your computer to accept the IP address assigned by the Viper SC+. Before powering on the unit, confirm that your computer's Ethernet port is set up to receive an IP address from an external DHCP server rather than using a static address. Refer to the relevant operating system documentation for details on configuring your computer to use DHCP

3.5. LOG IN

After you have connected your PC to the Viper SC+ by Ethernet cable and powered the Viper SC+, start your Web browser and enter **192.168.205.1** in the address bar. A connection Login window (or Web Server Authentication Window or Web Security window) like one of the following appears.



Connect to 192.168.205.1

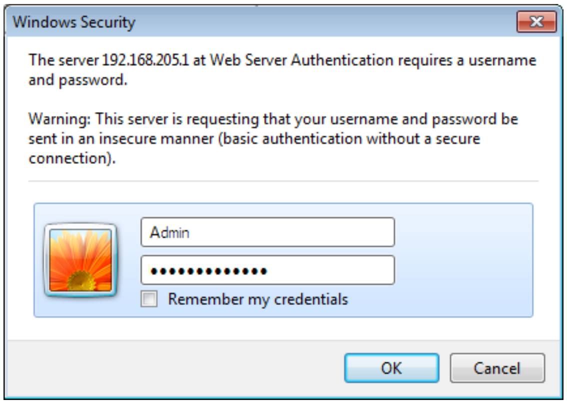
Web Server Authentication

User name: Admin

Password: ••••••••••••••

□ Remember my password

or



Windows Security

The server 192.168.205.1 at Web Server Authentication requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

Admin

•••••••••••••

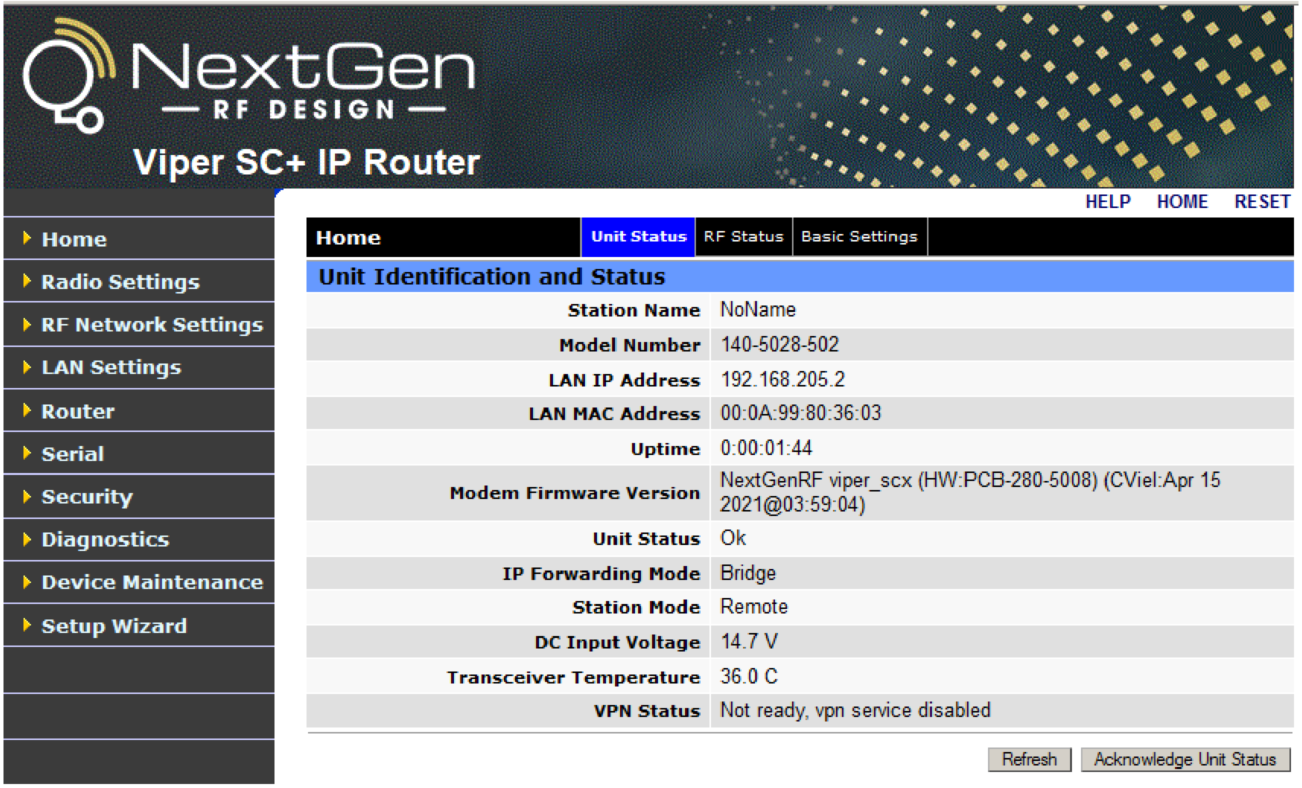
□ Remember my credentials

Enter a username and password. The default username and password the Viper SC+ ship with are **Admin** and **ADMINISTRATOR** (both Admin and ADMINISTRATOR are case-sensitive—enter in all capital letters) and click **OK**.

3.6. INTRODUCTION TO THE VIPER SC+ WEB INTERFACE

All operating parameters of the Viper SC+ are set through a web interface in your web browser once you have logged in. The built-in web server of the Viper SC+ makes configuration possible from any computer with network access to the Viper. The following figure shows the Home page of the Viper Web Interface.

Figure 18 –NextGen RF Viper SC+ IP Router Web Interface home page



Unit Identification and Status

Station Name	NoName
Model Number	140-5028-502
LAN IP Address	192.168.205.2
LAN MAC Address	00:0A:99:80:36:03
Uptime	0:00:01:44
Modem Firmware Version	NextGenRF viper_scx (HW:PCB-280-5008) (CViel:Apr 15 2021@03:59:04)
Unit Status	Ok
IP Forwarding Mode	Bridge
Station Mode	Remote
DC Input Voltage	14.7 V
Transceiver Temperature	36.0 C
VPN Status	Not ready, vpn service disabled

The first time you log in to the Viper SC+ if no configuration changes have been made to the unit from the factory, you will see a message instructing you to Change default settings (Use the Set-Up Wizard).

Note: If the computer you are using has previously been used to set up a NextGen RF router, you may need to delete browser history (specifically temporary internet files) for some pages of the web interface to display correctly.

The Viper SC+ IP Router Web interface is divided into two sections. In the left pane is the main navigation menu. On the right is the content area for the page.

The navigation menu on the left allows you to navigate to configuration pages for the Viper SC+ Router. For quick setup of a few key parameters, select **Setup Wizard** at the bottom of the main menu. The remainder of this chapter will take you through configuration pages of the Setup Wizard. More advanced information about parameters available for selection and configuration in all the tabbed pages is provided in the following chapter.

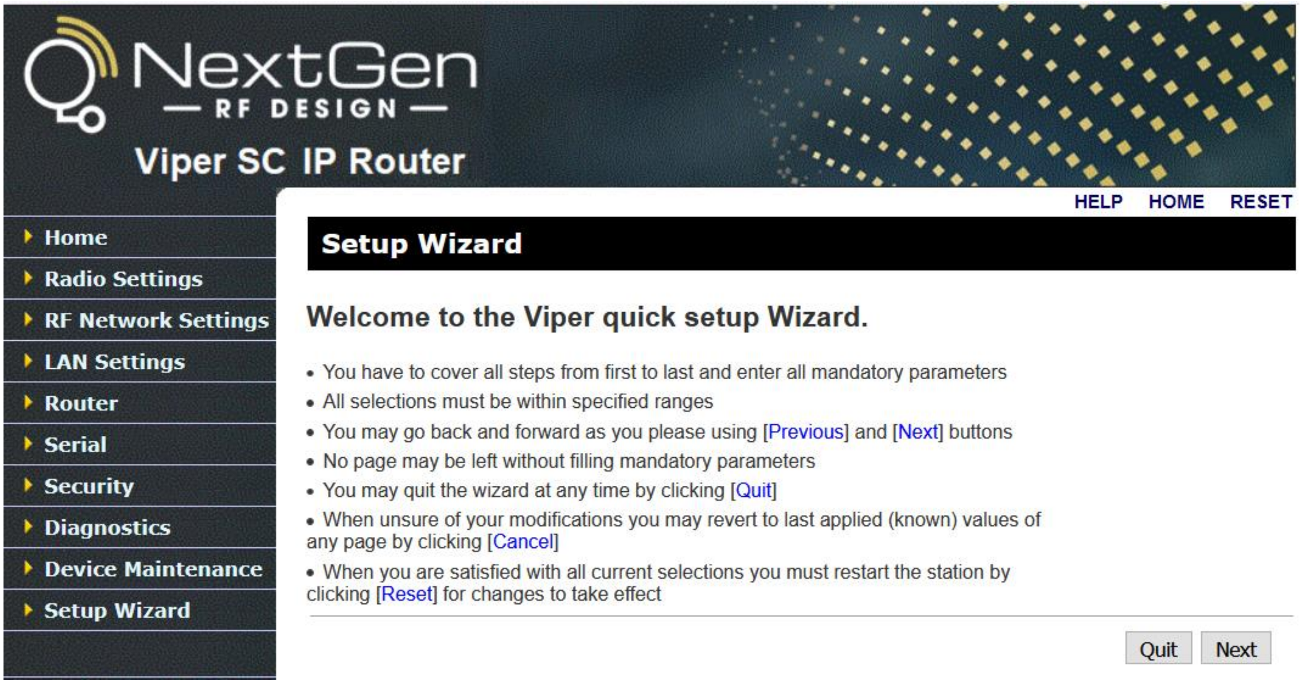
- To access online Help for content of a specific tab in the Viper Web Interface, click the **Help** link (near the top of the page) while in the tab.
- To return to the Home page Unit Status tab from any tab in the Viper Web Interface, click the **Home** link.

For some settings, a reset of the Viper is required before the setting will take effect. These settings are indicated by a yellow alert symbol (⚠).

3.7. INITIAL CONFIGURATION USING THE SETUP WIZARD

The first page of the Setup Wizard displays navigation information for the wizard

Figure 19 – Setup Wizard Welcome and Instructions



Setup Wizard

Welcome to the Viper quick setup Wizard.

- You have to cover all steps from first to last and enter all mandatory parameters
- All selections must be within specified ranges
- You may go back and forward as you please using [Previous] and [Next] buttons
- No page may be left without filling mandatory parameters
- You may quit the wizard at any time by clicking [Quit]
- When unsure of your modifications you may revert to last applied (known) values of any page by clicking [Cancel]
- When you are satisfied with all current selections you must restart the station by clicking [Reset] for changes to take effect

The Setup Wizard consists of five (5) steps. Each step is presented as a single page with a few simple options to fill in or select. Each of the five pages for each step of the Setup Wizard that follow contain the basic configuration settings that are most required to select or change to set up the Viper SC+ IP router for specific functionality.

The steps are as follows.

Step 1: Station Name and Mode settings: Station Name, IP Forwarding Mode, Relay Point, Access Point, and Multi-Speed Mode.

Step 2: Network IP settings: IP Address, Network Mask, and Default Gateway.

Step 3: Radio Setup: Bandwidth, Data and Control Packet Bit Rate, Rx and Tx Frequency ranges, and Tx Power.

Step 4: Encryption: Enable or Disable, and Encryption Pass Phrase.

Step 5: Setup completion and Viper reset.

Instructions for each of these steps are provided on the following pages.

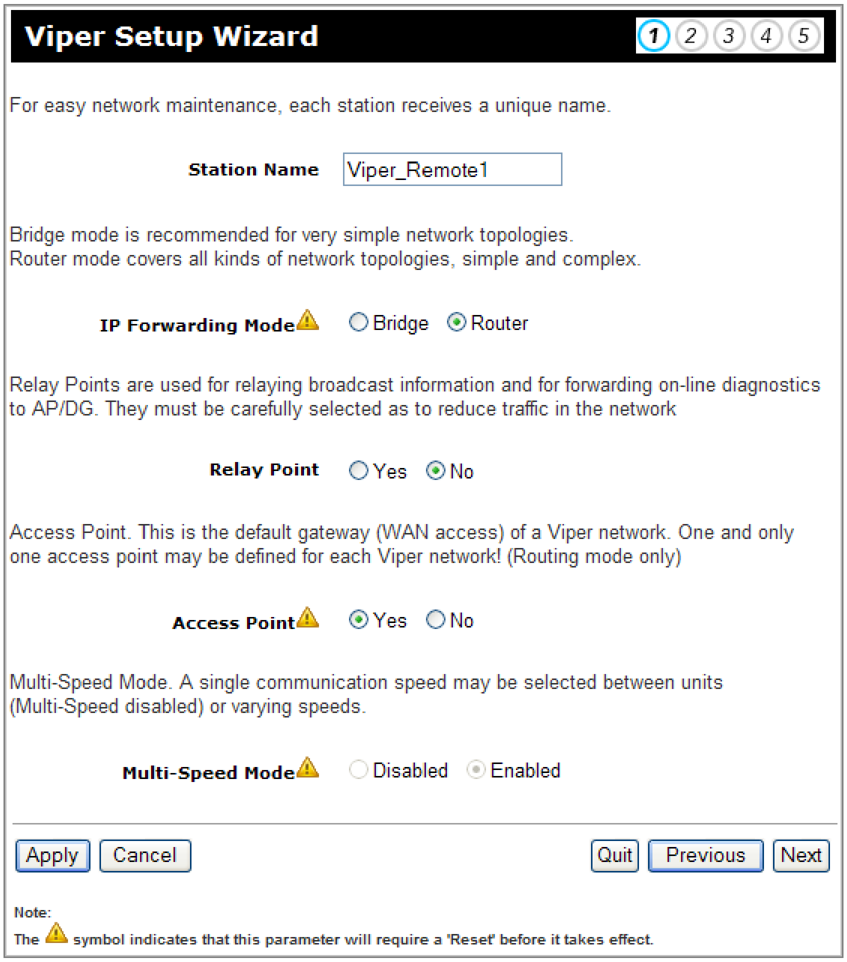
Note: some settings (indicated by a yellow alert symbol ⚠) in the Viper Setup Wizard, require a reset of the Viper before they will take effect. When you have finished with the Viper Setup Wizard, it will be necessary to reset the Viper to restart with the new configuration settings made in the Setup Wizard.

When you have read the information provided on the Welcome page carefully, click **Quit** to exit or click **Next** to proceed to Step 1 on the following page.

3.7.1. SETUP WIZARD STEP 1: STATION NAME AND MODE SETTINGS

The page for Step 1 of the Viper Setup Wizard allows you to set the Station Name, the IP Forwarding Mode, whether the Viper will function as a Relay Point, an Access Point, and whether Multi-Speed Mode will be enabled.

Figure 20 – Viper Setup Wizard Step 1



For easy network maintenance, each station receives a unique name.

Station Name Viper_Remote1

Bridge mode is recommended for very simple network topologies.
Router mode covers all kinds of network topologies, simple and complex.

IP Forwarding Mode⚠ ○ Bridge ● Router

Relay Points are used for relaying broadcast information and for forwarding on-line diagnostics to AP/DG. They must be carefully selected as to reduce traffic in the network

Relay Point ○ Yes ● No

Access Point. This is the default gateway (WAN access) of a Viper network. One and only one access point may be defined for each Viper network! (Routing mode only)

Access Point⚠ ● Yes ○ No

Multi-Speed Mode. A single communication speed may be selected between units (Multi-Speed disabled) or varying speeds.

Multi-Speed Mode⚠ ○ Disabled ● Enabled

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

Enter a Station Name, up to forty (40) characters in length. This should be a name that is unique (different from the names assigned to other units) on the network.

Select the IP Forwarding Mode. The Mode may be set as either Bridge or Router.

- Bridge mode is recommended for simple network topologies.
- Router mode covers network topologies from simple to complex.

The default IP Forwarding Mode is Bridge mode.

Select whether this Viper will function as a relay point. Relay points are used for relaying broadcast information and for forwarding online diagnostics to Access Point or(AP) or Default Gateway (DG). Relay points must be selected carefully to reduce traffic in the network. The default setting is No (not a relay point).

Select whether this Viper will function as an Access Point. This is the default gateway (for WAN access) of a Viper network. One and only one access point may be defined for each Viper network. The default setting is No.

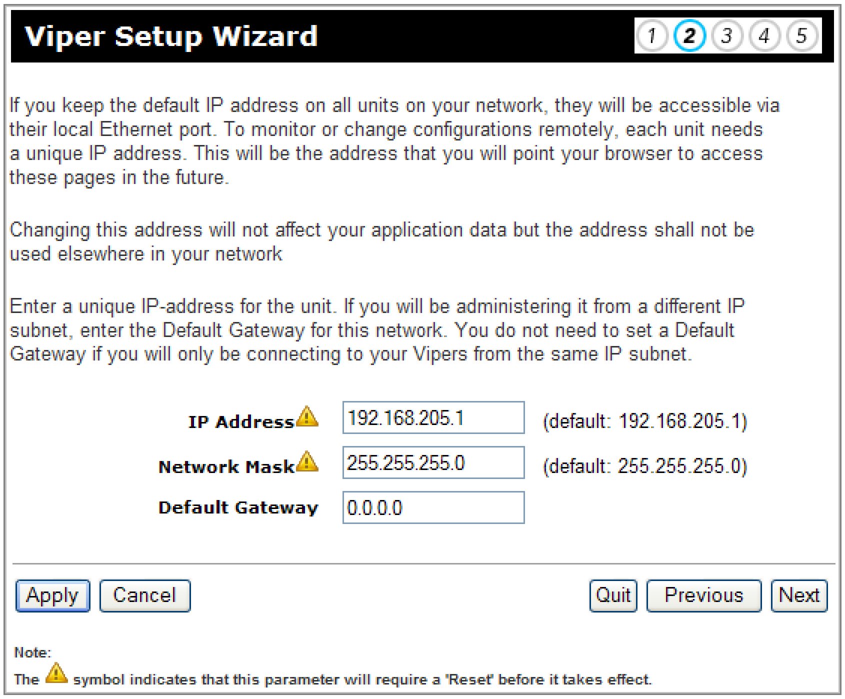
Select whether multi-speed mode will be enabled or disabled for the Viper router. The default setting is Enabled.

Click **Apply** to save any settings you have made in this page and then click **Next** to proceed to step 2 on the following page.

3.7.2. SETUP WIZARD STEP 2: NETWORK IP SETTINGS

The page for Step 2 of the Viper Setup Wizard allows you to set the IP address, Network Mask, and Default Gateway for the Viper.

Figure 21 – Viper Setup Wizard Step 2



Viper Setup Wizard

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 ⚠	192.168.205.1	(default: 192.168.205.1)
Network Mask ⚠	255.255.255.0	(default: 255.255.255.0)
Default Gateway	0.0.0.0	

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

Enter an IP Address, Network Mask, and Default Gate way for the Viper if applicable.

- The default IP Address is 192.168.205.1.
- The default Network Mask is 255.255.255.0.
- The Default Gateway is 0.0.0.0

There are several important considerations to be aware of for these settings in addition to the explanation on the page. Each Viper should be configured with a unique IP address. (If you are in the habit of taking the default settings on each page, they will all have the same address of 192.168.205.1.) The Network Mask determines whether units are configured to be on the same subnet. If the subnet has a Default Gateway, its IP address should be entered in the field provided. Note: Once you have changed the IP Address and applied the setting, and after you have **reset** the Viper to make it take effect, you will need to enter this *new* IP address in your browser Address Bar to access the web interface of the Viper.

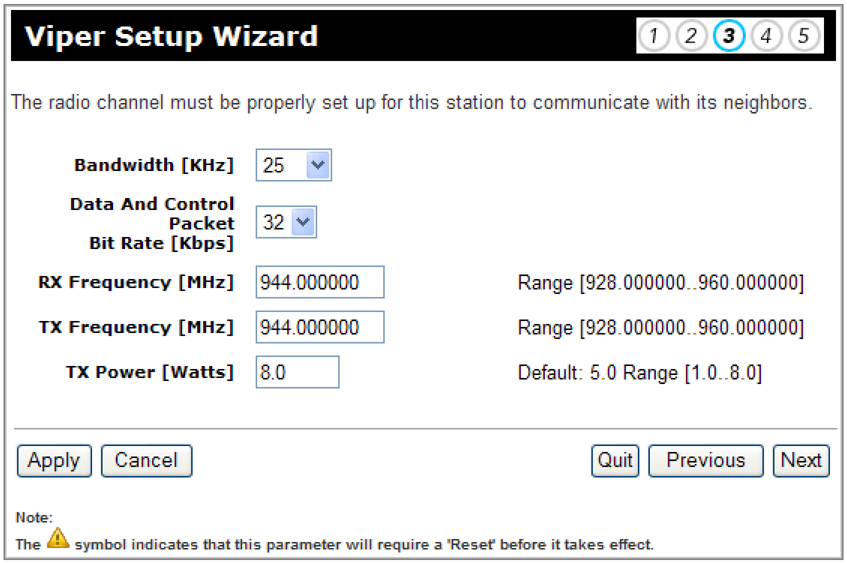
When finished, click **Apply** to save any settings you have made in this page and then click **Next** to proceed to Step 3 on the following page.

Note: If you change the IP Address and the Viper is reset, you will need to change the IP Address in your browser's Address bar to this address (and enter your username and password) to access this Viper.

3.7.3. SETUP WIZARD STEP 3: RADIO SETUP

The page for Step 3 of the Viper Setup Wizard allows you to set basic radio parameters for the Viper. Settings include the radio bandwidth (in kilohertz), Data and Control Packet Bit Rate (in kilobits per second, or kbps), Receive Frequency and Transmit Frequency (in megahertz), and Transmit power (in Watts).

Figure 22 – Viper Setup Wizard Step 3

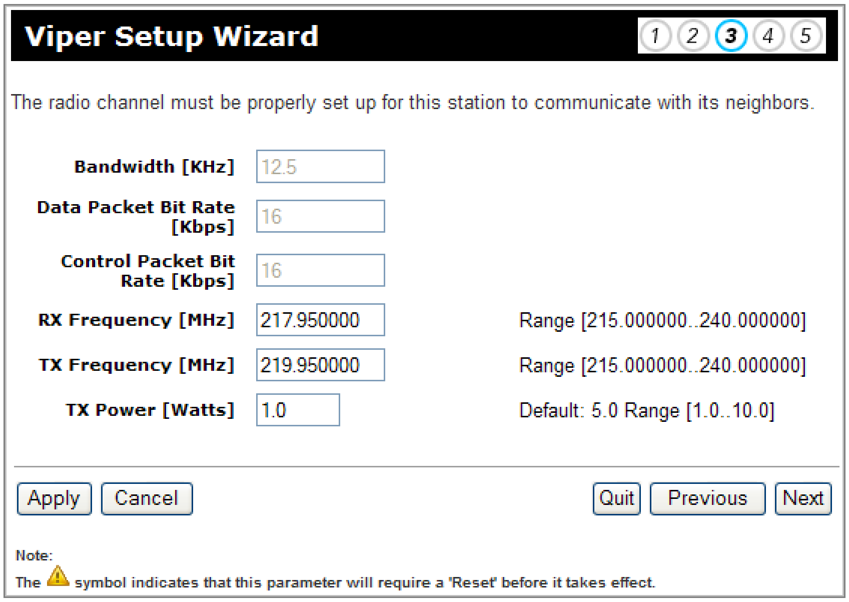


Viper Setup Wizard

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

Bandwidth [KHz]	25	
Data And Control Packet Bit Rate [Kbps]	32	
RX Frequency [MHz]	944.000000	Range [928.000000..960.000000]
TX Frequency [MHz]	944.000000	Range [928.000000..960.000000]
TX Power [Watts]	8.0	Default: 5.0 Range [1.0..8.0]

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



Viper Setup Wizard

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

Bandwidth [KHz]	12.5	
Data Packet Bit Rate [Kbps]	16	
Control Packet Bit Rate [Kbps]	16	
RX Frequency [MHz]	217.950000	Range [215.000000..240.000000]
TX Frequency [MHz]	219.950000	Range [215.000000..240.000000]
TX Power [Watts]	1.0	Default: 5.0 Range [1.0..10.0]

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

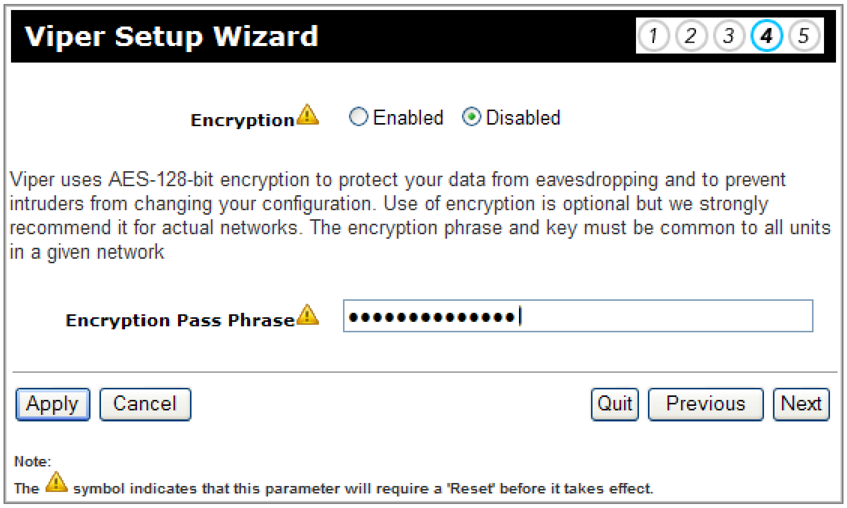
Default settings for this page vary by Viper model and organization that determines compliance for the country or geographical area in which it is operated. These factors typically determine available frequency range, bandwidth, and transmit power. Refer to RF Exposure Compliance Requirements and the frequency range specified for the model number in the . Selecting a frequency range or transmit power that is out of compliance (in the country where used) could void the user’s authority to operate the equipment.

When finished, click **Apply** to save any settings you have made in this page and then click **Next** to proceed to Step 4 on the following page.

3.7.4. SETUP WIZARD STEP 4: ENCRYPTION

The page for Step 4 of the Viper Setup Wizard allows you to enable or disable encryption. When enabled, 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 pass phrase and key must be common to all units in each network.

Figure 23 – Viper Setup Wizard Step 4



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⚠ ••••••••••••••

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

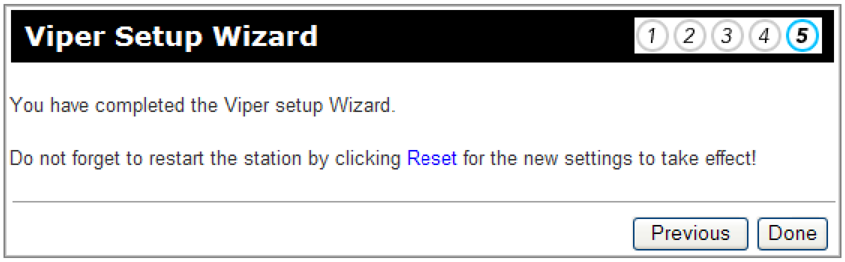
The default setting for encryption is Disabled and Vipers are typically shipped from the factory without an (or with a blank) Encryption Pass Phrase.

When finished, click **Apply** to save any settings you have made in this page and then click **Next** to proceed to the Step 5 on the final page of the Viper Setup Wizard.

3.7.5. SETUP WIZARD STEP 5: COMPLETION AND RESET

The final page, for Step 5 of the Viper Setup Wizard informs you that you have completed the Viper Setup Wizard.

Figure 24 – Viper Setup Wizard Step 5



You have completed the Viper setup Wizard.

Do not forget to restart the station by clicking Reset for the new settings to take effect!

You may use the Previous button to return to previous pages of the Setup Wizard to review configuration settings, but some changed settings will not take effect unless the Viper is reset (powered down and restarted). Click the Reset link to reset the Viper router or click **Done** and then reset the Viper router.

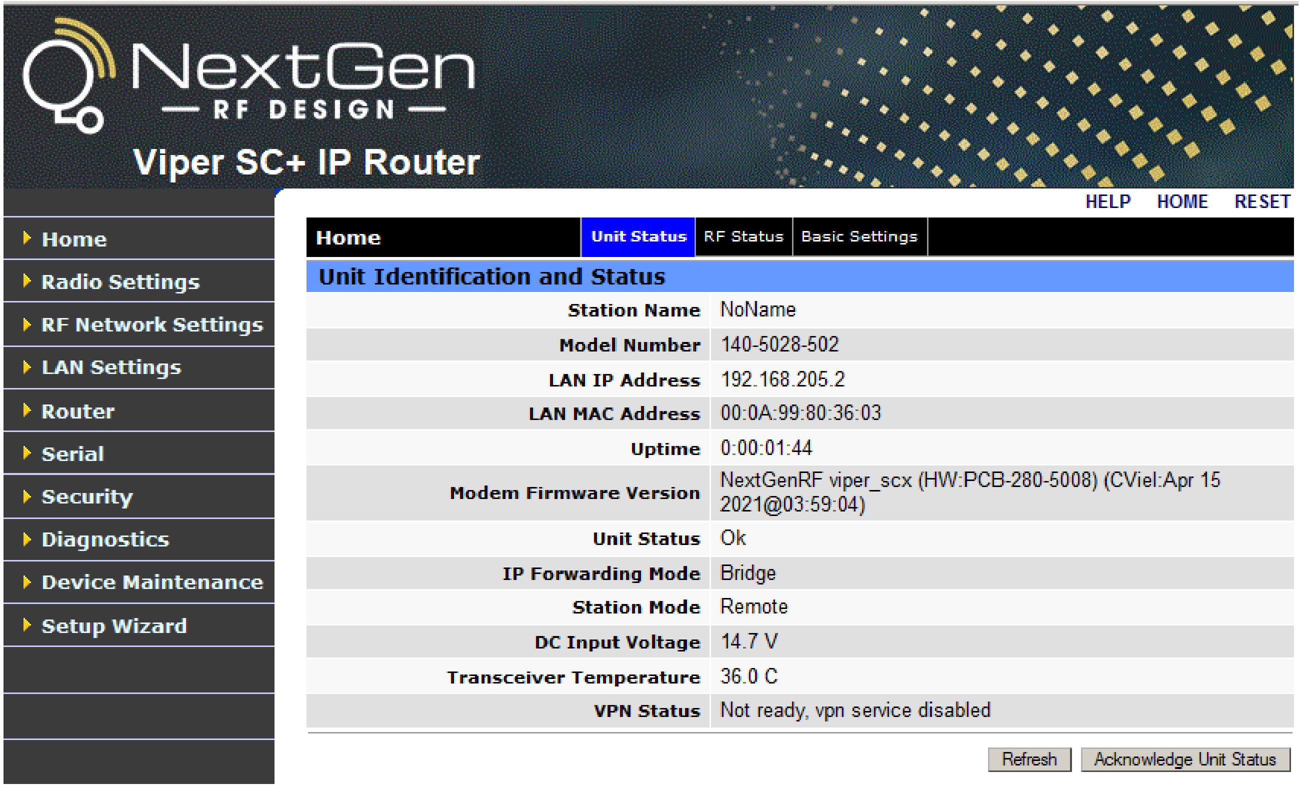
Some settings (indicated by a yellow alert symbol ⚠) made on earlier pages of the Viper Setup Wizard, require a reset of the Viper before they will take effect. Click Reset at this time to reset the Viper to restart with the configuration settings made in the Setup Wizard.

4. VIPER SC+ WEB INTERFACE

All operating parameters of the Viper SC+ are set through a web interface in your web browser once you have logged in. The built-in web server of the Viper SC+ makes configuration and status monitoring possible from any computer with network access to the Viper, either locally or remotely.

The Viper SC+ IP Router Web interface is divided into two sections. In the left pane is the main navigation menu. On the right is the content area for each page and displays the parameter settings available for the selected menu item.

Figure 25 – NextGen RF Viper SC+ IP Router Web Interface home page



Unit Identification and Status

Station Name	NoName
Model Number	140-5028-502
LAN IP Address	192.168.205.2
LAN MAC Address	00:0A:99:80:36:03
Uptime	0:00:01:44
Modem Firmware Version	NextGenRF viper_scx (HW:PCB-280-5008) (CViel:Apr 15 2021@03:59:04)
Unit Status	Ok
IP Forwarding Mode	Bridge
Station Mode	Remote
DC Input Voltage	14.7 V
Transceiver Temperature	36.0 C
VPN Status	Not ready, vpn service disabled

The first time you log in to the Viper SC+ if no configuration changes have been made to the unit from the factory, you will see a message instructing you to Change default settings (Use the Set-Up Wizard).

Note: If the computer you are using has previously been used to set up a NextGen RF router, you may need to delete browser history (specifically temporary internet files) for some pages of the web interface to display correctly.

The navigation menu on the left allows you to navigate to configuration pages for the Viper SC+ Router. Settings for the Viper SC+ are arranged by pages. Pages typically contain several tabs, each of which containing status information or configuration settings, which are distributed along the horizontal bar that contains the page label.

The Home page for example, shown in the previous figure, has three tabs: Unit Status, RF Status, and Basic Settings. You can navigate to each tab by clicking the tab label. The current tab, Unit Status in this example, is indicated by the tab label highlighted in blue.

- To access online Help for content of a specific tab in the Viper Web Interface, click the **Help** link (near the top of the page) while in the tab.
- To return to the Home page Unit Status tab from any tab in the Viper Web Interface, click the **Home** link.

- The Viper router can be reset if necessary, by clicking the **Reset** link. You will be asked to confirm that you want to reset the router and the Viper Web Interface will be unavailable until after the Viper powers up.

Any time you change a parameter in a tab, you must confirm the change by clicking the applicable button at the bottom of the web page tab.

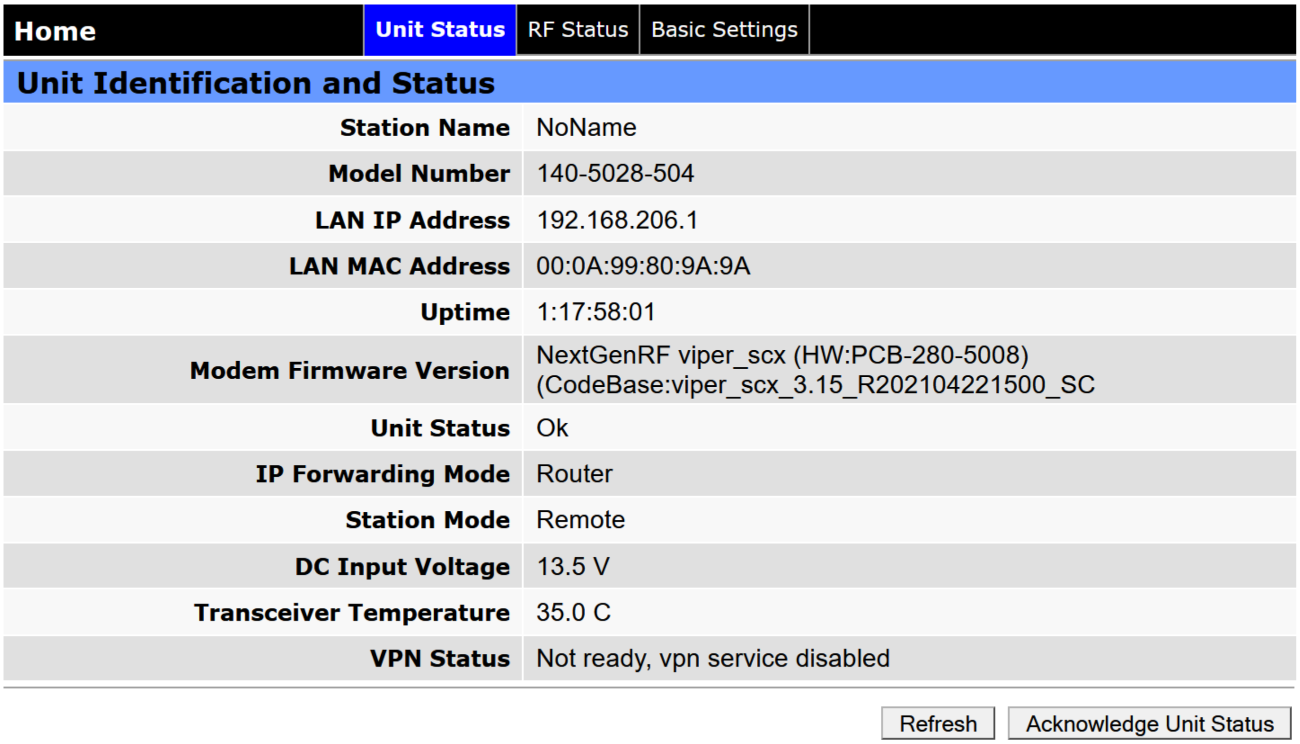
4.1. HOME

The Home page of the Viper Web Interface contains three tabs: Unit Status, RF Status, and Basic Settings.

4.1.1. UNIT STATUS

The Unit Status tab is the first tab displayed when navigating to the Viper Web interface. To return to this tab, select Home from the main navigation menu (or click the Home link at the upper right). From this tab you can view Unit Identification and Status information for the Viper router.

Figure 26 – Home – Unit Status tab



Unit Identification and Status

Station Name	NoName
Model Number	140-5028-504
LAN IP Address	192.168.206.1
LAN MAC Address	00:0A:99:80:9A:9A
Uptime	1:17:58:01
Modem Firmware Version	NextGenRF viper_scx (HW:PCB-280-5008) (CodeBase:viper_scx_3.15_R202104221500_SC
Unit Status	Ok
IP Forwarding Mode	Router
Station Mode	Remote
DC Input Voltage	13.5 V
Transceiver Temperature	35.0 C
VPN Status	Not ready, vpn service disabled

Unit Identification and Status

Station Name: User-defined name given to the unit for ease of reference and used by various services. The Station Name can be configured in the Basic Settings tab.

Model Number: The model or product catalog number of the Viper router.

LAN IP Address: The LAN IP Address assigned to the Viper. LAN IP Address, Network Mask, and Gateway are configured in the LAN Settings tab.

LAN MAC Address: The MAC Address on the Ethernet port of the Viper.

Uptime: The duration in days, hours, minutes, and seconds (DD:HH:MM:SS) that the unit has been powered up and operational since the last reset.

Modem Firmware Version: The version of the firmware currently running on the Viper.

Unit Status: Displays the status of the Viper and reports any errors. Have the content of the displayed Unit Status message available when contacting NextGen RF Technical Support. This information is also required if returning a unit for service under an RMA.

IP Forwarding Mode: Displays the IP Forwarding Mode, whether the Viper is operating as a bridge or router. The IP Forwarding Mode is configured in RF Network Settings » RF Network.

Station Mode: Displays whether the unit is configured to operate as a Relay Point, Access Point, or Remote. The Station Mode is also configured in RF Network Settings » RF Network.

DC Input Voltage: Displays the system input voltage currently seen by the unit.

Transceiver Temperature: Displays the transceiver input temperature. The Viper can be configured to display temperature in Celsius or Fahrenheit in the Basic Settings tab.

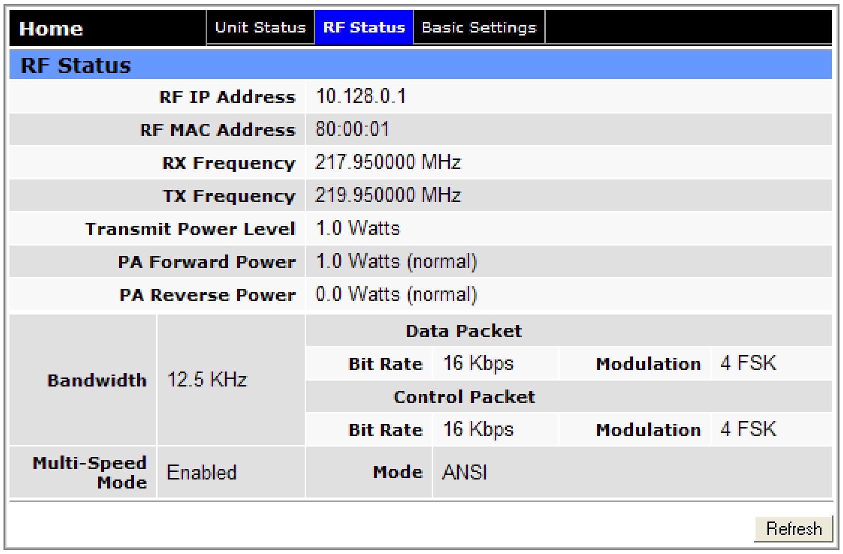
VPN Status: Displays the status of the VPN (Virtual Private Network). When operational will display OK/Ready. If the VPN is not operational, Not Ready and the reason it is not operational will display.

Refresh: Click Refresh to update the information displayed in the current tab.

Acknowledge Unit Status: This button allows you to acknowledge and clear errors. Errors remain stored, even after cycling power, to aid in troubleshooting intermittent faults. Click the Acknowledge Unit Status button to return web page displays and unit Status LED function to normal operation.

The RF Status tab is the second (middle) tab of the Home page of the Viper Web interface. To view this tab, select Home from the main navigation menu (or click Home) and click RF Status. From this tab you can view RF Status information for the Viper router.

Figure 27 – Home – RF Status tab



RF Status

RF IP Address	10.128.0.1
RF MAC Address	80:00:01
RX Frequency	217.950000 MHz
TX Frequency	219.950000 MHz
Transmit Power Level	1.0 Watts
PA Forward Power	1.0 Watts (normal)
PA Reverse Power	0.0 Watts (normal)

Bandwidth	12.5 KHz	Data Packet			
		Bit Rate	16 Kbps	Modulation	4 FSK
		Control Packet			
		Bit Rate	16 Kbps	Modulation	4 FSK
Multi-Speed Mode	Enabled	Mode	ANSI		

RF Status

RF IP Address: The RF IP Address (default is assigned by the factory, based on the unit's MAC address) is the IP address that is used when sending data and control packets in the Viper radio IP network. The RF IP Address can be configured in » RF Network.

RF MAC Address: The MAC address assigned to the Viper radio interface by the factory.

RX Frequency: The operating frequency currently being used for receiving data and control packets.

TX Frequency: The operating frequency currently being used for transmitting data and control packets.

Transmit Power Level: The current transmit power level setting.

PA Forward Power: The transmit power measured during the last transmission.

PA Reverse Power: The reverse power measured during the last transmission.

Bandwidth, Bit Rate, and Modulation: Displays the Bandwidth, and the Bit Rate and Modulation for the configured channel. When applicable, separate Bit Rates and Modulation will be displayed for the Data Packet and Control Packet.

Multi-Speed Mode: When Multi-Speed mode is enabled, the units communicate with each other at a fixed speed. A unit can be set to operate as a Multi-Speed Master or as a Multi-Speed Slave. A unit set to operate in Multi-Speed slave mode matches the speed of the unit set to operate in Multi-Speed Master mode. In a network operating with Multi-Speed, there must be at most one Multi-Speed Master unit and all other units must operate in Multi-Speed Slave mode. The Multi-Speed Mode can be configured in RF Network Settings » RF Network.

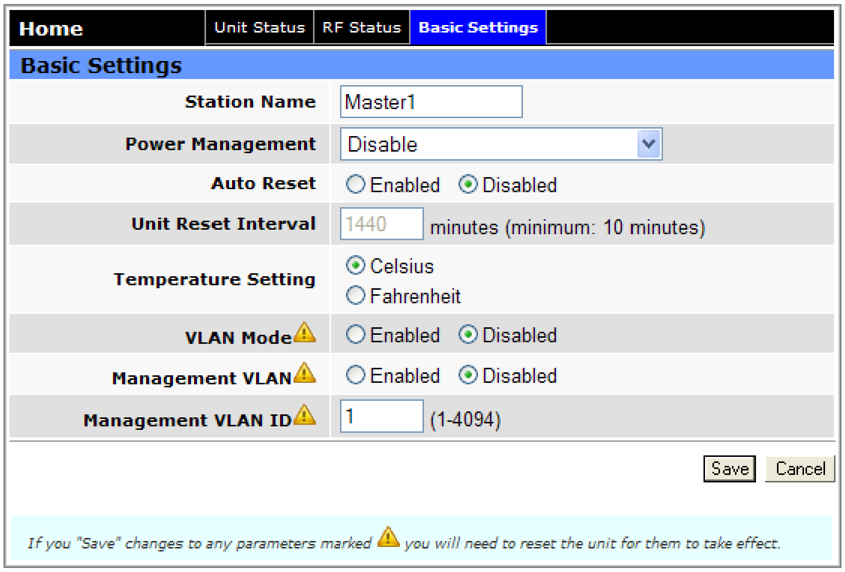
Mode: Indicates the mode of operation (ANSI, ANSI 900, ETSI)

Refresh: Click Refresh to update the information displayed in the current tab.

4.1.2. BASIC SETTINGS

The Basic Settings tab is the third (right-most) tab of the Home page of the Viper Web interface. To navigate to this tab, select Home from the main navigation menu (or click Home) and click Basic Settings. In this tab you can make basic configuration settings in the Viper router.

Figure 28 – Home – Basic Settings



Basic Settings

Station Name	Master1
Power Management	Disable
Auto Reset	○ Enabled ● Disabled
Unit Reset Interval	1440 minutes (minimum: 10 minutes)
Temperature Setting	● Celsius ○ Fahrenheit
VLAN Mode ⚠	○ Enabled ● Disabled
Management VLAN ⚠	○ Enabled ● Disabled
Management VLAN ID ⚠	1 (1-4094)

If you "Save" changes to any parameters marked ⚠ you will need to reset the unit for them to take effect.

Basic Settings

Station Name: This is the user-defined name given to the unit to differentiate it from other units and used by various services. Enter a name up to forty (40) characters in length that is unique (different from the names assigned to other units) on the network.

Power Management: When enabled, power management will allow the unit to go into a low-power mode when the ignition-sense is off (when the white wire is disconnected from the red wire or B+ supply). The default setting is disabled.

Auto Reset: Auto Reset allows you to set a time duration, after which the unit will automatically reset itself. This is disabled by default.

Unit Reset Interval: If Auto Reset is Enabled, enter the number of minutes (after each power up —ten minutes minimum) the unit should be up between resets. The default setting is disabled.

Temperature Setting: Select whether temperature will be reported in degrees Celsius or degrees Fahrenheit on the Unit Status tab of the Home page and in Online Diagnostics messages. The default setting is Celsius.

VLAN Mode: When the VLAN mode is enabled, the Ethernet interface can be configured to operate in "tagged" or "untagged" mode, the RF interface operates in "tagged" mode and the Serial ports operate in "untagged" mode.

> **Untagged:** Devices on this interface are not using VLAN tags. Incoming (ingress) packets are tagged with the port VLAN ID (PVID). VLAN tags are removed on outgoing (egress) packets.
>
> **Tagged:** Devices on this interface are using VLAN tags. Incoming (ingress) packets are forwarded with their VLAN ID. Outgoing (egress) packets keep their VLAN tags.
>
> See configuration tabs for each interface for more specific VLAN configuration options.

Management VLAN: When Management VLAN is enabled, access to the unit will be allowed only through the Management VLAN ID.

Management VLAN ID: The ID is a value from 1 to 4094, inclusive.

Save: Click Save to save any changes you have made in this tab. See Note below.

Cancel: Click Cancel to cancel any changes you may have made to any of the settings in this tab.

Note: If you change the VLAN Mode, Management VLAN, or Management VLAN ID setting in this tab, as indicated by the yellow alert symbol (⚠), a reset of the Viper is required before the setting will take effect.

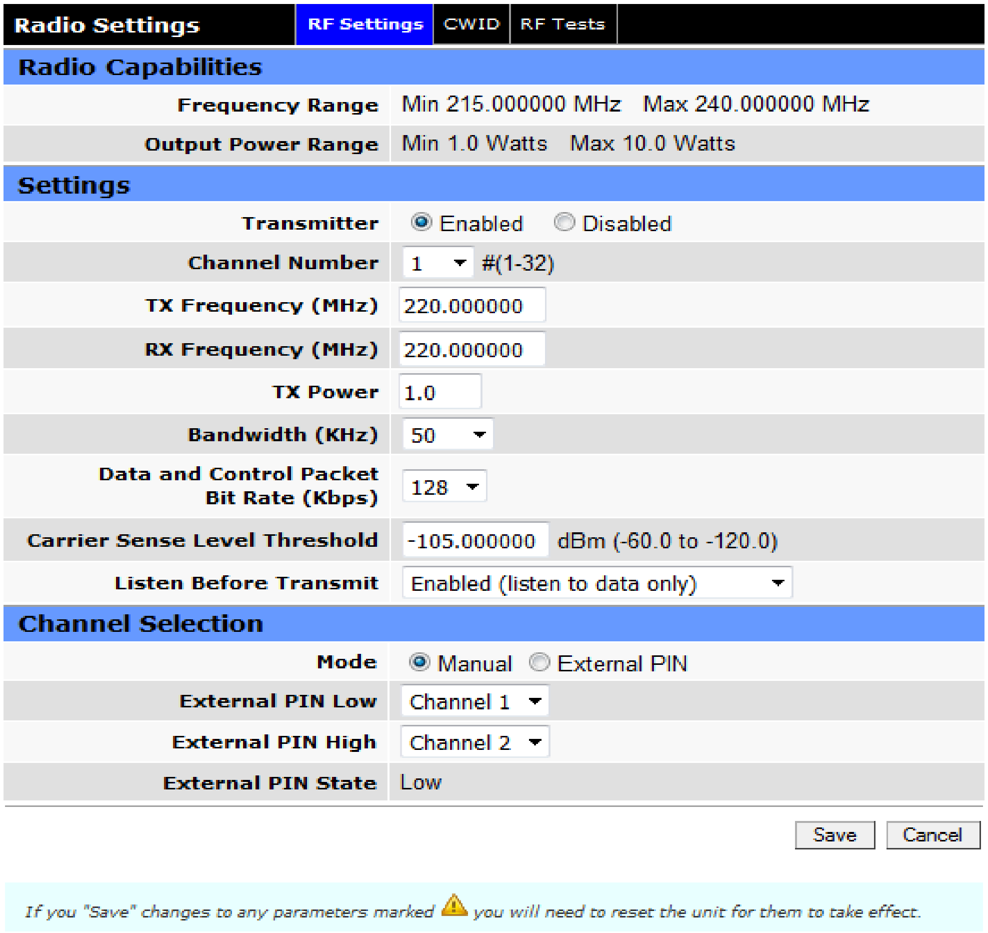
4.2. RADIO SETTINGS

The Radio Settings page contains three tabs: RF Settings, CWID, and RF Tests.

4.2.1. RF SETTINGS

RF Settings is the first (left-most) tab of the Radio Settings page. To navigate to this tab, select Radio Settings from the main menu. In this tab, you can view the Radio Capabilities and configure the channel number, frequency range for transmit and receive, bandwidth, transmit power, and other settings that determine how the radio will communicate.

Figure 29 – Radio Settings – RF Settings



Radio Capabilities	
Frequency Range	Min 215.000000 MHz Max 240.000000 MHz
Output Power Range	Min 1.0 Watts Max 10.0 Watts
Settings	
Transmitter	● Enabled ○ Disabled
Channel Number	1 #(1-32)
TX Frequency (MHz)	220.000000
RX Frequency (MHz)	220.000000
TX Power	1.0
Bandwidth (KHz)	50
Data and Control Packet Bit Rate (Kbps)	128
Carrier Sense Level Threshold	-105.000000 dBm (-60.0 to -120.0)
Listen Before Transmit	Enabled (listen to data only)
Channel Selection	
Mode	● Manual ○ External PIN
External PIN Low	Channel 1
External PIN High	Channel 2
External PIN State	Low

If you "Save" changes to any parameters marked ⚠ you will need to reset the unit for them to take effect.

Radio Capabilities

Frequency Range and Output Power Range

Frequency Range and Output Power Range are factory set and vary as determined by Viper model or product catalog number and the organization determining compliance for the country or geographical area in which the Viper is to be operated.

- 140-5018-502: VHF, 136.000-174.000 MHz, 6.25 - 50 kHz bandwidth, 1-10 W
- 140-5018-503: VHF, 136.000-174.000 MHz, 6.25 - 50 kHz bandwidth, 1-10 W – Dual RF Ports
- 140-5028-504: VHF, 215.000-240.000 MHz, 6.25 - 100 kHz bandwidth, 1-10 W
- 140-5028-505: VHF, 215.000-240.000 MHz, 6.25 - 100 kHz bandwidth, 1-10 W – Dual RF Ports
- 140-5048-302: UHF Range 3, 406.1125-470.000 MHz, 6.25 - 50 kHz bandwidth, 1-10 W
- 140-5048-303: UHF Range 3, 406.1125-470.000 MHz, 6.25 - 50 kHz bandwidth, 1-10 W – Dual RF Ports
- 140-5048-502: UHF Range 5, 450.000-511.975 MHz, 6.25 - 50 kHz bandwidth, 1-10 W
- 140-5048-503: UHF Range 5, 450.000-511.975 MHz, 6.25 - 50 kHz bandwidth, 1-10 W – Dual RF Ports

European, Australian, and New Zealand Compliant Models (ETSI AS/NZ)

- 140-5018-600: VHF, 142.000-174.000 MHz, 6.25 - 50 kHz bandwidth, 1-10 W
- 140-5048-601: VHF, 142.000-174.000 MHz, 6.25 - 50 kHz bandwidth, 1-10 W – Dual RF Ports
- 140-5048-400: UHF Range 3, 406.1125-470.000 MHz, 6.25 - 50 kHz bandwidth, 1-10 W
- 140-5048-401: UHF Range 3, 406.1125-470.000 MHz, 6.25 - 50 kHz bandwidth, 1-10 W – Dual RF Ports
- 140-5048-600: UHF Range 5, 450.000-511.975 MHz, 6.25 - 50 kHz bandwidth, 1-10 W
- 140-5048-601: UHF Range 5, 450.000-511.975 MHz, 6.25 - 50 kHz bandwidth, 1-10 W – Dual RF Ports

Note: *It is the user's responsibility of the user to check his or her FCC license or applicable regulatory agency for the country or geographical area in which the Viper will be operated to determine the correct parameters and settings for the channel frequencies, power level and bandwidth. Selecting a frequency range or transmit power that is out of compliance (in the country where used) could void the user's authority to operate the equipment.*

Settings

Transmitter: The Viper radio transmitter can be enabled or disabled. The factory default setting is Disabled, to disable the radio transmitter until the Viper is minimally configured. (Until the Setup Wizard is successfully completed.)

Channel Number: When the Viper Transmitter is Enabled, you may select a channel number. The number of channels available for selection depends on Frequency Range and Bandwidth. Viper supports up to 32 different frequency channel pairs.

Tx Frequency (MHz), **RX Frequency** (MHz), and **Tx Power:** The Viper can operate in simplex (same Tx and Rx frequency) or half-duplex (Tx and Rx frequencies are different) mode. All Vipers in a radio network must be set the same. The Tx Power setting allows you to increase or decrease the transmit power as required.

Bandwidth (kHz), **Data Packet Bit Rate** (kbps), and **Control Packet Bit Rate** (kbps):These settings are computed from the Channel size and frequency range.

Carrier Sense Level Threshold (dBm):The threshold Viper uses to determine whether a received RF signal is a valid message or unwanted noise. If RF level above the threshold is detected, the 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 radio-noisy environments or lowered to gain extra receive sensitivity. Lower thresholds should only be used when ambient RF noise is low. Receive sensitivity depends on the channel bandwidth and speed being used. Refer to Specifications for the Carrier sense by model. The default setting is -110 dBm.

Listen Before Transmit: The Viper can be configured to listen on the Rx frequency and determines if the RF channel is available. The channel is available as long as the received level is lower than the carrier sense threshold. When the channel is busy, Viper receives and decodes all remote messages. Outgoing data is buffered and sent when the channel becomes available. The default setting is Enabled (listen to data only).

Three options are available for Listen Before Transmit.

- Enabled (listen to noise and data)
- Enabled (listen to data only)
- Disabled

These are explained below.

Enabled (listen to noise and data): In this mode of operation, the Viper acts as a TCP server. It can accept up to 256 TCP connections from remote endpoints. Data received from any remote endpoint is sent over the serial port. Data received from the serial port is sent to every endpoint connected to the TCP server.

Received level is above the carrier sense threshold if:

- The Viper is receiving valid data,
- The Viper is not receiving data because two or more Vipers are transmitting at the same time causing a collision,
- The 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 the Viper is operating on.

Enabled (listen to data only): The Viper will monitor the RF level on the receive channel. When the received level is above the carrier sense threshold, the Viper will try to receive and decode all messages from remove Vipers. When data is ready to transmit, the Viper will first check the receive level. If the receive level is below the carrier sense threshold, the Viper will immediately transmit data. If the receive level is above the carrier threshold, the Viper will try to determine if it is receiving valid data or just noise. If it is receiving noise, the Viper will go ahead and transmit. If it is receiving valid data, the Viper will wait until the complete packet has been received before transmitting. The Viper will typically take 5 to 250 ms to determine if it is receiving data or just noise.

Disabled: The Viper will attempt to receive and decode data when the received RF level is above the carrier sense threshold. When the Viper has data to transmit it will immediately transmit the data. The Viper will immediately stop receiving packets and will transmit over any other Vipers that are on the air and over any interference that may be present. This mode ***should only be used in a polling-type environment*** where the user has strict control over the traffic that is generated.

Save: Click Save to save any changes you have made in this tab. See Note below.

Cancel: Click Cancel to cancel any changes you may have made to any of the settings in this tab.

Note: *It is the user's responsibility of the user to check his or her FCC license or applicable regulatory agency for the country or geographical area in which the Viper will be operated to determine the correct parameters and settings for the channel frequencies, power level and bandwidth. Selecting a frequency range or transmit power that is out of compliance (in the country where used) could void the user's authority to operate the equipment.*

Channel Selection

Mode (Manual): Use the channel selected in the "Settings" section.

Mode (External PIN): Use a channel based on the state of the RI pin of the COM port. When the mode is set to “External PIN”, channel change occurs at startup (to match the state of the PIN at that time) and on every state change of the external PIN.

External PIN Low: Channel number to use when the state of the RI pin is low.

External PIN High: Channel number to use when the state of the RI pin is high.

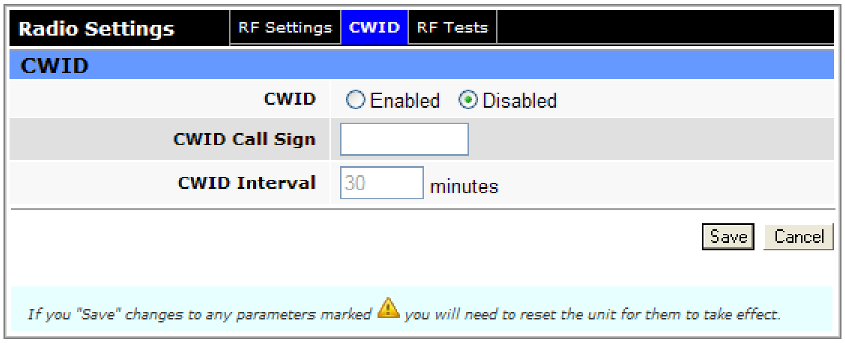
External PIN State: The current state of the external pin.

4.2.2. CWID

CWID is the second (middle) tab of the Radio Settings page. To navigate to this tab, select Radio Settings from the main menu and click CWID. In this tab you can configure the Viper CWID parameters.

Some regulatory agencies require a station identification. The Viper offers a Morse Code (CW) identifier or Continuous Wave Identification (CWID) that will identify the unit on the first transmission and at periodic intervals after that. This tab is used to enable this feature if required and enter the CWID call sign and specify how often it will be broadcast.

Figure 30 – Radio Settings – CWID



CWID

CWID ○ Enabled ● Disabled

CWID Call Sign

CWID Interval 30 minutes

If you "Save" changes to any parameters marked ⚠ you will need to reset the unit for them to take effect.

CWID

CWID: If CWID is enabled, the Viper will broadcast the specified CWID; if disabled, the Viper will not. The default setting is Disabled.

CWID Call Sign: This is the CWID or “call sign” to be broadcast if CWID is enabled.

CWID Interval: This is the time interval, in minutes, after which the CWID will be broadcast.

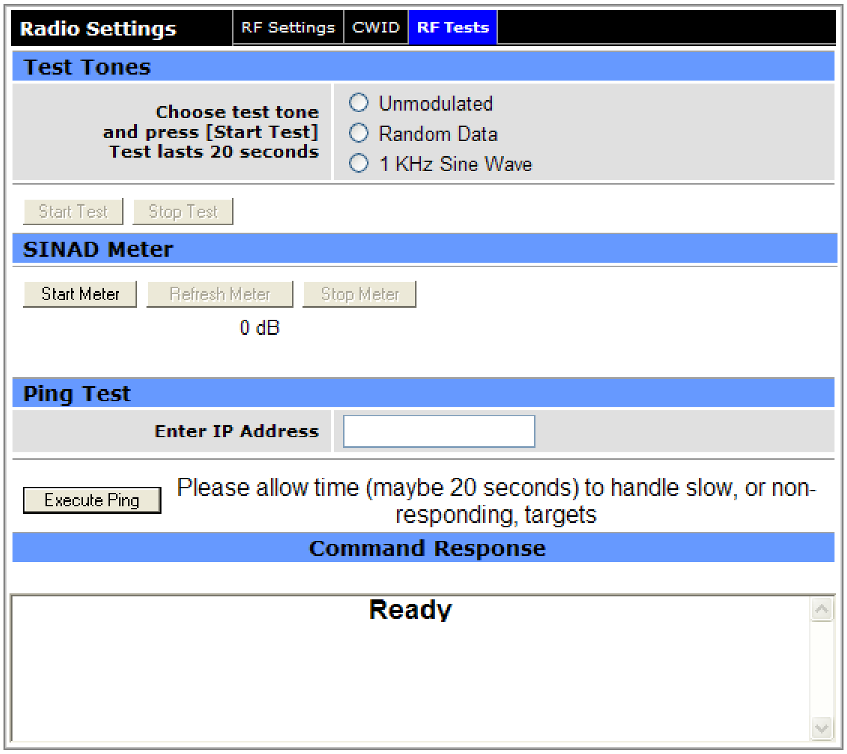
Save: Click Save to save any changes you have made. See Note below.

Cancel: Click Cancel to cancel any changes you may have made to any of the settings in this tab.

4.2.3. RF TESTS

RF Tests is the third (right-most) tab of the Radio Settings page. To navigate to this tab, select Radio Settings from the main menu and click RF Tests. In this tab you can generate and send Test Tones, display the SINAD meter reading, or conduct a Ping Test and Command Response.

Figure 31 – Radio Settings – RF Tests



Choose test tone and press [Start Test] Test lasts 20 seconds

0 dB

Please allow time (maybe 20 seconds) to handle slow, or non-responding, targets

Ready

Test Tones

Note: This test may cause other Vipers to stop transmitting for the duration of the test tone if they have been configured to Listen Before Transmit, since the test tone selected may be noise (Unmodulated or 1 kHz Sine Wave) or data (Random Data).

Test Tones

Allows a tone to be transmitted for testing purposes. The test tone will be transmitted for 20 seconds after the Start Test button is clicked unless the Stop Test button is clicked, which will stop transmitting the test tone. Three test tones are available.

– Unmodulated
– Random Data
– 1 kHz Sine Wave

Only one of these three types of test tone may be transmitted for each test.

Once the type of test tone is selected,

– Click Start Test to start transmitting. The selected tone will be transmitted for 20 seconds
– Click Stop Test if it is necessary to stop transmission of the test tone before 20 seconds.

SINAD Meter

SINAD (Signal to Noise and Distortion 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 is determined by the formula:

SINAD = 10Log (SND/ND)

Where:

SND = combined Signal + Noise + Distortion power level
ND = combined Noise+ Distortion power level
0db ≤ SINAD < 50 dB

The receiver must be fed a 1 kHz tone.

– Click Start Meter to start the SINAD meter. The calculated SINAD value is displayed.
– Click Refresh Meter to refresh the SINAD value calculated by the Meter.
– Click Stop Meter to stop the SINAD meter.

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 (Internet Control Message Protocol) packet (echo request) to a target host and listening for the ICMP echo response. Ping estimates the round-trip time (in milliseconds) and records any packet loss.

Enter IP Address

Enter an IP address in dot-decimal format of the unit to ping. For example, 192.168.205.100.

Execute Ping — Once you have entered an IP address to for the Ping command, click Execute Ping to execute the Ping command. Allow enough time (20 seconds) to handle slow or non-responding targets.

Command Response

If the Ping command executed above was successful, the response times appear in the text box when complete.

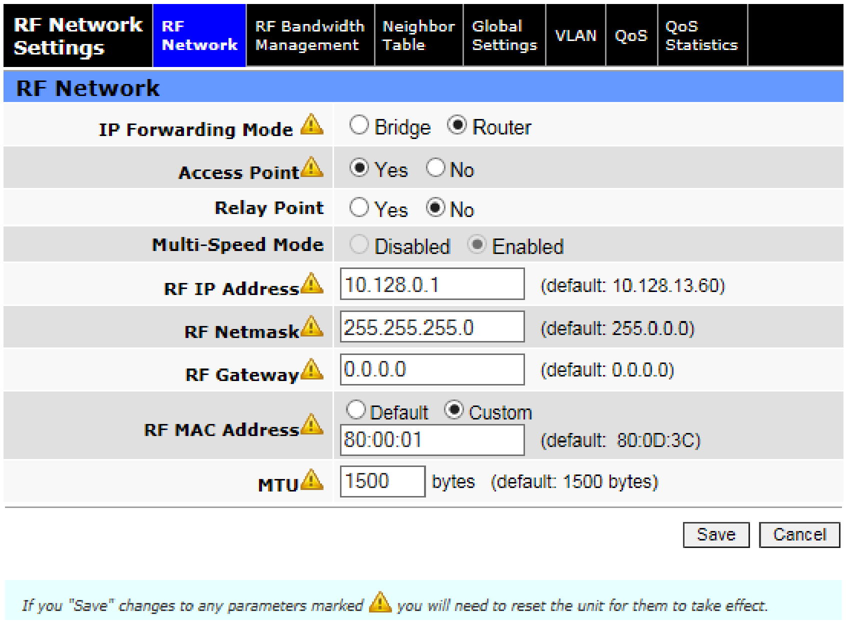
4.3. RF NETWORK SETTINGS

The RF Network Settings page contains seven tabs: RF Network, RF Bandwidth Management, Neighbor Table, Global Settings, VLAN, QoS (for Quality of Service), and QoS Statistics.

4.3.1. RF NETWORK

RF Network is the first (left-most) tab of the RF Network Settings page. To navigate to this tab, select RF Network Settings from the main menu. The RF Network tab allows you to configure settings for the Viper RF network.

Figure 32 – RF Network Settings – RF Network



RF Network

IP Forwarding Mode ⚠	○ Bridge ● Router
Access Point ⚠	● Yes ○ No
Relay Point	○ Yes ● No
Multi-Speed Mode	○ Disabled ● Enabled
RF IP Address ⚠	10.128.0.1 (default: 10.128.13.60)
RF Netmask ⚠	255.255.255.0 (default: 255.0.0.0)
RF Gateway ⚠	0.0.0.0 (default: 0.0.0.0)
RF MAC Address ⚠	○ Default ● Custom 80:00:01 (default: 80:0D:3C)
MTU ⚠	1500 bytes (default: 1500 bytes)

If you "Save" changes to any parameters marked ⚠ you will need to reset the unit for them to take effect.

RF Network

IP Forwarding Mode: Select whether this Viper will operate as a bridge or router. The default setting is Router.

Access Point: Select whether this Viper will be an Access Point. The Access Point is the default gateway (WAN access) of a Viper network. One and only one access point may be defined for each Viper network. All Vipers in the network will set their default route to point to the Access Point. Viper can only be configured as an Access point if it is operating in Router mode. The default setting is No (the Viper will not be operating as an Access Point).

Relay Point: Select whether this Viper will operate as a Relay Point. For Vipers that are spread over multiple RF coverage areas the user needs to identify the units that will form the backbone between the coverage areas so that any unit can talk to any other unit in the network regardless of their locations. The units forming the backbone between the coverage areas are the Relay Point units. Selecting this parameter will force the unit to repeat all necessary information from one coverage area to the next. The default setting is No (the Viper will not be operating as a Relay Point).

Multi-Speed Mode: Select whether Multi-Speed Mode will be disabled or enabled. When Multi-Speed Mode is disabled—the default setting, the units communicate with each other at a fixed data rate (Refer to APPENDIX B for data rates by model). By enabling Multi-Speed Mode, the Viper can be set to operate as a rate follower to match the speed of the Base unit set to operate as the rate-controller. This means the Viper will adjust to the over-the-air data rate to that of the rate-controller. Only Viper Base Station units can be configured as a rate controller.

RF IP Address: The RF IP address is the IP address used when sending data and control packets on the Viper radio network. The default RF IP address will have the form 10.x.y.z, where x, y, and z are based on the last six digits of the unit's Ethernet MAC address.

RF Netmask: Set the RF Netmask to a valid common RF IP netmask for all units on the network. The default is 255.0.0.0.

RF Gateway: Set the RF Gateway to the IP address that will be used to forward packets to outside networks. The default is 0.0.0.0.

RF MAC Address: The RF MAC Address is a shortened version of the Ethernet MAC address which is used to identify the Viper RF interface to other Vipers 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. The default setting is to use the default RF MAC address, displayed in the format DD:EE:FF.

MTU (Maximum Transfer Unit): This value represents the maximum number of bytes the Viper will send in a packet. Enter a value from 576 to 1500. The default value is 1500.

Save: Click Save to save any changes you have made to settings in this tab. See Note below.

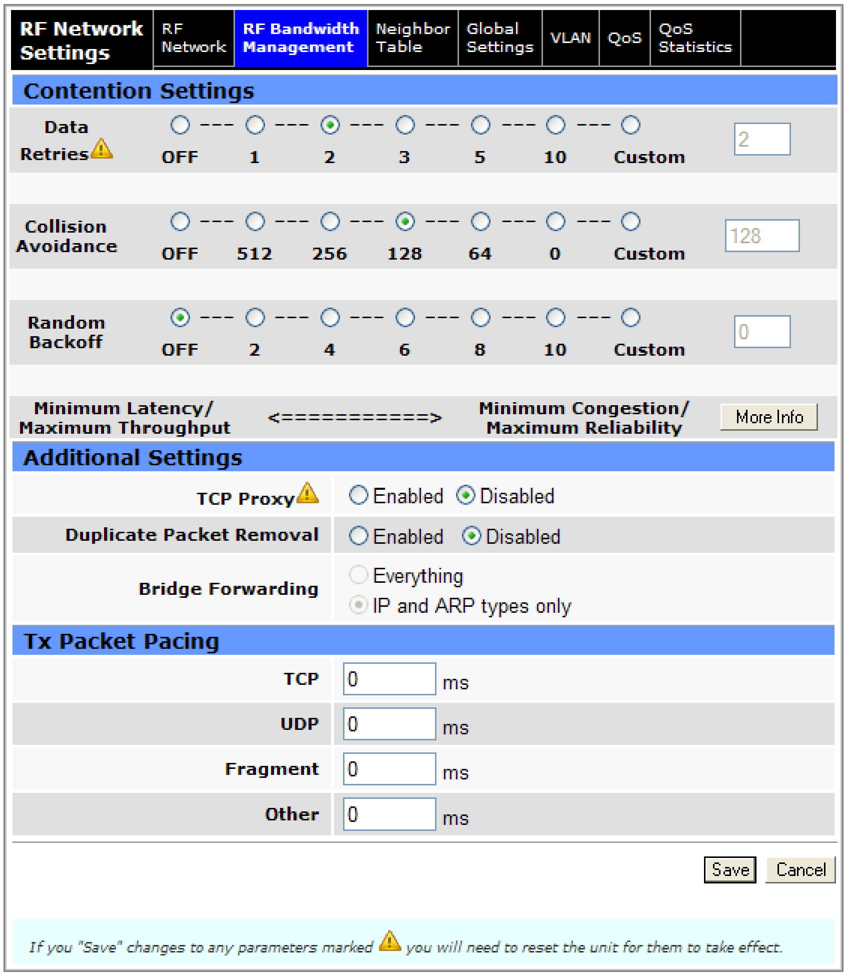
Cancel: Click Cancel to cancel any changes you may have made to any of the settings in this tab.

Note: If you change the IP Forwarding Mode, Access Point, RF IP Address, RF Netmask, RF MAC Address, or MTU settings in this tab, as indicated by the yellow alert symbol (⚠), a reset of the Viper is required before the setting will take effect.

4.3.2. RF BANDWIDTH MANAGEMENT

RF Bandwidth Management is the second (from left) tab of the RF Network Settings page. To navigate to this tab, select RF Network Settings from the main menu and click RF Bandwidth Management. In this tab you can make configuration settings for RF contention, TCP Proxy, Duplicate Packet Removal and Bridge Forwarding, and Transmit Packet Pacing.

Figure 33 – RF Network Settings – RF Bandwidth Management



Contention Settings

Data Retries ⚠	○ OFF	○ 1	● 2	○ 3	○ 5	○ 10	○ Custom	2
Collision Avoidance	○ OFF	○ 512	○ 256	● 128	○ 64	○ 0	○ Custom	128
Random Backoff	● OFF	○ 2	○ 4	○ 6	○ 8	○ 10	○ Custom	0

Minimum Latency/ Maximum Throughput <===========> Minimum Congestion/ Maximum Reliability

Additional Settings

TCP Proxy ⚠	○ Enabled ● Disabled
Duplicate Packet Removal	○ Enabled ● Disabled
Bridge Forwarding	○ Everything ● IP and ARP types only

Tx Packet Pacing

TCP	0 ms
UDP	0 ms
Fragment	0 ms
Other	0 ms

If you "Save" changes to any parameters marked ⚠ you will need to reset the unit for them to take effect.

Contention Settings

These are bandwidth management selectors. These selections allow the user to tune the device parameters based on the desired network operation. Selections toward the left favor minimum latency and maximum throughput; selections toward the right favor minimum congestion and maximum reliability. You may select from the numerical values offered or select Custom and enter any whole-number values within the range shown.

Data Retries: When data retries are enabled, the receiving Viper will reply with a very short RF acknowledge message each time a unicast data packet is received correctly. The RF acknowledge allows the transmitting Viper to Verify that the packet was received successfully. This does, however, add a small amount of latency to each packet, reducing overall throughput. If the transmitting Viper does not receive an RF acknowledge, it will retransmit the message again up to the maximum number of data retries specified.

If a remote Viper becomes completely unreachable or is disconnected, all packets destined for that unit will be transmitted the maximum number of times since the packet is never correctly received. Continually transmitting and retransmitting packets to an unreachable remote will reduce available bandwidth to the remaining functional Vipers.

Setting data retries to zero yields the maximum throughput since no RF acknowledgement s are transmitted over the air. However, enabling data retries will provide the maximum level of reliability of the network.

Valid settings for data retries are values in the range of zero (off) to ten (0 to 10), inclusive. The default setting is 2.

Note: When Data Retries is set to Off, the unit is in “No Acks Required” mode. All other settings enable Acknowledgements.

Collision Avoidance: When enabled, the collision avoidance feature will transmit a short two-way handshake between the transmitting and receiving Viper. This tells any adjacent Vipers that a data transmission will be taking place. Adjacent Vipers will wait until the data transmission is complete before they try to capture the air by sending a new packet.

This feature is particularly useful when remote Vipers are located at sites where they are unable to hear each other transmit directly and both remotes want to transmit data to the same base station at the same time. In this scenario they may often try to transmit at the same time yielding a corrupted message at the base station.

The two-way handshake reserves airtime from the network for the packet transmission. It will however add a small, fixed latency to each packet. The added latency is small relative to the time it takes to transmit a large packet when the chance of collision is greatest. However, when short packets need to be transmitted, it can sometimes take just as long to complete the two-way handshake as it does to send the short packet.

For this reason, the collision avoidance parameter allows the user to specify the packet size threshold above which the two-way handshake is implemented. For example, if the Collision Avoidance is set for 128, the Viper will complete a two-way handshake before sending packets that are larger than 128 bytes, reducing potential congestion. The Viper will **not** complete the two-way handshake before sending packets that are smaller than 128 bytes, improving throughput.

Setting collision avoidance to a value of 1500 or above effectively disables the feature, as the maximum data packet size is 1500 Bytes. Valid settings are Off, or values in the range from 0 to 512, inclusive. The default value is 128.

Random Backoff: When a data transmission competes in a busy network, there may be several new Vipers waiting to send data. If all these Vipers start transmitting at the exact same time, collisions will occur. To reduce the chance that more than one Viper starts transmitting at a time, the user can enable a random backoff. The Viper will randomly pick a time slot to begin its transmission. The user can specify the maximum number of time slots that the viper will wait before it starts transmitting. If the Viper detects that another unit started transmitting before itself, it will wait until their data transmission is complete before tries to capture the air again.

Each time slot is equal to the time that it takes to complete a collision avoidance two-way handshake. If the user specifies a random backoff of 4, then the Viper will wait up to a maximum of 4 time slots before it starts its transmission. On each new transmission, the Viper radio will randomly pick a time slot (from the time slot number zero, up to the maximum time slot) to begin its transmission.

Normally the random backoff should be set higher for systems that may have a lot of contention. Random backoff can be disabled for systems that have a very controlled traffic pattern, where two or more Vipers are not expected to try to transmit at the same time.

This parameter is often set equal to the estimated number of Vipers in the system that my try to start transmitting at the same time.

When enabled this feature on average adds latency to each transmission. The latency will be noticeable when conducting a standard Ping test, as the total Ping time will increase and be more variable in nature.

Valid settings for random backoff are values in the range of zero (off) to ten (0 to 10), inclusive. The default setting is 2.

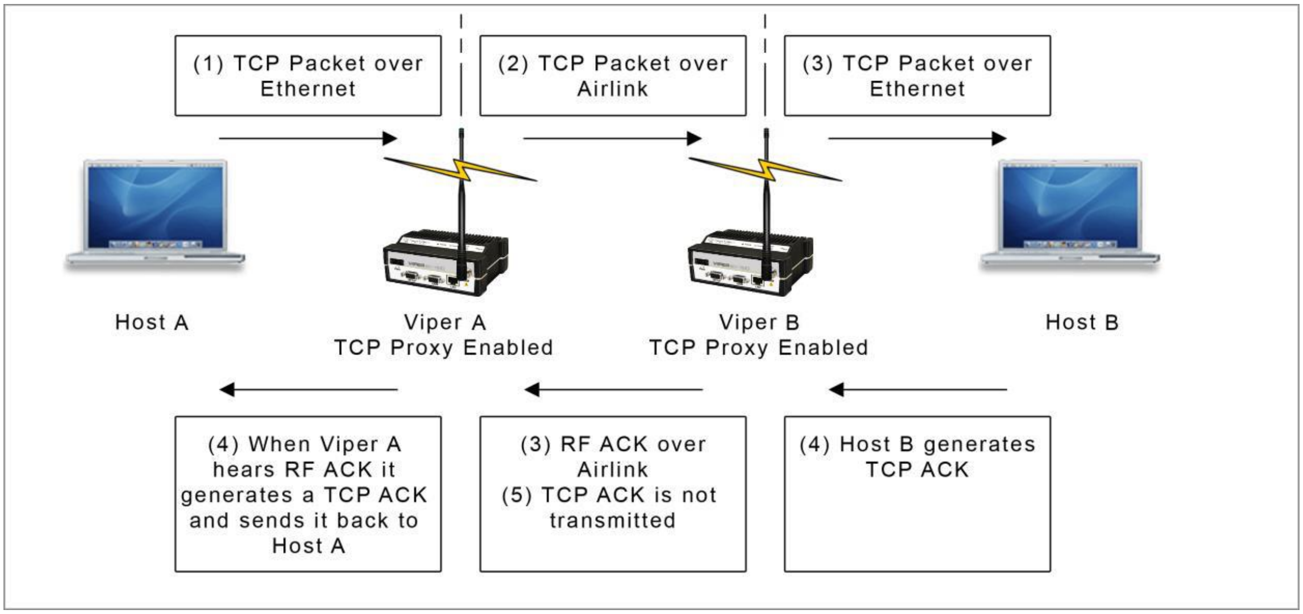
More Info: Clicking More Info displays the above information.

Additional Settings

TCP Proxy: The TCP Proxy setting is available only when the Viper is configured in Router Mode. The default setting is Disabled.

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

Figure 34 – TCP Proxy


(1) TCP Packet over Ethernet
(2) TCP Packet over Airlink
(3) TCP Packet over Ethernet
Host A
Viper A
TCP Proxy Enabled
Viper B
TCP Proxy Enabled
Host B
(4) When Viper A hears RF ACK it generates a TCP ACK and sends it back to Host A
(3) RF ACK over Airlink
(5) TCP ACK is not transmitted
(4) Host B generates TCP ACK

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

1) Host A sends a TCP data packet to Viper A.
2) Viper A transmits the packet over the air to Viper B.
3) Viper B immediately responds with an RF acknowledgement and sends the TCP data packet to Host B.
4) Viper A hears an RF acknowledgement from Viper 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. send it over the air—saving bandwidth on the airlink.

Duplicate Packet Removal: Enable or disable the duplicate packet removal algorithm. The default is Disabled (to preserve compatibility with older versions of the firmware). This algorithm detects duplicate packets that might appear through the system because of retransmits.

Bridge Forwarding: Selections for Bridge Forwarding are either Everything, or IP and ARP types only. The default setting is IP and ARP types (Ethernet II types 0x0800, 0x0806) only.

By selecting the Everything setting, the Viper will forward all 802.3 Ethernet II packet types. Use this setting to transport protocols such as IPX, 802.1Q, etc.

Note: Bridge Forwarding is not available in Router mode because the Viper will automatically forward all packets according to its routing table. When selecting Router forwarding mode, all relevant IP settings must be configured.

Tx Packet Pacing

In a Viper network, a polling device may want to send a query to a remote device and wait for an amount of time for a response. Failure to obtain a response will trigger the polling device to resend a query. If the polling device resends the query too fast, it may collide (on the RF) with the previous response causing the new query and the old response to be lost.

In this poll/response scenario, the user may not be able to configure the wait period between the request and the response in the polling device. The Tx pacing parameter allows the user to configure a waiting period to insert in the Viper unit after each packet is sent out over the RF interface. This waiting period gives enough time for the response to come back to the polling device without causing any collisions on the RF interface.

These parameters set the amount of time for the Viper unit to remain idle after sending a packet over the RF interface. If it is set to 100 ms, it will send a packet, wait 100 ms, send the next packet, wait 100 ms, etc. Normally, the pacing is set to 0, meaning: do not wait, send the next packet right away.

TCP: The TCP packet pacing (in milliseconds). Default setting is zero (0).

UDP: The UDP packet pacing (in milliseconds). Default setting is zero (0).

Fragment: Fragment packet pacing (in milliseconds). Default setting is zero (0).

Other: Pacing (in milliseconds) for any other type of packet. Default setting is zero (0).

Save: Click Save to save any changes you have made to settings in this tab. See Note below.

Cancel: Click Cancel to cancel any changes you may have made to any of the settings in this tab.

Note: If you change the Data Retries, or TCP Proxy settings in this tab, as indicated by the yellow alert symbol (⚠), a reset of the Viper is required before the setting will take effect.

4.3.3. NEIGHBOR TABLE

Neighbor Table is the third (from left) tab of the RF Network Settings page. To navigate to this tab, select RF Network Settings from the main menu and click Network Table.

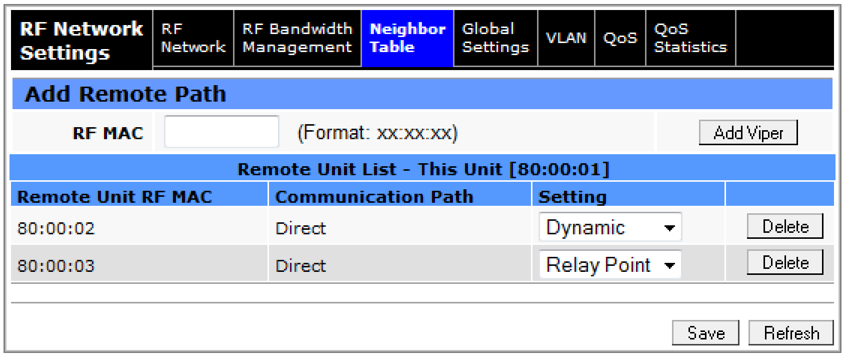
The appearance of the Neighbor Table displayed, and the controls provided to generate, build, or maintain it, will differ depending on whether the Viper is configured as a Bridge or a Router.

4.3.3.1. Neighbor Table for Bridge Mode

In Bridge mode, the Neighbor Table tab allows you to add relay points to the Neighbor Table manually by adding the RF MAC address for each Viper. Vipers may be designated as Dynamic or as a Relay Point. Remote Units may also be deleted from the list if required. The Neighbor Table feature allows unicast data packets to be sent as a directed message to a Viper that has been designated as a relay point. Other relay points will not repeat this message. However, if a broadcast message is sent, then all relay points will repeat the broadcast IP packets.

Note: Most serial data will be sent as broadcast packets unless specifically programmed as unicast UDP or TCP packets.

Figure 35 – RF Network Settings – Neighbor Table (Bridge Mode)



Add Remote Path

RF MAC (Format: xx:xx:xx) Add Viper

Remote Unit List - This Unit [80:00:01]

Remote Unit RF MAC	Communication Path	Setting	
80:00:02	Direct	Dynamic	Delete
80:00:03	Direct	Relay Point	Delete

Save Refresh

Add Remote Path

RF MAC: Enter the MAC address of the unit to be added to the Neighbor Table (Remote Unit List).

Click **Add Viper** to add the address to the table below.

Remote Unit List

The Remote Unit List is the Neighbor Table when the Viper is in Bridge Mode. The RF MAC address of the Viper is displayed in the top header row of the table for reference.

Note: The Remote Unit List (Neighbor) table is updated every time the Viper sends (or receives) data to (or from) the Viper to the remote unit.

Remote Unit RF MAC: This table column displays the RF MAC address for each remote unit.

Communication Path: This column indicates the communication path from this unit to the remote.

- **Direct** means that there is no intervening unit.
- **Relay Point** means that there is a relay point in between.

Setting: Displays the current setting for the remote that is represented in the table row and allows you to change it if required.

- **Dynamic**
  The remote unit was discovered dynamically by sending or receiving a packet.
- **Relay Point**
  This unit is a static entry in the remote table.

Delete: Allows you to remove entries from the table. To delete a unit from the table, click Delete in the row of the table that represents the unit to be deleted.

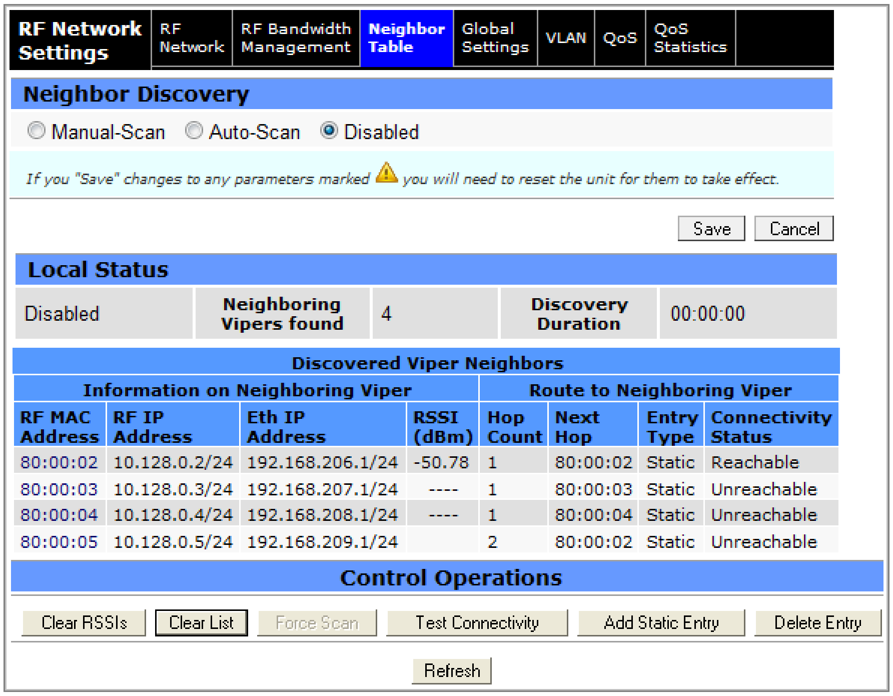
Save: Click Save to save any changes you have made to the Neighbor Table.

Cancel: Click Cancel to cancel any change.

4.3.3.2. Neighbor Table for Router Mode

The Viper SC+ is an IP packet router radio that forwards packets to their destination based on routing statements (which network to send a packet to) in the routing table. The routing statements are automatically populated into the routing table by entries from the Neighbor Table (shown in the following figure). Neighbors can be enrolled into the Neighbor Table by three different methods: Auto-Scan, Manual Scan, and Static Entries.

Figure 36 – RF Network Settings – Neighbor Table (Router Mode)



Neighbor Discovery

○ Manual-Scan ○ Auto-Scan ● Disabled

If you "Save" changes to any parameters marked ⚠ you will need to reset the unit for them to take effect.

Local Status

Disabled	Neighboring Vipers found	4	Discovery Duration	00:00:00

Discovered Viper Neighbors

Information on Neighboring Viper				Route to Neighboring Viper			
RF MAC Address	RF IP Address	Eth IP Address	RSSI (dBm)	Hop Count	Next Hop	Entry Type	Connectivity Status
80:00:02	10.128.0.2/24	192.168.206.1/24	-50.78	1	80:00:02	Static	Reachable
80:00:03	10.128.0.3/24	192.168.207.1/24	----	1	80:00:03	Static	Unreachable
80:00:04	10.128.0.4/24	192.168.208.1/24	----	1	80:00:04	Static	Unreachable
80:00:05	10.128.0.5/24	192.168.209.1/24		2	80:00:02	Static	Unreachable

Control Operations

Neighbor Discovery

Manual Scan, Auto-Scan, or **Disabled:** Select Manual Scan or Auto-Scan for the method of neighbor discovery or select Disabled to disable neighbor discovery. Here is what happens when each of these options is selected and then saved. The default setting is Manual Scan.

> **Manual Scan:** The Viper starts in the Ready state. In the Ready state, the unit is quiet (no neighbor discovery control messages are sent). If the user clicks Force Scan (button in Control Operations section near the bottom), the Viper initiates the Scanning for Neighbors state in which the unit is learning about other remote units and the remote units are learning about the Viper. The Viper goes from the Scanning for Neighbors state to the Saving Neighbor Table state when it stops learning any new neighbor information for a specified amount of time (this time interval can be changed using the parameter neighborDiscovery.convergeTimeout, expressed in milliseconds). In the Saving Neighbor Table state, the content of the neighbor table is stored into nonvolatile memory. Then, if the unit reboots, the content of the neighbor table is retrieved from this nonvolatile memory. Finally, the Viper goes from the Saving Neighbor Table state to the Ready state.

Auto-Scan: The Viper starts in the Scanning for Neighbors state. In the Scanning for Neighbors state, the Viper is learning about remote units and the remote units are learning about the Viper. The Viper goes from the Scanning for Neighbors state to the Ready state when it stops learning any new neighbor information for a specified amount of time (this value can be changed using the parameter neighborDiscovery.convergeTimeout, expressed in milliseconds). In the Ready state, the Viper is generating keep-alive packets. (The rate at which keep-alive packets are generated can be changed using the parameter neighborDiscovery.keepAliveTimeout.) In the Ready state, the Viper performs broken-link detection. The Viper is monitoring the keep-alive packets of other units that are one (1) hop away. The Viper knows the interval at which other units are generating their keep-alive packets. If a unit fails to receive four (4) keep-alive packets in a row from another unit, it removes that unit from its neighbor table and goes into the Scanning for Neighbors state. If the user clicks Force Scan (button in the Control Operations section near the bottom), the Viper goes into the Scanning for Neighbors state. If any remote units initiate the Scanning for Neighbors state, the local Viper also goes into the Scanning for Neighbors state.

Disabled: The neighbor discovery module is disabled, and the Viper will not learn about any new neighbors. It will not generate any keep-alive packets.

NextGen RF recommends the following.

Auto-Scan: This feature is only for projects that contain no more than ten (10) radios with very strong RF paths.

Manual Scan: This should only be used to enroll all the remotes for the first time, then disable. After a Manual Scan, disabling the discovery mode locks all routes into place. Review all Neighbor entries and edit them if necessary, to ensure that they are the correct and most reliable RF paths and delete RF paths that are not required. For example, in most master and remote polling configurations, the remotes only need to have the master in their Neighbor Tables.

Disabled: This will disable neighbor discoveries and allow you to Add Static Entries or use the Viper Route Generator (VRG) application to populate the neighbor entries.

Note: NextGen RF strongly recommends visiting the NextGen RF support website and downloading the VRG application. If necessary, contact NextGen RF Technical Support for assistance with using the VRG application.

Save: Click Save to save your changes if you change the method or disable neighbor discovery.

Cancel: Click Cancel to cancel any change.

Local Status

There are five states of operation reported in the local status section of the tab: Ready, Scanning for Neighbors, Saving Neighbor Table, Testing Connectivity, or Disabled.

Ready: The Neighbor Discovery module is in the Ready state when it is not scanning for other units. If the Viper is operating in Manual Scan, it does nothing. If the Viper is operating in the 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 is saving all neighbor entries of the type of Dynamic into nonvolatile memory. When the save is complete, all these entries are now of type Locked. This state only occurs when the Neighbor Discovery module is operating in Manual Scan mode.

Testing Connectivity: The Neighbor Discovery module is verifying that the 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 ten (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 to complete the neighbor-discovery learning process.

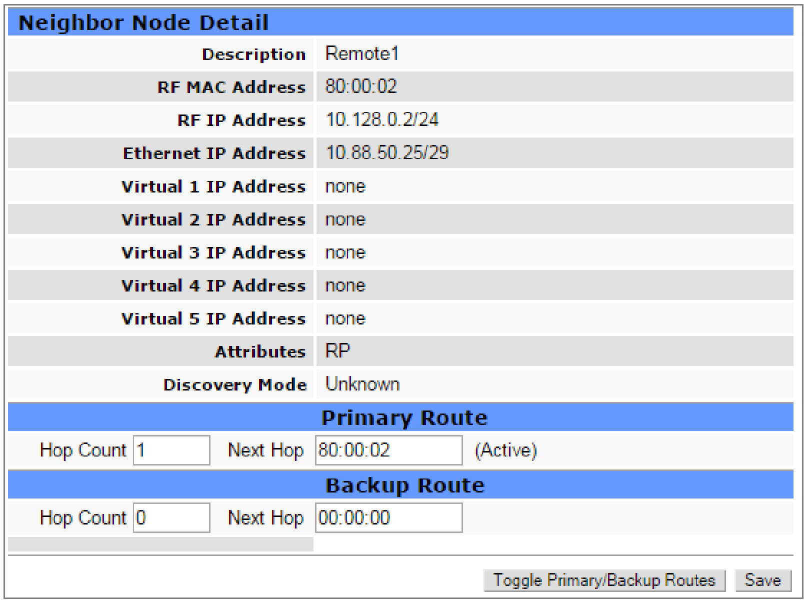
Discovered Viper Neighbors

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

Information on Neighboring Vipers

RF MAC Address: Identifies each entry uniquely. Click the RF Mac Address entries to display the details of the selected device in the Neighbor Node Detail window.

Figure 37 – Neighbor Node Detail window



Neighbor Node Detail

Description	Remote1
RF MAC Address	80:00:02
RF IP Address	10.128.0.2/24
Ethernet IP Address	10.88.50.25/29
Virtual 1 IP Address	none
Virtual 2 IP Address	none
Virtual 3 IP Address	none
Virtual 4 IP Address	none
Virtual 5 IP Address	none
Attributes	RP
Discovery Mode	Unknown

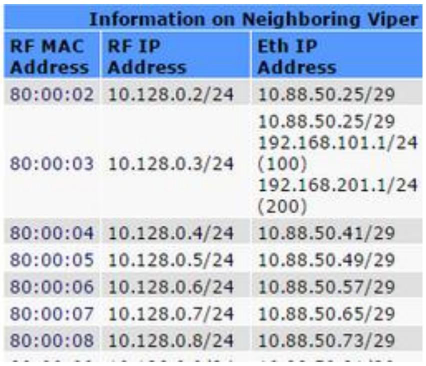
Primary Route

Hop Count 1 Next Hop 80:00:02 (Active)

Backup Route

Hop Count 0 Next Hop 00:00:00

RF IP Address and Ethernet IP Address: This Neighbor Discovery module uses this information to build the routing table. VLAN IDs (if applicable) are displayed in parentheses:



Information on Neighboring Viper

RF MAC Address	RF IP Address	Eth IP Address
80:00:02	10.128.0.2/24	10.88.50.25/29
80:00:03	10.128.0.3/24	10.88.50.25/29 192.168.101.1/24 (100) 192.168.201.1/24 (200)
80:00:04	10.128.0.4/24	10.88.50.41/29
80:00:05	10.128.0.5/24	10.88.50.49/29
80:00:06	10.128.0.6/24	10.88.50.57/29
80:00:07	10.128.0.7/24	10.88.50.65/29
80:00:08	10.128.0.8/24	10.88.50.73/29

RSSI (dBm): The RSSI is logged for all units that are only one (1) hop away. For units that are more than one hop away or unreachable, the RSSI is not logged.

Route to Neighboring Vipers

Hop Count and **Next Hop**: Indicates the route by which the remote unit can be reached. When the Hop Count is one (1), the device can be reached directly. When the Hop Count is more than one (1), it can be reached by passing through another Viper, as identified by the Next Hop.

Entry Type
There are three types of entries.

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 discover mode. If the Save button is clicked, all Static neighbor entries are saved in nonvolatile memory. They are restored to the table after a reboot.

Dynamic: A Dynamic neighbor entry is anyone that has been learned by the Neighbor Discovery module. It can be updated or deleted by the Neighbor Discovery module when it detects changes in the topology.

Locked: A Locked neighbor entry is a Dynamic neighbor entry that has been saved into nonvolatile memory. A Locked neighbor entry behaves like a Dynamic neighbor, except it is saved into nonvolatile memory and will be restored into the table after a reboot.

Control Operations

The Control Operations section of the tab contains only buttons that allow you to modify the Neighbor Table.

Clear RSSIs: Clears RSSI values from the table.

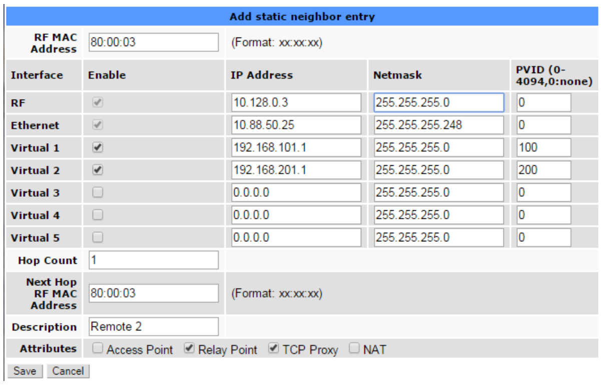
Clear List: Clicking Clear List deletes neighbor units from the table. (Auto-Scan or Force Scan will populate the table with neighbors discovered from the new discovery process, but you must click Refresh

Force Scan: Clicking Force Scan starts the Neighbor Discovery process to update the table. (You must click the Refresh button to update the table displayed to see new entries.)

Test Connectivity: Clicking Test Connectivity starts a Ping test to each neighbor in the table. “Reachable” will be displayed in the Connectivity Status column of the table if the Ping is successful. (Click Refresh to update the table).

Add Static Entry: Click this button to open a new window that allows you to enter static entries (as shown in the following figure). The RF MAC Address, RF IP address, Ethernet IP address, RF netmask, Ethernet netmask, Hop count and the MAC address of the next hop and a description of it must be entered. Use the check boxes at the bottom of the window to set the attribute whether the unit is an Access Point (AP), Relay Point (RP), using NAT (NAT) or using the TCP proxy (TCP). Note that the netmask format is a.b.c.d. Click Save to add the entry to the neighbor table; click cancel to close the window without saving.

Figure 38 – Add static neighbor entry window

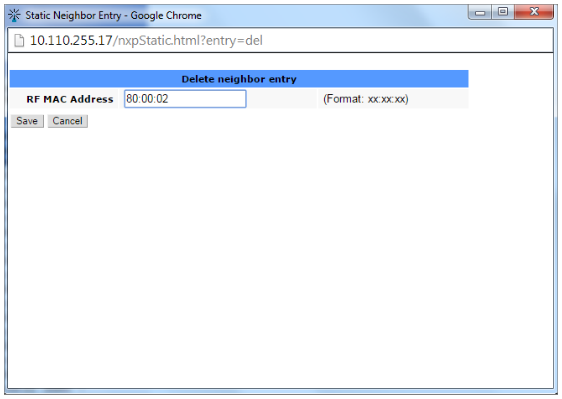


Add static neighbor entry

RF MAC Address	80:00:03	(Format: xx:xx:xx)		
Interface	Enable	IP Address	Netmask	PVID (0-4094,0:none)
RF	☑	10.128.0.3	255.255.255.0	0
Ethernet	☑	10.88.50.25	255.255.255.248	0
Virtual 1	☑	192.168.101.1	255.255.255.0	100
Virtual 2	☑	192.168.201.1	255.255.255.0	200
Virtual 3	□	0.0.0.0	255.255.255.0	0
Virtual 4	□	0.0.0.0	255.255.255.0	0
Virtual 5	□	0.0.0.0	255.255.255.0	0
Hop Count	1			
Next Hop RF MAC Address	80:00:03	(Format: xx:xx:xx)		
Description	Remote 2			
Attributes	□ Access Point ☑ Relay Point ☑ TCP Proxy □ NAT			

Delete Entry: To delete an entry, click the Delete Entry button, and then enter the RF MAC address of the unit that you want to delete. Then, click the Save button.

Figure 39 – Delete a static neighbor entry screen



10.110.255.17/nxpStatic.html?entry=del

Delete neighbor entry

RF MAC Address: 80:00:02 (Format: xx:xx:xx)

Refresh: Click Refresh to update the information displayed in the Local Status section.

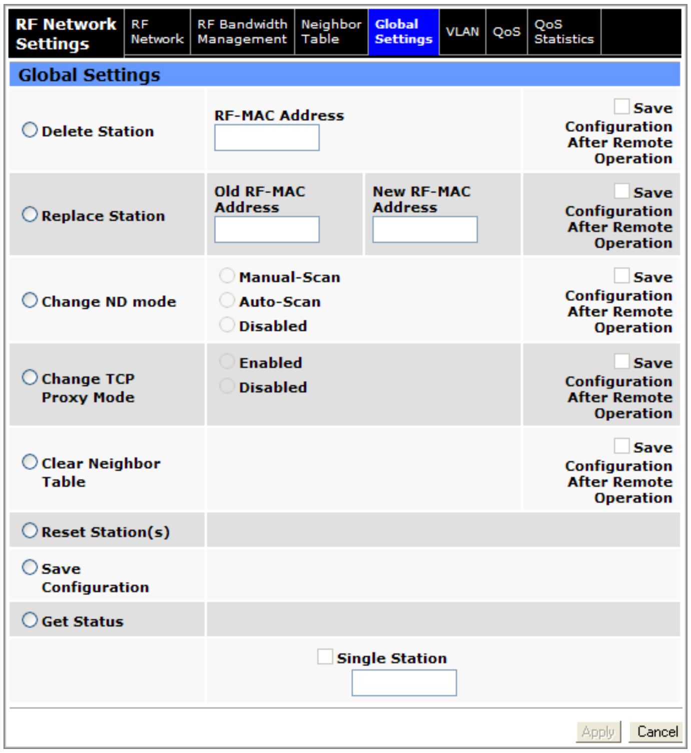
4.3.4. GLOBAL SETTINGS

Global Settings is the fourth (from left) tab of the RF Network Settings page. To navigate to this tab, select RF Network Settings from the main menu and click Global Settings. This tab allows you to make several Global Settings for the RF Network.

Note: Settings in this tab are only available when the Viper is in Router mode.

The Global Settings tab allows you to make changes for a single Viper or to the entire Viper network. It allows you to make changes to remote units’ Neighbor Tables.

Figure 40 – RF Network Settings – Global Settings



Global Settings

○ Delete Station	RF-MAC Address		□ Save Configuration After Remote Operation
○ Replace Station	Old RF-MAC Address	New RF-MAC Address	□ Save Configuration After Remote Operation
○ Change ND mode	○ Manual-Scan ○ Auto-Scan ○ Disabled		□ Save Configuration After Remote Operation
○ Change TCP Proxy Mode	○ Enabled ○ Disabled		□ Save Configuration After Remote Operation
○ Clear Neighbor Table			□ Save Configuration After Remote Operation
○ Reset Station(s)			
○ Save Configuration			
○ Get Status			
	□ Single Station		

Global Settings

Note: All selections in this tab apply to all Vipers in the network unless you check the Single Station check box near the bottom of the tab and enter the RF MAC Address of the Viper to which the change will be applied.

Delete Station: Enter the RF MAC Address of the station to be deleted from the Neighbor Table of all Vipers on the network. To save this change to the configuration after remote operation, place a check in the check box at the right.

Replace Station: Enter the RF MAC Address of the unit that will be removed and the RF MAC Address of the Viper that will replace it. To save this change to the configuration after remote operation, place a check in the check box at the right.

This setting allows you to change the Neighbor Discovery (ND) mode for all Vipers in the network. When this option is set, you can select Manual Scan, Auto-Scan, or Disabled for all Vipers. To save this change to the configuration after remote operation, place a check in the check box at the right.

Change TCP Proxy Mode: You can change the TCP Proxy mode for all Vipers in the network to enabled or disabled. To save this change to the configuration after remote operation, place a check in the check box at the right.

Clear Neighbor Table: To clear the Neighbor Tables for all Vipers in the network, select this setting. To save this change to the configuration after remote operation, place a check in the check box at the right.

Save Configuration: This will send a Save Configuration command to all Vipers in the network.

Get Status: This will send a Get Status command to all Vipers in the network. The status will be displayed in the Neighbor Table tab of the RF Network Settings page.

Single Station: If this check box is checked and the RF MAC Address of a Viper on the network is entered into the field below, any other selection made in this tab will apply to the Viper whose RF MAC Address is entered. When the box is not checked, any setting made in this tab will apply to all Vipers on the network.

Apply: Click Apply to apply any changes you have made to Global Settings.

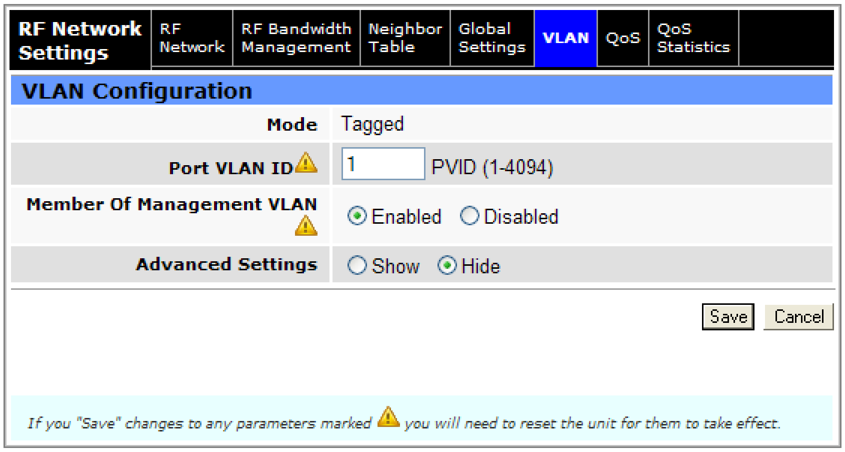
Cancel: Click Cancel to cancel any changes you may have made to any settings in this tab.

4.3.5. VLAN

VLAN (Virtual Local Area Network) is the fifth (from left) tab of the RF Network Settings page. To navigate to this tab, select RF Network Settings from the main menu and click VLAN. This tab allows you to make VLAN Configuration settings for the RF Network.

VLAN is available in both Bridge and Router mode. In Bridge mode, the user can specify either tagged or untagged operation for the RF interface when VLAN is enabled. In Router mode, the RF interface can only be tagged when VLAN is enabled.

Figure 41 – RF Network Settings – VLAN (with Advanced Settings hidden)



VLAN Configuration

Mode	Tagged
Port VLAN ID⚠	1 PVID (1-4094)
Member Of Management VLAN ⚠	● Enabled ○ Disabled
Advanced Settings	○ Show ● Hide

If you "Save" changes to any parameters marked ⚠ you will need to reset the unit for them to take effect.

VLAN Configuration

Mode: The RF interface operates in VLAN Tagged mode only. In Untagged mode, devices on this interface are not using VLAN tags. Incoming (ingress) packets are tagged with the port VLAN ID (PVID). VLAN tags are removed on outgoing (egress) packets. See the Advanced Settings section that follows for more options.

Port VLAN ID: Sets the Port VLAN ID (PVID).

Member of Management VLAN: When the Management VLAN is enabled, you can access the internal functions of the Viper (HTTP, FTP, Command Shell) through this port if Member of Management VLAN is enabled. This is true only for ports of Tagged type. Ports of Untagged type can always access the internal functions of the Viper (HTTP, FTP, Command Shell).

Advanced Settings (Show or Hide): Click **Show** to show advanced settings in the lower part of the tab; click **Hide** to hide the advanced settings.

Save: Click Save to save any changes you have made in this tab. See Note below.

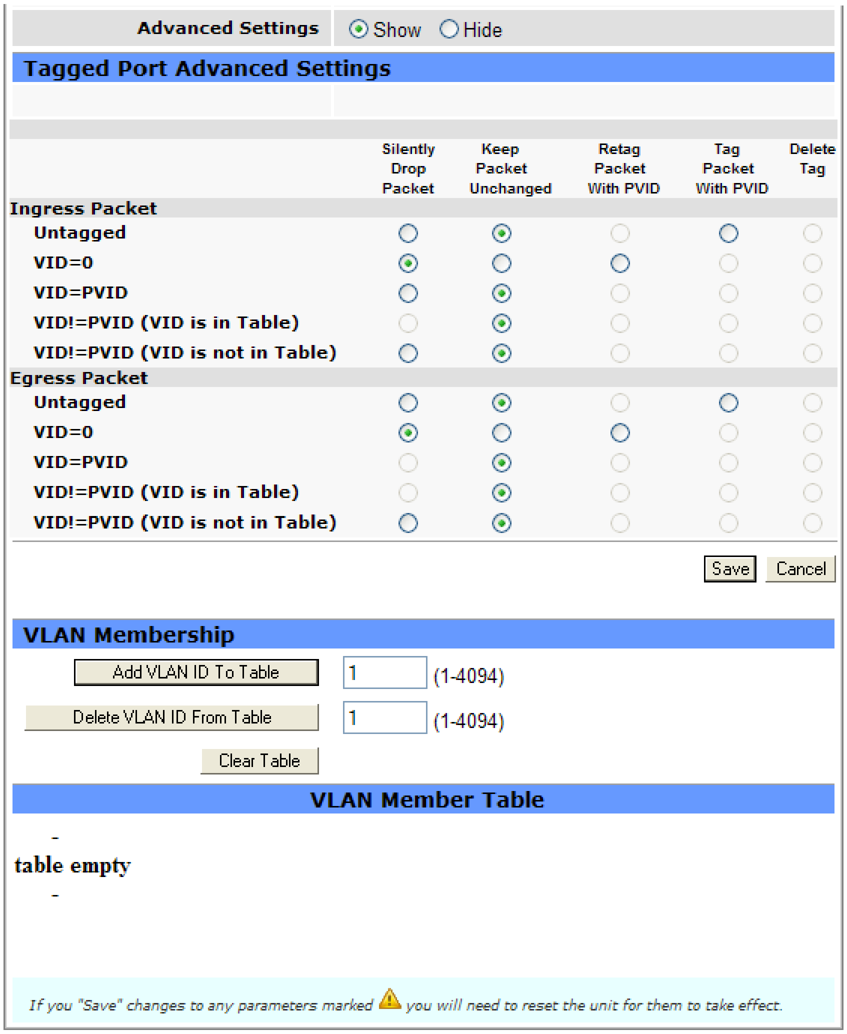
Cancel: Click Cancel to cancel any changes you may have made to any of the settings in this tab.

Note: If you change the Port VLAN ID or Member of Management VLAN setting in this tab, as indicated by the yellow alert symbol (⚠), a reset of the Viper is required before the setting will take effect.

4.3.5.1. Advanced Settings For RF Network Settings » VLAN

When you click Show to show the advanced settings in the VLAN tab of the RF Network Settings page, the tab expands downward to show the advanced settings. The following figure shows the Advanced Settings section when the Viper is configured for Router mode. In Bridge mode the Viper may operate in Tagged mode or Untagged mode and this section does not appear drastically different except the name of the section will reflect the port mode selected and some selections are less restricted than those shown in the following figure.

Figure 42 – RF Network Settings – VLAN tab showing Advanced Settings only



Advanced Settings ● Show ○ Hide

Tagged Port Advanced Settings

	Silently Drop Packet	Keep Packet Unchanged	Retag Packet With PVID	Tag Packet With PVID	Delete Tag
Ingress Packet					
Untagged	○	●	○	○	○
VID=0	●	○	○	○	○
VID=PVID	○	●	○	○	○
VID!=PVID (VID is in Table)	○	●	○	○	○
VID!=PVID (VID is not in Table)	○	●	○	○	○
Egress Packet					
Untagged	○	●	○	○	○
VID=0	●	○	○	○	○
VID=PVID	○	●	○	○	○
VID!=PVID (VID is in Table)	○	●	○	○	○
VID!=PVID (VID is not in Table)	○	●	○	○	○

VLAN Membership

Add VLAN ID To Table: 1 (1-4094)

Delete VLAN ID From Table: 1 (1-4094)

VLAN Member Table

-
table empty
-

If you "Save" changes to any parameters marked ⚠ you will need to reset the unit for them to take effect.

The Advanced Settings provide options for ingress packets (packets coming into the Viper) and egress packets (packets leaving the Viper) and for maintaining and displaying a VLAN Member Table.

Advanced Settings Tagged Port or Untagged Port

The title of the Advanced Settings section of the RF Network Settings » VLAN tab will reflect the Port mode selected. This section allows you to specify what actions are to be taken with ingress and egress packets, based on their VLAN ID (VID) tag (or absence of a VID tag).

VID is the VLAN ID contained in the packet.
PVID is the Port VLAN ID (the VLAN ID associated with the interface and configured in the Viper Web Interface).

Ingress Packet

Untagged (The packet has no VLAN ID tag): If incoming packets are untagged, you can choose to silently drop these packets, keep them unchanged, or tag the packets with the PVID. For Untagged Port Mode, the default setting is to tag the packet with the PVID. For Tagged Port Mode, the default setting is to keep the packet unchanged.

VID=0: If incoming packets have a VLAN ID set to zero (0), you can choose to silently drop these packets, keep them unchanged, re-tag the packets with the PVID, or delete their tag. For both modes, Untagged Port Mode and Tagged Port Mode, the default setting is to silently drop the packet.

VID=PVID (The packet has a VLAN ID that is the same as the PVID): If incoming packets have a VLAN ID that is the same as the PVID, you can choose to silently drop these packets, keep them unchanged, or delete their tag. For both modes, Untagged Port Mode and Tagged Port Mode, the default setting is to keep the packet unchanged.

VID!=PVID (VID is not equal to PVID): If incoming packets have a VLAN ID that is not the same as the PVID, you can choose to silently drop these packets, keep them unchanged, re-tag the packets with PVID, or delete their tag. The default for this setting, which is for Untagged Port Mode only, is to silently drop the packet.

VID!=PVID (VID is not equal to PVID) but **VID is in Table** — Tagged Port Mode only
If incoming packets have a VLAN ID that is not the same as the PVID, but is in the VLAN Member Table, you can choose to silently drop these packets, keep them unchanged, retag the packets, or delete their tags. The default for this setting, which is for Tagged Port Mode only, is to keep the packet unchanged.

VID!=PVID (VID is not equal to PVID) and **VID is not in Table** — Tagged Port Mode only
If incoming packets have a VLAN ID that is not the same as the PVID and is not in the VLAN Member Table, you can choose to silently drop these packets, keep them unchanged, re-tag the packets, or delete their tags. The default for this setting, which is for Tagged Port Mode only, is to keep the packet unchanged.

Egress Packet

Untagged (The packet has no VLAN ID tag): If exiting packets are untagged, you can choose to silently drop these packets, keep them unchanged, or tag them with PVID. For both modes, Untagged Port Mode and Tagged Port Mode, the default setting is to keep the packet unchanged.

VID=0: If exiting packets have a VLAN ID set to zero (0), you can choose to silently drop these packets, keep them unchanged, re-tag them with PVID, or delete their tag. For both modes, Untagged Port Mode and Tagged Port mode, the default setting is to silently drop the packet.

VID=PVID: If exiting packets have a VLAN ID that is in the VLAN Member Table, you can choose to silently drop these packets, keep them unchanged, or delete their tag. For Untagged Port Mode, the default setting is to delete the tag. For Tagged Port Mode, the default setting is to keep the packet unchanged.

VID!=PVID (VID is not equal to PVID) — Untagged Port Mode only

If exiting packets have a VLAN ID that is not the same as the PVID, you can choose to silently drop these packets, keep them unchanged, re-tag the packets with PVID, or delete their tag. The default for this setting, which is for Untagged Port Mode only, is to silently drop the packet.

VID!=PVID (VID is not equal to PVID) but **VID is in Table** — Tagged Port Mode only

If exiting packets have a VLAN ID that is not the same as the PVID, but is in the VLAN Member Table, you can choose to silently drop these packets or keep them unchanged retag their packets or delete their tags. The default for this setting, which is for Tagged Port Mode only, is to keep the packet unchanged.

VID!=PVID (VID is not equal to PVID) and **VID is not in Table** — Tagged Port Mode only

If exiting packets have a VLAN ID that is not the same as the PVID and is not in the VLAN Member Table, you can choose to silently drop these packets, keep them unchanged, retag the packets, or delete their tags. The default for this setting, which is for Tagged Port Mode only, is to keep the packet unchanged.

Save: Click Save to save any changes you have made in this tab. See the Note that follows.

Cancel: Click Cancel to cancel any changes you may have made to any of the settings in this tab.

VLAN Membership

Add VLAN ID To Table: To add a VLAN ID, enter the VLAN ID (as a number between 1 and 4094, inclusive) and then click this button. The VLAN ID is added to the VLAN Member Table in the section below.

Delete VLAN ID From Table: To remove a VLAN ID, enter the VLAN ID (as a number between 1 and 4094, inclusive) that is displayed in the VLAN Member Table in the section below, and then click this button. The VLAN ID is removed from the table.

Clear Table: To delete all VLAN ID entries from the VLAN Member Table from the section below at once, click this button. The VLAN Member Table section of the tab displays “table empty.”

VLAN Member Table

This section of the RF Network Settings » VLAN tab displays Member VLANs in table form as defined using the fields and buttons in the above section. In no table entries exist, “table empty” is displayed.

Note: If you made a change to the Port VLAN ID or Member of Management VLAN setting above in this tab, as indicated by the yellow alert symbol (⚠), a reset of the Viper is required before the setting will take effect.

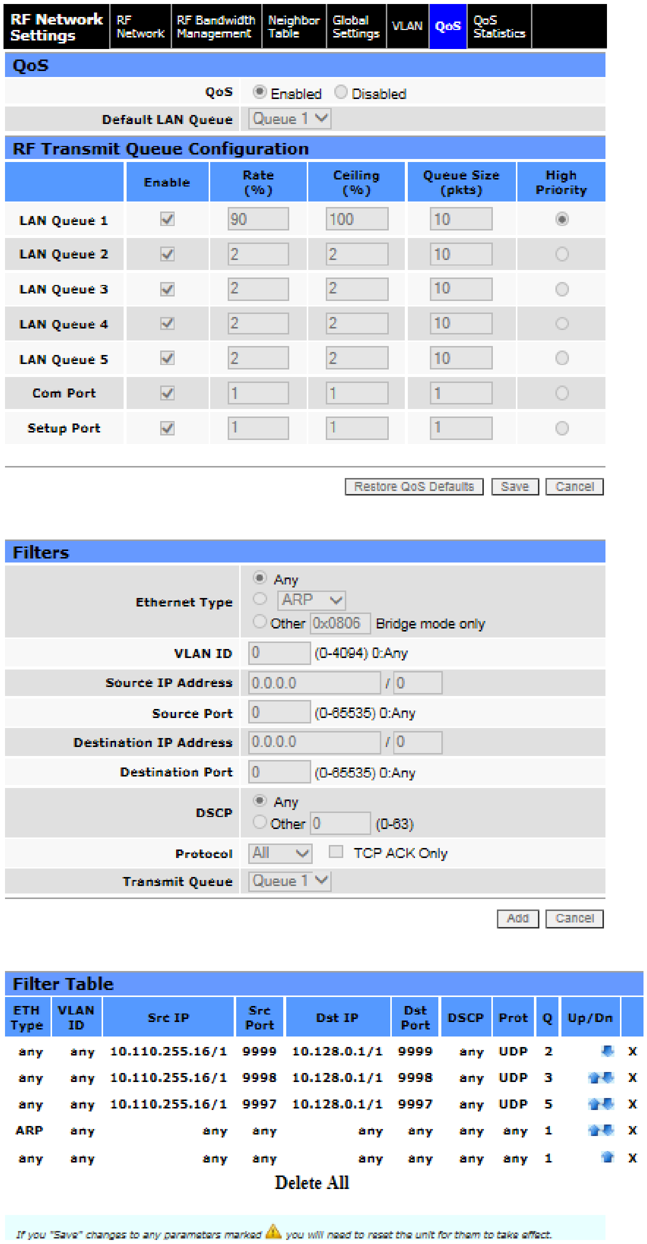
4.3.6. QOS

QoS (Quality of Service) is the sixth (from left) tab of the RF Network Settings page. To navigate to this tab, select RF Network Settings from the main menu and click QoS. This tab allows you to make QoS configuration settings for the RF Network.

Up to seven (7) transmit queues can be used to classify the packets before they are actually transmitted over the RF interface. Two of the RF transmit queues are used for packets coming from the serial ports of the Viper (one per serial port: one for COM; and one for SETUP). The remaining five (5) RF transmit queues are used for packets coming from the Ethernet interface. The user can specify filters to classify the packets coming from the Ethernet interface into any of these five remaining RF transmit queues. All seven transmit queues can be configured for minimum guaranteed bit rate, maximum bit rate, and maximum number of packets the queue can hold.

Packets generated by the Viper itself are sent into a hidden RF transmit queue called the control transmit queue, which is not listed in the QoS tab and does not have any configurable options. In this queue, packets are transmitted over the RF interface in FCFS (first-come, first-served) order.

Figure 43 – RF Network Settings – QoS



QoS

QoS	● Enabled ○ Disabled
Default LAN Queue	Queue 1

RF Transmit Queue Configuration

	Enable	Rate (%)	Ceiling (%)	Queue Size (pkts)	High Priority
LAN Queue 1	☑	90	100	10	●
LAN Queue 2	☑	2	2	10	○
LAN Queue 3	☑	2	2	10	○
LAN Queue 4	☑	2	2	10	○
LAN Queue 5	☑	2	2	10	○
Com Port	☑	1	1	1	○
Setup Port	☑	1	1	1	○

Filters

Ethernet Type	● Any ○ ARP ○ Other 0x0806 Bridge mode only
VLAN ID	0 (0-4094) 0:Any
Source IP Address	0.0.0.0 / 0
Source Port	0 (0-65535) 0:Any
Destination IP Address	0.0.0.0 / 0
Destination Port	0 (0-65535) 0:Any
DSCP	● Any ○ Other 0 (0-63)
Protocol	All □ TCP ACK Only
Transmit Queue	Queue 1

Filter Table

ETH Type	VLAN ID	Src IP	Src Port	Dst IP	Dst Port	DSCP	Prot	Q	Up/Dn	
any	any	10.110.255.16/1	9999	10.128.0.1/1	9999	any	UDP	2	⬇	X
any	any	10.110.255.16/1	9998	10.128.0.1/1	9998	any	UDP	3	⬆⬇	X
any	any	10.110.255.16/1	9997	10.128.0.1/1	9997	any	UDP	5	⬆⬇	X
ARP	any	any	any	any	any	any	any	1	⬆⬇	X
any	any	any	any	any	any	any	any	1	⬆	X

If you "Save" changes to any parameters marked ⚠ you will need to reset the unit for them to take affect.

QoS

QOS (Enable or Disable): Enable or disable the QoS (Quality of Service) module. When QoS is disabled, only the hidden control transmit queue is operational (packets are transmitted over the RF interface first come, first served).

Default LAN Queue: Allows you to select one of the configured LAN Queues as the default queue. A packet coming from the Ethernet interface that must be sent over the RF interface will be placed into the default transmit queue unless a specific filter is defined that indicates which RF transmit queue to use.

RF Transmit Queue Configuration

Enable (or Disable): Place a check mark in the check box to enable a queue. Clear the check box to disable the queue. At least one LAN port queue must be always enabled.

Rate (%): The minimum guaranteed bit rate (expressed as a percentage of the available bandwidth). Minimum value is 0 %. Maximum value is 100 %. A value of 0 % means discard any packets sent to this queue.

Ceiling (%): The maximum bit rate (expressed as a percentage of the available bandwidth). Minimum value is 1 %. Maximum value is 100 %.

Queue Size (packets): The maximum number of packets the transmit queue can hold. Minimum value is 1 packet. Maximum value is 128 packets.

High Priority: When sending packets, the packet scheduler sends a packet from one transmit queue, moves to the next transmit queue and sends one packet, then moves to the next transmit queue, etc. All this is done while maintaining the configured throughputs per transmit queue. When the high priority queue is set, this queue will be processed first when transmitting, and once per every two other queues.

Restore QoS Defaults: Click to restore default configuration settings for RF Transmit Queues.

Save: Click Save to save any changes you have made in this tab.

Cancel: Click Cancel to cancel any changes you may have made to any of the settings in this tab.

Filters

Settings in this section allow you to define up to 128 QoS filters to classify the packets in the various RF transmit queues. The following fields are used to define filters.

Ethernet Type: Configurable in bridge mode only. Select one of the standard Ethernet types (e.g., ARP, IPv4, VLAN tag, etc.), or enter the hex value of any Ethernet types defined by the IEEE (http://standards.ieee.org/develop/regauth/ethertype/eth.txt)

VLAN ID: The VLAN identifier is used only if operating in bridge mode.

Source IP Address: Use this to specify a range of IP addresses that will represent valid source IP addresses. (For example, 200.200.200.0/24, 200.200.200.1/32.)

Source Port: The UDP/TCP source port number. (A value of 0 means any value.)

Destination IP Address: Use this to specify a range of IP addresses that will represent valid destination IP addresses. (For example, 200.200.200.0/24, 200.200.200.1/32.)

Destination Port: The UDP/TCP destination port number. (A value of 0 means any value.)

DSCP: The Differentiated Services Code Point (DSCP) consists of the six (6) most significant bits of the eight-bit Type of Service (ToS) field in the IP header. Select Any to not filter by this value. The following table contains DSCP values and descriptions.

Table 14 DSCP (Differentiated Services Code Point) Values and Descriptions

Value	Description
0	CS0 – 000000 – Best Effort
8	CS1 – 001000 – Class 1
16	CS2 – 010000 – Class 2
24	CS3 – 011000 – Class 3
32	CS4 – 100000 – Class 4
40	CS5 – 101000 – Express
48	CS6 – 110000 – Reserved
10	AF11 – 001010 – Class 1 Low
12	AF12 – 001100 – Class 1 Medium
14	AF13 – 001110 – Class 1 High
18	AF21 – 010010 – Class 2 Low
20	AF22 – 010100 – Class 2 Medium
22	AF23 – 010110 – Class 2 High
26	AF31 – 011010 – Class 3 Low
28	AF32 – 011100 – Class 3 Medium
30	AF33 – 011110 – Class 3 High
34	AF41 – 100100 – Class 4 Low
36	AF42 – 100100 – Class 4 Medium
38	AF43 – 100110 – Class 4 High
46	EF – 101110 – Expedited Forwarding

Protocol: The protocol number in the IP header of the packet. Possible selections are All, ICMP, TCP, and UDP. Leave this filed set to All if this value does not matter.

TCP ACK Only When this option is checked, the filter will look for TCP packets with a TCP header only (no TCP data) and with only the ACK flag set.

Transmit Queue: Specify the above transmit queue to use for packets that correspond to all of the criteria in the filter defined above.

Add: Click to add filters.

Cancel: Click Cancel to cancel any changes to filters.

Filter Table

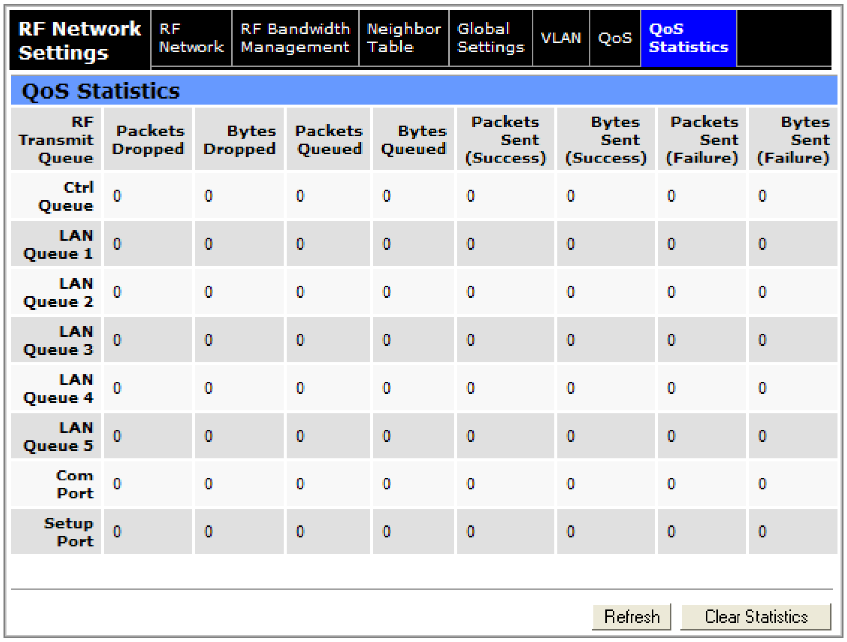
This area displays, in table format, any filters that have been defined above and added. Before packets are transmitted over the RF interface, these filters are applied to determine the proper RF transmit queue to use. The filters are passed from the top down until a match is found. These filters only apply when the QoS module is enabled.

Delete All: clicking the Delete All link will clear all filters that have been defined and are displayed in the filter table.

4.3.7. QOS STATISTICS

QoS Statistics is the seventh (right-most) and final tab of the RF Network Settings page. To navigate to this tab, select RF Network Settings from the main navigation menu and click QoS Statistics. This tab provides a table of statistics related to the Quality of Service (QoS) for each of the transmit queues in the Viper.

Figure 44 – RF Network Settings – QoS Statistics



QoS Statistics

RF Transmit Queue	Packets Dropped	Bytes Dropped	Packets Queued	Bytes Queued	Packets Sent (Success)	Bytes Sent (Success)	Packets Sent (Failure)	Bytes Sent (Failure)
Ctrl Queue	0	0	0	0	0	0	0	0
LAN Queue 1	0	0	0	0	0	0	0	0
LAN Queue 2	0	0	0	0	0	0	0	0
LAN Queue 3	0	0	0	0	0	0	0	0
LAN Queue 4	0	0	0	0	0	0	0	0
LAN Queue 5	0	0	0	0	0	0	0	0
Com Port	0	0	0	0	0	0	0	0
Setup Port	0	0	0	0	0	0	0	0

QoS Statistics

RF Transmit Queue: Identifies the transmit queue: the transmit control queue, transmit queues enabled and described in the RF Network Settings » QoS tab, or COM port queue or Setup port queue.

Packets Dropped: Number of packets dropped because the RF transmit queue is full.

Bytes Dropped: Number of bytes dropped because the RF transmit queue is full.

Packets Queued: Number of packets in the RF transmit queue. (Refresh the tab contents to see the current number.)

Bytes Queued: Number of bytes in the RF transmit queue. (Refresh the tab contents to see the current number.)

Packets Sent (Success): Number of packets that have been successfully moved from the RF transmit queue and sent over the RF interface.

Bytes Sent (Success): Number of bytes that have been successfully moved from the RF transmit queue and sent over the RF interface.

Packets Sent (Failure): Number of packets moved from the RF transmit queue that failed to be sent over the RF interface.

Bytes Sent (Failure): Number of bytes moved from the RF transmit queue that failed to be sent over the RF interface.

Refresh: Click Refresh to refresh the tab contents and update values displayed in the QoS Statistics table.

Clear Statistics: Click Clear Statistics to clear the QoS Statistics table, reset all values to zero and restart counting.

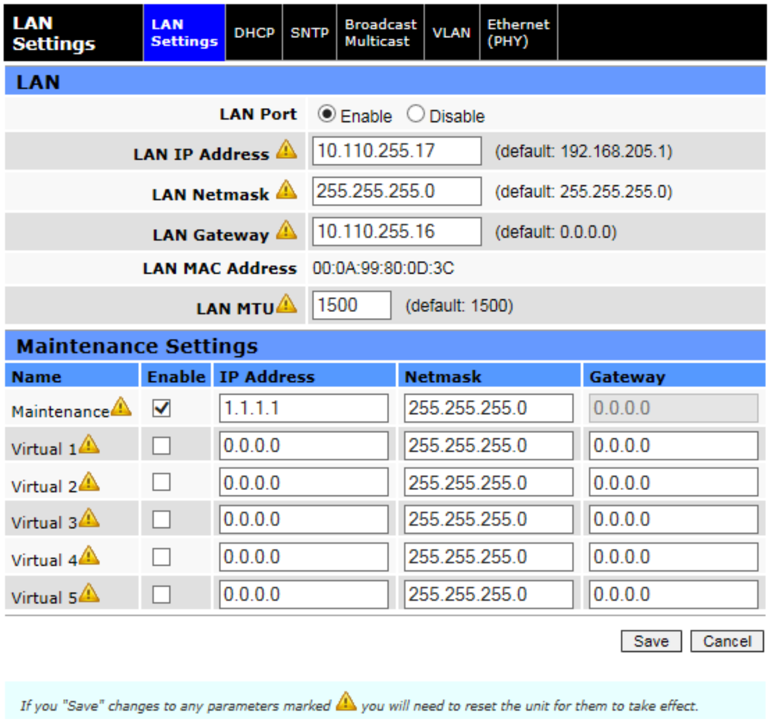
4.4. LAN SETTINGS

The LAN Settings page contains six tabs: LAN Settings, DHCP, Broadcast Multicast, VLAN, and Ethernet (PHY).

4.4.1. LAN SETTINGS

LAN Settings is the first (left-most) tab in the LAN Settings page. To navigate to this tab, select LAN Settings from the main menu. This tab allows you to set the LAN IP Address, Netmask, gateway, and MTU for the Viper and specify the IP Address and Netmask of the maintenance server.

Figure 45 – LAN Settings – LAN Settings



LAN

LAN Port	● Enable ○ Disable	
LAN IP Address ⚠	10.110.255.17	(default: 192.168.205.1)
LAN Netmask ⚠	255.255.255.0	(default: 255.255.255.0)
LAN Gateway ⚠	10.110.255.16	(default: 0.0.0.0)
LAN MAC Address	00:0A:99:80:0D:3C	
LAN MTU⚠	1500	(default: 1500)

Maintenance Settings

Name	Enable	IP Address	Netmask	Gateway
Maintenance⚠	☑	1.1.1.1	255.255.255.0	0.0.0.0
Virtual 1⚠	☐	0.0.0.0	255.255.255.0	0.0.0.0
Virtual 2⚠	☐	0.0.0.0	255.255.255.0	0.0.0.0
Virtual 3⚠	☐	0.0.0.0	255.255.255.0	0.0.0.0
Virtual 4⚠	☐	0.0.0.0	255.255.255.0	0.0.0.0
Virtual 5⚠	☐	0.0.0.0	255.255.255.0	0.0.0.0

If you "Save" changes to any parameters marked ⚠ you will need to reset the unit for them to take effect.

LAN

LAN Port: The LAN port interface can be enabled or disabled. The default setting is enabled.

LAN IP Address: Allows each Viper to be set to a unique valid IP address. The default IP address for the Viper LAN port is 192.168.205.1.

LAN Netmask: Together with the LAN IP Address, the LAN netmask determines the subnet the Viper is on. The netmask selected depends on the network topology. The default LAN netmask is 255.255.255.0.

LAN MAC Address: The Media Access Control (MAC) address is a unique address that a manufacturer assigns to each networking device. The MAC address is expressed as six hexadecimal numbers separated by colons in a format similar to AA:BB:CC:DD:EE:FF, for example.

LAN Gateway: This is the IP Address of the Access Point to be used as the gateway to the management network. If the Viper is the Access Point, do not change the LAN Gateway from the default address. The default address is 0.0.0.0.

For each Viper network, one and only one Access Point may be defined. This is the Default Gateway (for WAN access). Remote Vipers use the RF IP address of the Viper that is set up to be the Access Point in the network, if that Access Point is in the neighbor table. Once it scans and finds an Access Point, the Viper will then fill in the LAN Gateway automatically as that Access Point's RF IP address. There is normally never any reason to change the LAN Gateway address, as the Viper does this for you whenever you perform a scan on the network or statically add an Access Point Viper to the neighbor table.

LAN MTU: The Maximum Transfer Unit (MTU) is the maximum number of bytes the unit will send in a packet. Acceptable values range from 576 to 1500. The default value is 1500.

Maintenance Settings

The maintenance IP interface allows access to the device from a host on the LAN only. All devices on the same network will be typically given the same maintenance IP address and netmask so that a technician can move from one device to the other and access them using the same IP address.

Virtual 1 to 5

Virtual IP interfaces can only be configured in router mode.

Default gateway: Usually one default gateway is configured. The user can select to set the default gateway on the LAN interface, on one of the virtual IP interfaces or the RF interface if the device is operating in router mode. Multiple gateway can be set if the device is operating in router mode with VLAN enabled, the device will then operate in VRF mode (Virtual Route Forwarding).

VRF mode: This mode is on when router mode and VLAN mode are active. Each IP packet will be forwarded inside the Viper network with their original VLAN tag. When it comes time to select a default route for a packet, preference will be given to the gateway that is on the interface with the same VLAN tag (PVID).To activate a maintenance or virtual IP, click the **Enable** box in the given row and configure each address as described below:

IP Address: Enter a maintenance IP address that is different from the LAN IP Address. The default maintenance IP address is 1.1.1.1.

Netmask: Together with the IP address, the netmask determines the subnet the IP address of the Viper is on. The netmask selected depends on the network topology. The default netmask is 255.255.255.0.

Gateway: This is the IP Address of the Access Point to be used as the gateway to the management network. If the Viper is the Access Point, do not change the LAN Gateway from the default address. The default address is 0.0.0.0.

Save: Click **Save** to save any changes you have made in this tab. See Note below.

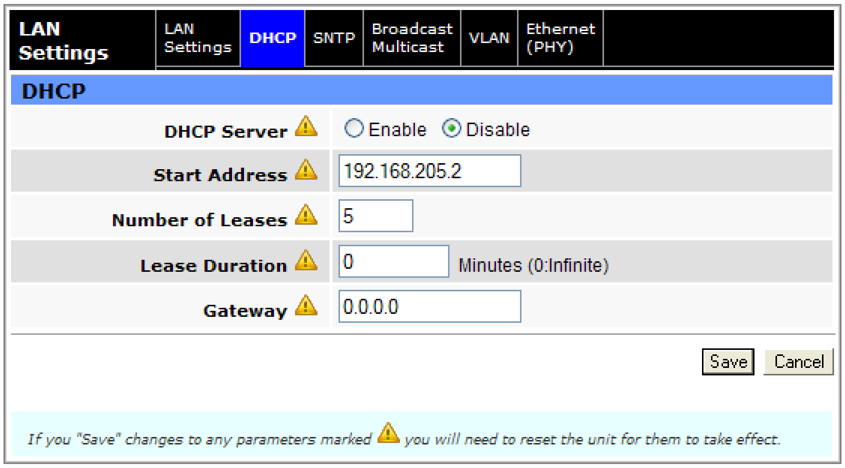
Cancel: Click **Cancel** to cancel any changes you may have made to any of the settings in this tab.

Note: If you change any settings on this page other than to enable/disable the LAN Port, a reset of the Viper is required before the setting will take effect.

4.4.2. DHCP

DHCP is the second (from left) tab in the LAN Settings page. To navigate to this tab, select LAN Settings from the main menu and click DHCP. In this tab you can enable or disable the DHCP (Dynamic Host Configuration Protocol) Server in the Viper and set other DHCP parameters.

Figure 46 – LAN Settings – DHCP



DHCP

DHCP Server ⚠	○ Enable ● Disable
Start Address ⚠	192.168.205.2
Number of Leases ⚠	5
Lease Duration ⚠	0 Minutes (0:Infinite)
Gateway ⚠	0.0.0.0

If you "Save" changes to any parameters marked ⚠ you will need to reset the unit for them to take effect.

DHCP

DHCP Server: The DHCP (Dynamic Host Configuration Protocol) Server can be enabled or disabled. The default setting is DHCP Server enabled.

Start Address: This is the first address that will be leased to other devices on the subnet when the DHCP Server is enabled. When a Viper is configured as a DHCP server, this filed represents the beginning IP address of the pool managed by the DHCP Server. Normally the Viper automatically calculates a default lease Start address as the Ethernet IP address of the Viper plus one.

Number of Leases: The maximum number of IP Addresses that will be leased out to units connected to the Viper when the DHCP server is enabled. It represents the maximum number of DHCP clients that will be able to lease an IP address from the Viper.

Lease Duration: The length of time in minutes that each IP address will be leased to a DHCP client before it expires and a new lease is required. Zero (0) minutes means leases do not expire.

Gateway: This is the IP address of the gateway assigned by the DHCP Server. In router mode, the default gateway is the IP address of the Viper itself. In bridge mode, the default gateway is 0.0.0.0. To override the default setting, enter a valid IP address to specify the gateway.

Save: Click Save to save any changes you have made in this tab. See Note below.

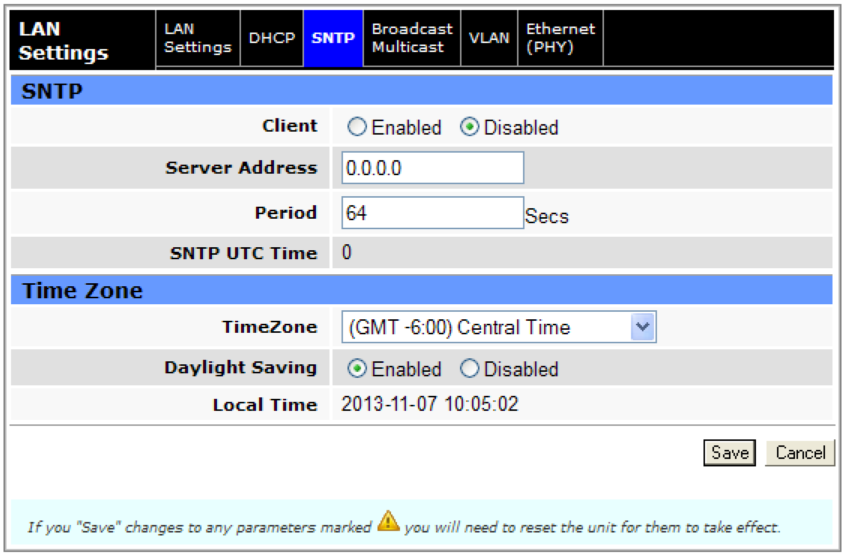
Cancel: Click Cancel to cancel any changes you may have made to any of the settings in this tab.

Note: If you change any of the above setting in this tab, as indicated by the yellow alert symbol (⚠), a reset of the Viper is required before the setting will take effect.

4.4.3. SNTP

SNTP is the third (from left) tab of the LAN Settings page. To navigate to this tab, select LAN Settings from the main menu and click SNTP. From this tab you can set parameters for the Simple Network Time Protocol (SNTP).

Figure 47 – LAN Settings – SNTP



SNTP

Client	○ Enabled ● Disabled
Server Address	0.0.0.0
Period	64 Secs
SNTP UTC Time	0

Time Zone

TimeZone	(GMT -6:00) Central Time
Daylight Saving	● Enabled ○ Disabled
Local Time	2013-11-07 10:05:02

If you "Save" changes to any parameters marked ⚠ you will need to reset the unit for them to take effect.

SNTP

Client: The SNTP (Simple Network Time Protocol) Client can be enabled or disabled. The default setting is disabled.

Server Address: When the SNTP client is enabled, enter the IP address of an SNTP Server.

Period: Enter the amount of time in seconds between that will elapse between each time the SNTP server will be polled to obtain the current time. The default setting is 64 seconds (1 minute, 4 seconds) between polling.

SNTP UTC Time: Display the time received from the SNTP Server (in seconds) when it was most-recently polled. (This field is read-only and non-zero only when SNTP client is enabled and an SNTP server has been polled.

Time Zone

Time Zone: Allows you to select the time zone applicable for the location of the Viper. Facilitates translation of UTC time to local time.

Daylight Saving: Allows you to specify whether Daylight Saving time is in effect for the locale and time of year where the Viper is located.

Local Time: Displays the local date and time (to seconds) when the SNTP client is enabled, an SNTP server has been polled, and settings for time zone and daylight-saving time have been configured correctly.

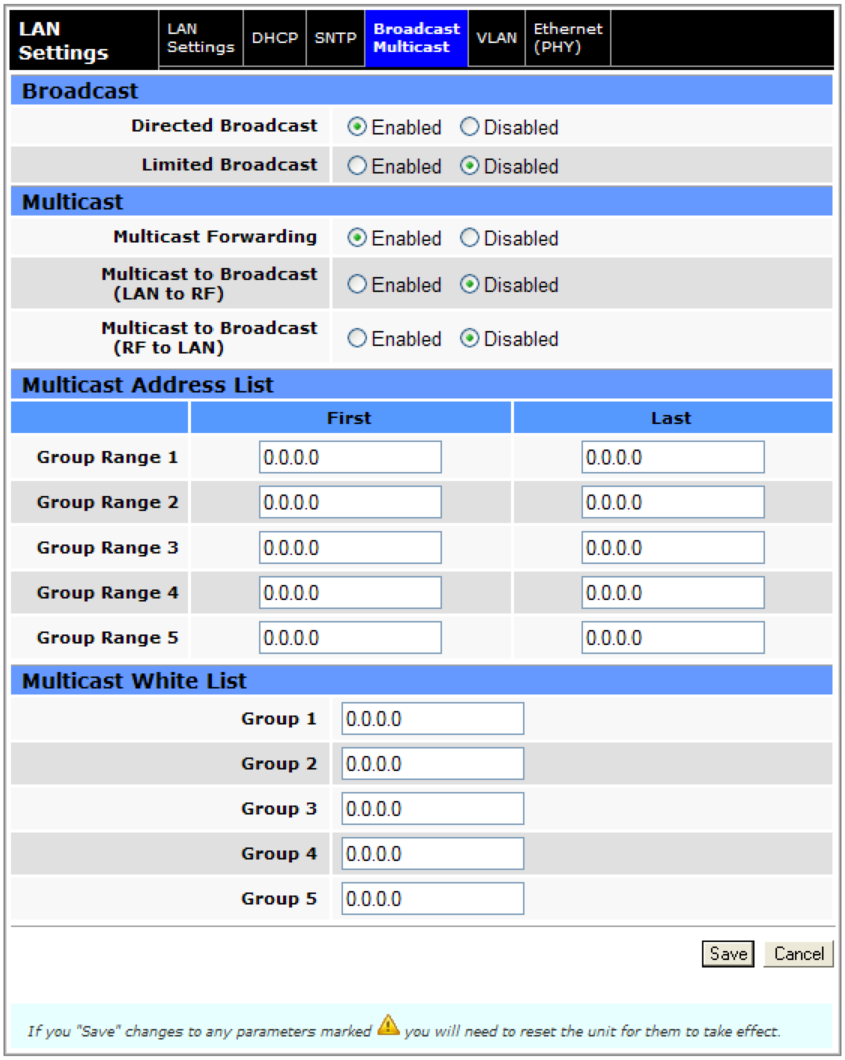
Save: Click Save to save any changes you have made in this tab.

Cancel: Click Cancel to cancel any changes you may have made to any of the settings in this tab.

4.4.4. BROADCAST MULTICAST

Broadcast Multicast is the fourth (from left) tab in the LAN Settings page. To navigate to this tab, select LAN Settings from the main menu and click Broadcast Multicast. This tab allows you to set parameters for Broadcast and Multicast from the Viper.

Figure 48 – LAN Settings – Broadcast Multicast



Broadcast

Directed Broadcast	● Enabled ○ Disabled
Limited Broadcast	○ Enabled ● Disabled

Multicast

Multicast Forwarding	● Enabled ○ Disabled
Multicast to Broadcast (LAN to RF)	○ Enabled ● Disabled
Multicast to Broadcast (RF to LAN)	○ Enabled ● Disabled

Multicast Address List

	First	Last
Group Range 1	0.0.0.0	0.0.0.0
Group Range 2	0.0.0.0	0.0.0.0
Group Range 3	0.0.0.0	0.0.0.0
Group Range 4	0.0.0.0	0.0.0.0
Group Range 5	0.0.0.0	0.0.0.0

Multicast White List

Group 1	0.0.0.0
Group 2	0.0.0.0
Group 3	0.0.0.0
Group 4	0.0.0.0
Group 5	0.0.0.0

If you "Save" changes to any parameters marked ⚠ you will need to reset the unit for them to take effect.

Broadcast

Directed Broadcast: This parameter controls the forwarding of directed broadcast packets from the LAN interface to the RF interface. Directed Broadcast is enabled by default.

Limited Broadcast: This parameter controls the forwarding of limited broadcast packets from the LAN interface to the RF interface. Limited Broadcast is disabled by default.

Multicast

Multicast Forwarding: This parameter controls the forwarding of multicast packets from the LAN interface to the RF interface (and vice-versa). The packets forwarded from the LAN to the RF interface are identified by the Multicast Address List. (All other multicast packets are dropped.) On the other hand, the Multicast Whitelist controls which multicast packets are passed from the RF interface to the LAN interface. When the Multicast Whitelist is empty, all multicast packets received from the RF interface are passed on the LAN interface, otherwise only the multicast packets identified in the whitelist are passed over the LAN. The default setting for Multicast Forwarding is enabled.

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). The default setting for Multicast to Broadcast for LAN to RF is disabled.

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). The default setting for Multicast to Broadcast for RF to LAN is disabled.

Multicast Address List

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

Multicast White List

All packets received from the RF interface with a multicast destination IP address matching one of the multicast addresses 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 not 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.

Save: Click Save to save any changes you have made in this tab.

Cancel: Click Cancel to cancel any changes you may have made to any of the settings in this tab.

4.4.5. VLAN

VLAN (Virtual Local Area Network) is the fifth (second from left) tab of the LAN Settings page. To navigate to this tab, select LAN Settings from the main menu and click VLAN. This tab contains configuration settings for VLAN set up through the LAN. Settings are similar to those in the VLAN tab shown earlier for the RF Network Settings, except settings in this page are for VLAN on the LAN interface. (Settings in the previous VLAN tab were for VLAN on the RF interface).

VLAN Configuration (bridge mode)

The parameters in this page are only active when VLAN is enabled (see Home->Basic Settings->VLAN Mode)

Mode: Select the VLAN mode of operation.

Untagged: Devices on this interface are not using VLAN tags. Incoming (ingress) packets are tagged with the port VLAN ID (PVID). VLAN tags are removed on outgoing (Egress) packets. See the "Advanced Settings" section for more options.

Tagged: Devices on this interface are using VLAN tags. Incoming (ingress) packets are forwarded with their VLAN ID. Outgoing (Egress) packets are also keeping their VLAN tags. See the "Advanced Settings" section for more options.

Port VLAN ID

Set the port VLAN ID (PVID).

Member of Management VLAN: When the "Management VLAN" is enabled, user can access the internal functions of the Viper (HTTP, FTP, Command Shell) through this port if "Member of Management VLAN" is enabled. This is true only for ports of type "Tagged". Ports of type "Untagged" can always access the internal functions of the Viper (HTTP, FTP, Command Shell).

1.1.4.1.1 ADVANCED SETTINGS

Change the advanced settings (the default actions are highlighted).

<table>
<tr><th colspan="2">UNTAGGED PORT MODE</th></tr>
<tr><th colspan="2">Ingress Packets (Packets Entering The Interface)</th></tr>
<tr><th>Packet Type</th><th>Action</th></tr>
<tr><td>Untagged (The packet has no VLAN ID tag)</td><td>• Silently drop packet
• Keep packet unchanged
• Retag packet with PVID
• Tag packet with PVID
• Delete tag</td></tr>
<tr><td>VID=0 (The packet has a VLAN ID set to 0)</td><td>• Silently drop packet
• Keep packet unchanged
• Retag packet with PVID
• Tag packet with PVID
• Delete tag</td></tr>
</table>

UNTAGGED PORT MODE	
VID=PVID (The packet has a VLAN ID equal to the PVID)	• Silently drop packet • Keep packet unchanged • Retag packet with PVID • Tag packet with PVID • Delete tag
VID!=PVID (The packet has a VLAN ID not equal to the PVID)	• Silently drop packet • Keep packet unchanged • Retag packet with PVID • Tag packet with PVID • Delete tag
Egress Packets (Packets Leaving The Interface)	
Packet Type	**Action**
Untagged (The packet has no VLAN ID tag)	• Silently drop packet • Keep packet unchanged • Retag packet with PVID • Tag packet with PVID • Delete tag
VID=0 (The packet has a VLAN ID set to 0)	• Silently drop packet • Keep packet unchanged • Retag packet with PVID • Tag packet with PVID • Delete tag

UNTAGGED PORT MODE	
VID=PVID (The packet has a VLAN ID equal to the PVID)	• Silently drop packet • Keep packet unchanged • Retag packet with PVID • Tag packet with PVID • Delete tag
VID!=PVID (The packet has a VLAN ID not equal to the PVID)	• Silently drop packet • Keep packet unchanged • Retag packet with PVID • Tag packet with PVID • Delete tag

TAGGED PORT MODE	
Ingress Packets (Packets Entering The Interface)	
Packet Type	**Action**
Untagged (The packet has no VLAN ID tag)	• Silently drop packet • Keep packet unchanged • Retag packet with PVID • Tag packet with PVID • Delete tag
VID=0 (The packet has a VLAN ID set to 0)	• Silently drop packet • Keep packet unchanged • Retag packet with PVID • Tag packet with PVID • Delete tag
VID=PVID (The packet has a VLAN ID equal to the PVID)	• Silently drop packet • Keep packet unchanged • Retag packet with PVID • Tag packet with PVID • Delete tag
VID!=PVID (The packet has a VLAN ID not equal to the PVID and the packets VLAN ID is in the VLAN Member Table)	• Silently drop packet • Keep packet unchanged • Retag packet with PVID • Tag packet with PVID

	• Delete tag
VID!=PVID (The packet has a VLAN ID not equal to the PVID and the packets VLAN ID is not in the VLAN Member Table)	• Silently drop packet • Keep packet unchanged • Retag packet with PVID • Tag packet with PVID • Delete tag
Egress Packets (Packets Leaving The Interface)	
Packet Type	**Action**
Untagged (The packet has no VLAN ID tag)	• Silently drop packet • Keep packet unchanged • Retag packet with PVID • Tag packet with PVID • Delete tag
VID=0 (The packet has a VLAN ID set to 0)	• Silently drop packet • Keep packet unchanged • Retag packet with PVID • Tag packet with PVID • Delete tag
VID=PVID (The packet has a VLAN ID equal to the PVID)	• Silently drop packet • Keep packet unchanged • Retag packet with PVID • Tag packet with PVID • Delete tag

VID!=PVID (The packet has a VLAN ID not equal to the PVID and the packets VLAN ID is in the VLAN Member Table)	• Silently drop packet • Keep packet unchanged • Retag packet with PVID • Tag packet with PVID • Delete tag
VID!=PVID (The packet has a VLAN ID not equal to the PVID and the packets VLAN ID is not in the VLAN Member Table)	• Silently drop packet • Keep packet unchanged • Retag packet with PVID • Tag packet with PVID • Delete tag

VLAN Configuration (router mode)

The parameters in this page are only active when VLAN is enabled (see Home->Basic Settings->VLAN Mode)

1.1.5 ETHERNET, VIRTUAL 1, VIRTUAL 2, ..., VIRTUAL 5

Configure the VLAN parameters of the interface

PVID: Setting the interface PVID to 0 will let it operate like it was a regular interface without VLAN tagging. This is so that some interfaces operate in VLAN mode and other in regular mode.

Mode (Untagged): Devices on this interface are not using VLAN tags. Incoming (ingress) packets are tagged with the port VLAN ID (PVID). VLAN tags are removed on outgoing (Egress) packets.

Mode (Tagged): Devices on this interface are using VLAN tags. Incoming (ingress) packets are forwarded with their VLAN ID. Outgoing (Egress) packets are also keeping their VLAN tags.

Member of Mgmt. VLAN: When this parameter is set, external applications can access the device internal applications (HTTP server, FTP server, etc.) by using the IP address (and if set, the PVID) of this interface. This parameter is only active in router mode.

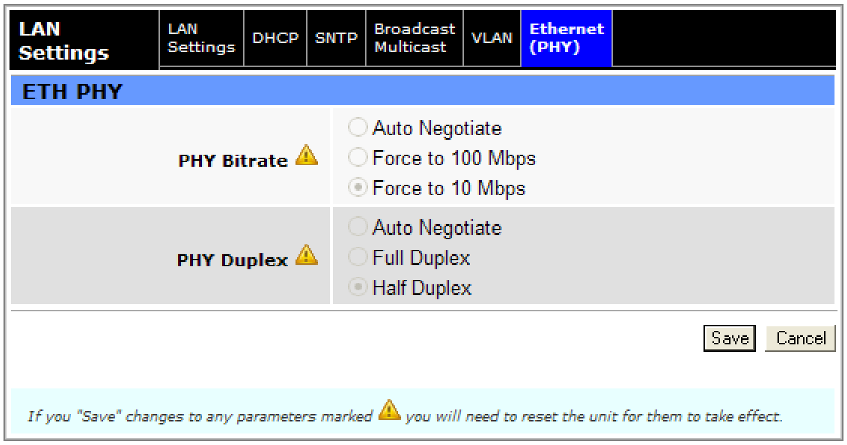
Note: An IP packet received on a LAN interface with a PVID will be routed inside the Viper network with its VLAN tag attached to it (if the ingress interface is an untagged interface, the VLAN tag following the packet with be the interface PVID). The IP packet plus its VLAN tag will be used for VRF routing.

VRF mode: This mode is on when router mode and VLAN mode are active. Each IP packet will be forwarded inside the Viper network with their original VLAN tag. When it comes time to select a default route for a packet, preference will be given to the gateway that is on the interface with the same VLAN tag (PVID).

4.4.6. ETHERNET (PHY)

Ethernet (PHY) is the sixth (right-most) tab of the LAN Settings page. To navigate to this tab, select LAN Settings form the main menu and click Ethernet (PHY). PHY is an abbreviation for the physical layer of the OSI model. (For this reason an Ethernet transceiver is often called a PHYceiver. It is a component that operates at the physical layer of the OSI network model.) This tab contains settings for configuration or negotiation of physical bitrate and duplex mode of the Viper SC+ Ethernet interface.

Figure 49 – Ethernet (PHY)



ETH PHY

PHY Bitrate ⚠
○ Auto Negotiate
○ Force to 100 Mbps
● Force to 10 Mbps

PHY Duplex ⚠
○ Auto Negotiate
○ Full Duplex
● Half Duplex

If you "Save" changes to any parameters marked ⚠ you will need to reset the unit for them to take effect.

PHY Bitrate: Select whether the bitrate of the transceiver will auto-negotiate or be set constant at 100 Mbps or 10 Mbps.

Auto Negotiate: Let the Ethernet interface determine the best speed based on the device facing it.
Force to 100 Mbps: Manually configure the speed of the Ethernet interface to 100 Mbps.
Force to 10 Mbps: Manually configure the speed of the Ethernet interface to 10 Mbps.
Only one of these three options may be selected, as they are mutually exclusive.

PHY Duplex: Select whether the duplex mode of the transceiver will auto-negotiate or be set to Full- or Half-Duplex.

Auto Negotiate: Let the Ethernet interface determine the best mode based on the device facing it.
Full Duplex: Manually configure the mode of the Ethernet interface to Full duplex.
Half Duplex: Manually configure the mode of the Ethernet interface to Half duplex.

Only one of these three options may be selected, as they are mutually exclusive.

Save: Click Save to save any changes you have made in this tab. See Note below.

Cancel: Click Cancel to cancel any changes you may have made to any of the settings in this tab.

Note: If you change the PHY Bitrate or PHY Duplex setting in this tab, as indicated by the yellow alert symbol (⚠), a reset of the Viper is required before the setting will take effect.

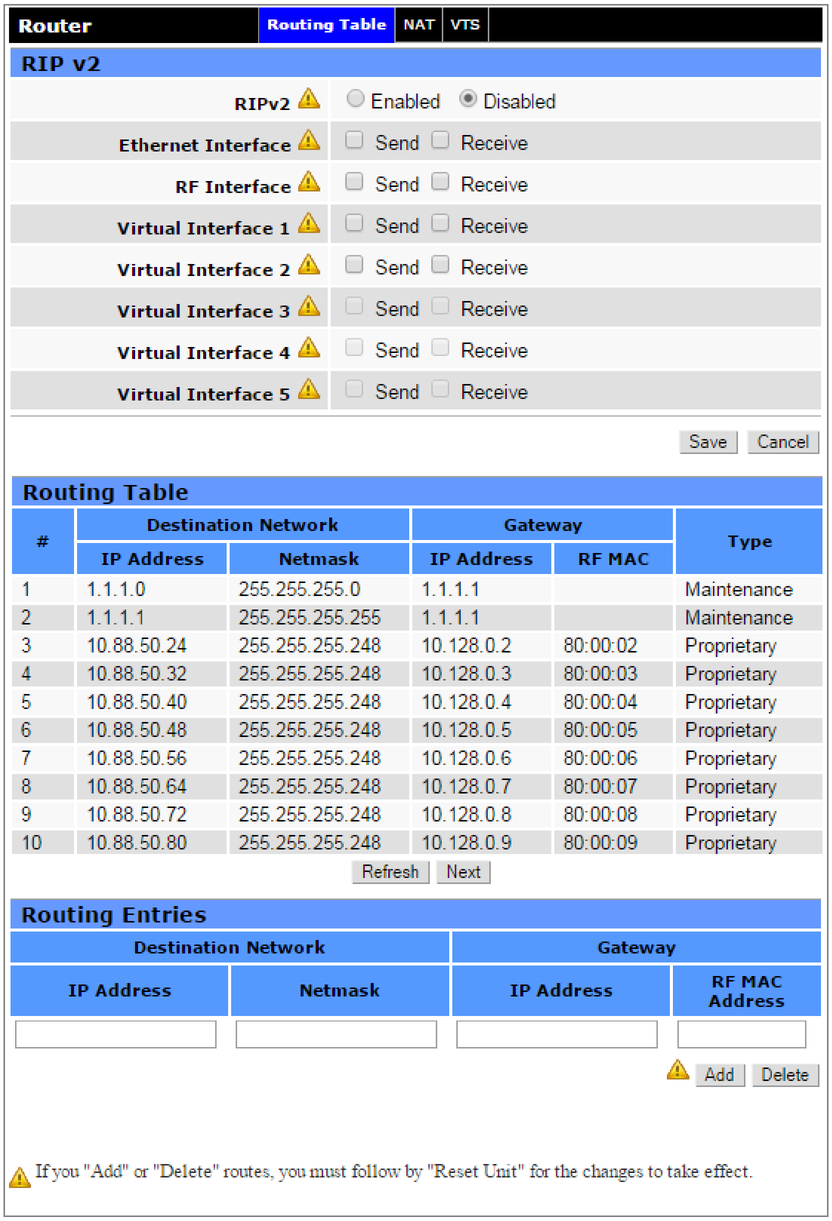
Router

The Router page contains three tabs: Routing Table, NAT, and VTS.

4.4.7. ROUTING TABLE

Routing Table is the first (left-most) tab in the Router page. To navigate to this tab, select RF Network Settings from the main menu and click Routing Table. The Viper supports RIPV2 (Routing Information Protocol version 2). This tab allows you to enable or disable RIPv2, view the routing table and connection type and add or delete routing entries.

Figure 50 – Router – Routing Table



RIP v2

RIPv2 ⚠	○ Enabled ● Disabled
Ethernet Interface ⚠	□ Send □ Receive
RF Interface ⚠	□ Send □ Receive
Virtual Interface 1 ⚠	□ Send □ Receive
Virtual Interface 2 ⚠	□ Send □ Receive
Virtual Interface 3 ⚠	□ Send □ Receive
Virtual Interface 4 ⚠	□ Send □ Receive
Virtual Interface 5 ⚠	□ Send □ Receive

Routing Table

#	Destination Network		Gateway		Type
	IP Address	Netmask	IP Address	RF MAC	
1	1.1.1.0	255.255.255.0	1.1.1.1		Maintenance
2	1.1.1.1	255.255.255.255	1.1.1.1		Maintenance
3	10.88.50.24	255.255.255.248	10.128.0.2	80:00:02	Proprietary
4	10.88.50.32	255.255.255.248	10.128.0.3	80:00:03	Proprietary
5	10.88.50.40	255.255.255.248	10.128.0.4	80:00:04	Proprietary
6	10.88.50.48	255.255.255.248	10.128.0.5	80:00:05	Proprietary
7	10.88.50.56	255.255.255.248	10.128.0.6	80:00:06	Proprietary
8	10.88.50.64	255.255.255.248	10.128.0.7	80:00:07	Proprietary
9	10.88.50.72	255.255.255.248	10.128.0.8	80:00:08	Proprietary
10	10.88.50.80	255.255.255.248	10.128.0.9	80:00:09	Proprietary

Routing Entries

Destination Network		Gateway	
IP Address	Netmask	IP Address	RF MAC Address

⚠ If you "Add" or "Delete" routes, you must follow by "Reset Unit" for the changes to take effect.

RIPv2

RIPv2: RIPv2 (Router Information Protocol version 2) is a dynamic IP routing protocol based on the distance vector algorithm. RIPv2 is used only in Router mode. The default setting is Disabled. When enabled, select which interfaces that you want to enable or disable RIP updates:

Send: Viper radio will broadcast RIP updates on the specified interface.
Receive: Viper radio will listen for RIP updates on the specified interface.

Save: Click Save to save the change if you change RIPv2 from Enabled to Disabled or from Disabled to Enabled. See Note below.

Cancel: Click Cancel to cancel any change you may have made to enable or disable RIPv2.

Note: If you change the RIPv2 Enabled or Disabled setting in this tab, a reset of the Viper is required before the setting will take effect, as indicated by the yellow alert symbol (⚠).

Routing Table

The Routing Table area displays a table of IP routes that are active in the Viper.

In general, the Viper's routing table is populated by the entries in the Neighbor Table. However, there are some instances in which routes may be required to be entered manually, but in most cases the Neighbor Table entries will be enough.

– A row number that the Viper uses internally to organize routing entries in the Routing Table.

Destination Network:

IP Address. Displays the IP Address of the Destination Network.

Netmask. Together with the IP Address, the Netmask determines the subnet of the Destination Network.

Gateway

IP Address. Displays the IP Address of the Gateway.
RF MAC. If the route to the Gateway is pointing to another Viper, the RF MAC address is displayed in this column.

Type: There are three different types of routes.

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

Refresh: Click Refresh to update the Neighbor Table to show the most recent information available.

Routing Entries

Fields in the Routing Entries section of the Routing Table tab allow you to manually add or delete entries to or from the Routing Table above.

Destination Network

IP Address

Enter the IP Address for the Destination Network.

Netmask

Enter the Netmask for the Destination Network.

Gateway

IP Address

Enter the IP Address for the Gateway.

RF MAC Address

Enter the RF MAC Address of the destination Gateway

Add: To add a Routing Entry, enter the IP Address and Netmask of the Destination Network and the IP Address and RF MAC Address of the Gateway for the Routing Entry to be added, and then click Add. See Note below.

Delete: To remove an entry from the Routing Table, enter the IP Address and Netmask of the Destination Network and the IP Address and RF MAC Address of the Gateway shown in the table above, and then click Delete. See Note below.

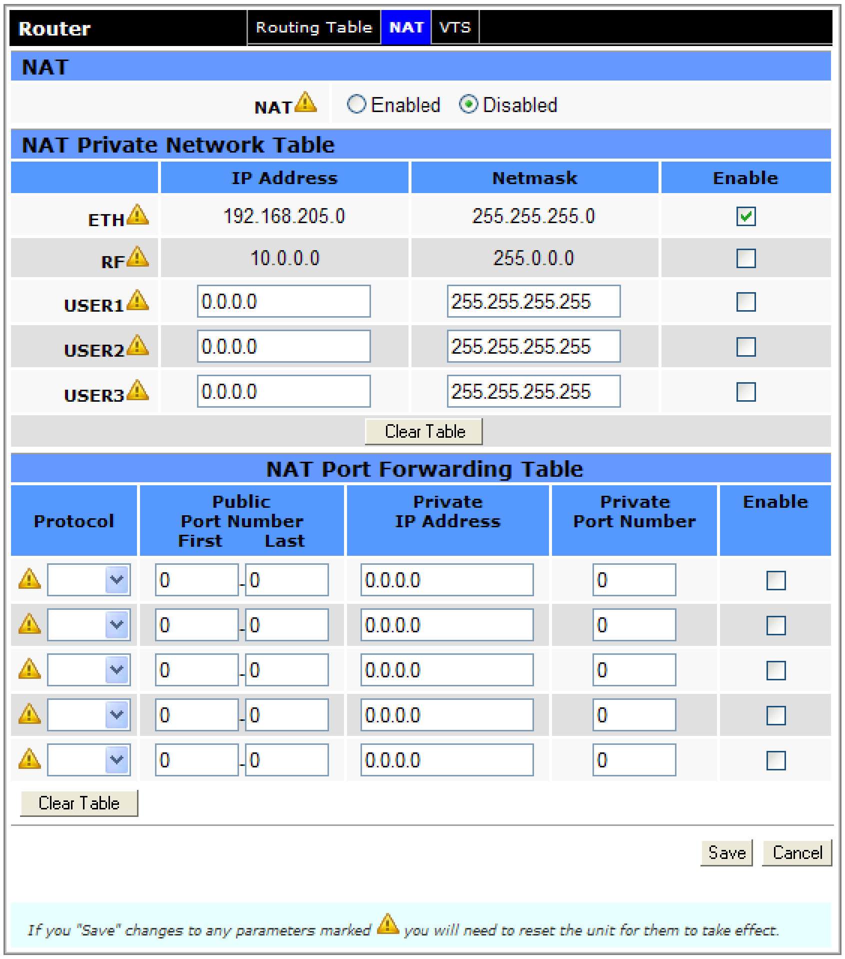
Note: If you Add or Delete routing entries in the Routing Table, a reset of the Viper is required before the routing table change will take effect, as indicated by the yellow alert symbol (⚠).

4.4.8. NAT

NAT (Network Address Translation) is the second (middle) tab of the Router page. To navigate to this tab, select Router from the main menu and click NAT. From this tab, you can enable or disable Network Address Translation, maintain a Private Network Table for NAT and NAT Port Forwarding Table.

NAT technology is a method by which IP addresses are mapped from one address space to another. In Viper, it is normally used on the WAN side of an IP network to hide local IP addresses from an external IP network (that is, the Internet). On Viper units, the user can select which one of the two interfaces (Ethernet or RF) will be considered private.

Figure 51 – Router – NAT



NAT

NAT⚠ ○ Enabled ● Disabled

NAT Private Network Table

	IP Address	Netmask	Enable
ETH⚠	192.168.205.0	255.255.255.0	☑
RF⚠	10.0.0.0	255.0.0.0	□
USER1⚠	0.0.0.0	255.255.255.255	□
USER2⚠	0.0.0.0	255.255.255.255	□
USER3⚠	0.0.0.0	255.255.255.255	□

NAT Port Forwarding Table

Protocol	Public Port Number First	Public Port Number Last	Private IP Address	Private Port Number	Enable
⚠	0	0	0.0.0.0	0	□
⚠	0	0	0.0.0.0	0	□
⚠	0	0	0.0.0.0	0	□
⚠	0	0	0.0.0.0	0	□
⚠	0	0	0.0.0.0	0	□

If you "Save" changes to any parameters marked ⚠ you will need to reset the unit for them to take effect.

NAT

NAT: NAT may be enabled or disabled on the Viper. The default setting is Disabled.

NAT Private Network Table

Parameters in this section allow customization of the NAT firewall protection.

ETH (hidden by NAT): The Network Address Translation table hides IP Addresses on the Ethernet side when enabled.

RF (Hidden by NAT): The Network Address Translation table hides IP Addresses on the RF side when enabled.

User1, User2, User3 : Specific IP Addresses or Subnets can be specified and will be hidden by the Network Address table when the IP Address and Netmask are entered into the row and enabled.

Clear Table: Click Clear Table to clear all entries from the NAT Private Network Table.

NAT Port Forwarding Table

This table allows entry of specific public ports or ranges of ports to be forwarded to the private network hidden by the Network Address Translation table.

Clear Table: Click Clear Table to clear all entries from the NAT Port Forwarding Table.

Save: Click Save to save the change if you enable or change any of the settings in this tab. See Note below.

Cancel: Click Cancel to cancel any change you may have made to any of the settings in this tab.

Note: If you change the NAT Enabled or Disabled setting in this tab, a reset of the Viper is required before the setting will take effect, as indicated by the yellow alert symbol (⚠).

For more information about Network Address Translation (NAT) capabilities of the Viper and how it is implemented in the Viper router, including an overview and examples, see APPENDIX G– NAT Overview.

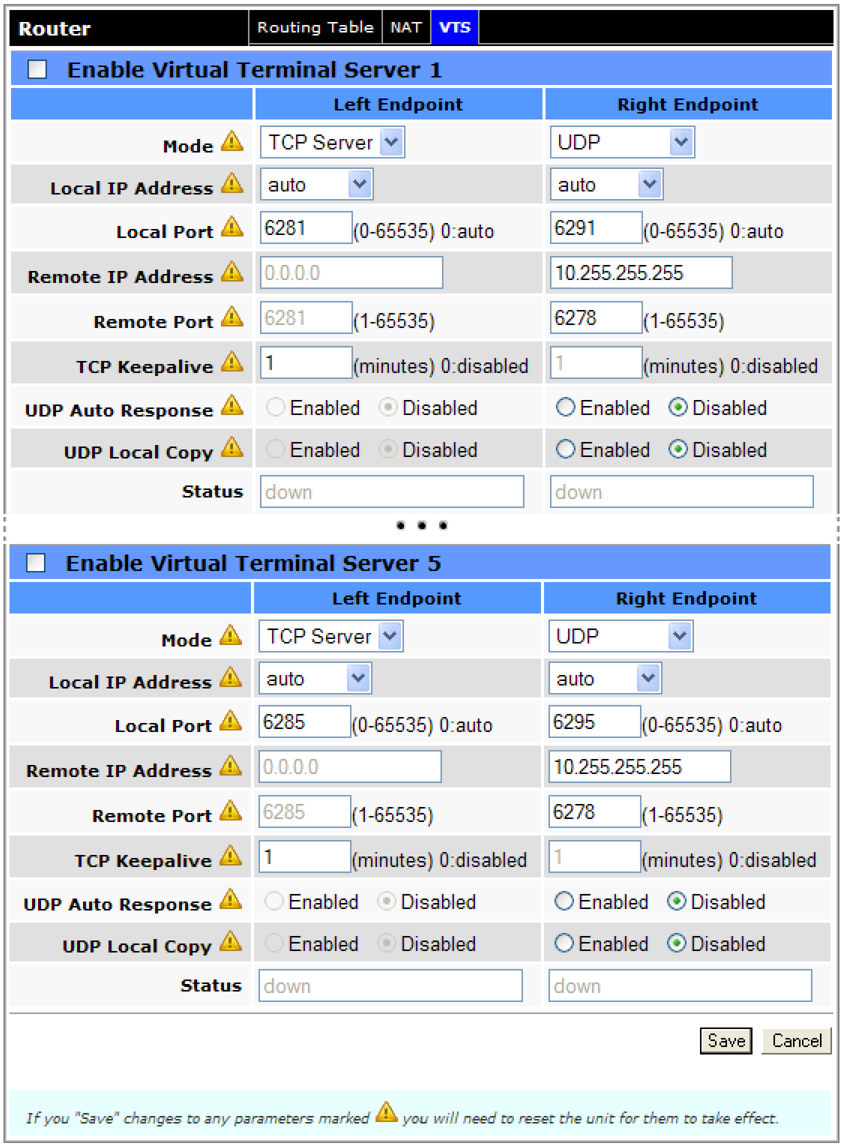
4.4.9. VTS

VTS (Virtual Terminal Server) is the third (right-most) tab of the Router page. To navigate to this tab, select Router from the main menu and click VTS. From this tab you can configure the Virtual Terminal Server parameters.

The Virtual Terminal Server (VTS) is an application running inside the Viper that creates two socket endpoints. One socket endpoint is called “left” and the other is called “right.” Any data received from the left socket endpoint is sent over the right socket endpoint. Any data received from the right socket endpoint is sent over the left socket endpoint. The socket endpoints can operate in TCP server mode, TCP client mode, or UDP mode.

Up to five (5) Virtual Terminal Servers can be configured and enabled. Each Virtual Terminal Server that is enabled works independently of any others.

Figure 52 – Router – VTS



Router | Routing Table | NAT | VTS

□ Enable Virtual Terminal Server 1

	Left Endpoint	Right Endpoint
Mode ⚠	TCP Server	UDP
Local IP Address ⚠	auto	auto
Local Port ⚠	6281 (0-65535) 0:auto	6291 (0-65535) 0:auto
Remote IP Address ⚠	0.0.0.0	10.255.255.255
Remote Port ⚠	6281 (1-65535)	6278 (1-65535)
TCP Keepalive ⚠	1 (minutes) 0:disabled	1 (minutes) 0:disabled
UDP Auto Response ⚠	○ Enabled ● Disabled	○ Enabled ● Disabled
UDP Local Copy ⚠	○ Enabled ● Disabled	○ Enabled ● Disabled
Status	down	down

• • •

□ Enable Virtual Terminal Server 5

	Left Endpoint	Right Endpoint
Mode ⚠	TCP Server	UDP
Local IP Address ⚠	auto	auto
Local Port ⚠	6285 (0-65535) 0:auto	6295 (0-65535) 0:auto
Remote IP Address ⚠	0.0.0.0	10.255.255.255
Remote Port ⚠	6285 (1-65535)	6278 (1-65535)
TCP Keepalive ⚠	1 (minutes) 0:disabled	1 (minutes) 0:disabled
UDP Auto Response ⚠	○ Enabled ● Disabled	○ Enabled ● Disabled
UDP Local Copy ⚠	○ Enabled ● Disabled	○ Enabled ● Disabled
Status	down	down

Save Cancel

If you "Save" changes to any parameters marked ⚠ you will need to reset the unit for them to take effect.

Enable Virtual Terminal Server 1 through 5

Enable Virtual Server 1, Enable Virtual Server 2, Enable Virtual Server 3, … Enable Virtual Server 5

To enable an instance of the Virtual Terminal Server, click to place a check mark in the box.

Mode: There are three modes available.

- **TCP Server mode**: Up to 128 TCP clients can connect to the TCP server.
- **TCP Client mode**: The client will attempt connection to the TCP server identified by the remote address and remote port number.
- **UDP**: Receive UDP packets on the local port number and send UDP packets to the remote address and remote port number.

Local IP Address: The source IP Address of outgoing packets is selected either automatically (by the IP stack) or it can be fixed to the IP address associated with any of the interfaces.

Local Port: The port used to accept incoming packets.

Remote IP Address: The IP address packets are to be sent to.

Remote Port: IP packets are sent to the remote IP address for the application associated with the port number entered.

TCP Keepalive: This parameter is expressed in minutes. The minimum value, zero (0), disables this feature. The maximum allowed value is 1440 minutes (which is equal to 24 hours or 1 day).

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 for the amount of time specified. 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 will close the existing TCP connection.

To disable this feature, set the TCP keepalive to 0 (zero). With the TCP keepalive feature disabled, the Viper will leave the TCP connection open indefinitely. An existing TCP connection will only close if the remote endpoint closes the connection or if the Viper is unable to successfully communicate with the remote endpoint during a data transmission.

UDP Auto-Response: When sending a UDP packet, do not use the remote port and remote IP address configured, but rather sent to the IP address and port number of the last UDP packet received. When this feature is enabled, any packet to be transmitted is dropped until at least one packet has been received.

UDP Local Copy: When the socket operates in UDP mode and the remote address is a multicast (or limited broadcast) address, the packet can be sent out without giving a copy to internal applications. Local Copy enabled means a copy of the packet is sent to internal applications. Local Copy disabled means do not send a copy of the packet to internal applications.

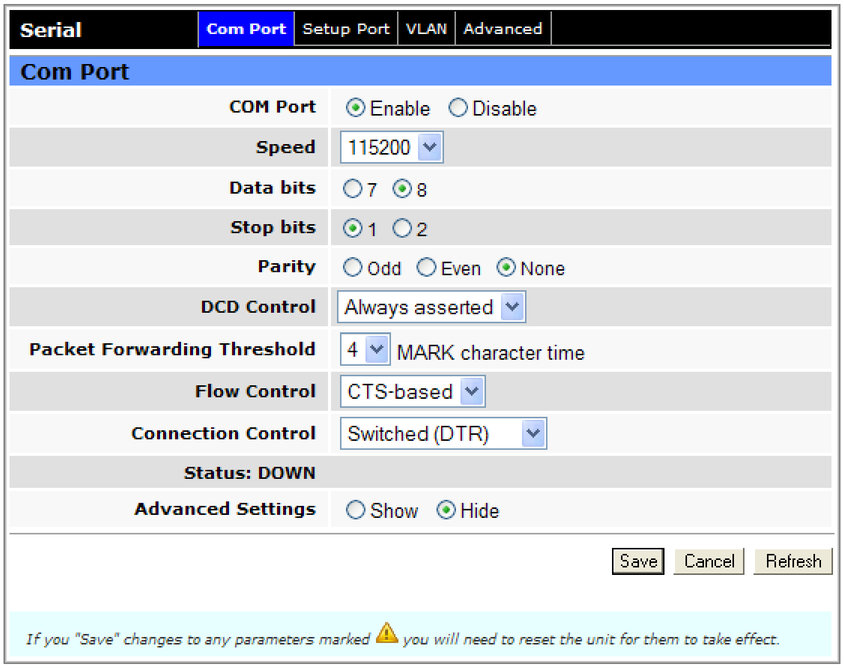
Status: Status of the TCP Server mode may display as down or listening (N TCP Clients up).
Status of the TCP Client mode may display as down, connecting, or up.
Status of UDP may display as down or up.

The Serial page contains four tabs: Com Port, Serial Port, VLAN, and Advanced.

4.4.10. COM PORT AND SETUP PORT

COM Port is the first (left-most) tab, and the Setup Port tab is next to it to the right. To navigate to the COM Port tab, select Serial from the main menu; to navigate to the Setup Port tab, select Serial from the main menu and then select Setup Port. The two tabs are nearly identical and provide access to all the same settings—the only difference is the port that the configuration settings are for. In each of the two tabs, you can enable or disable the applicable port and set serial communication parameters for it.

Figure 53 – Serial – COM Port

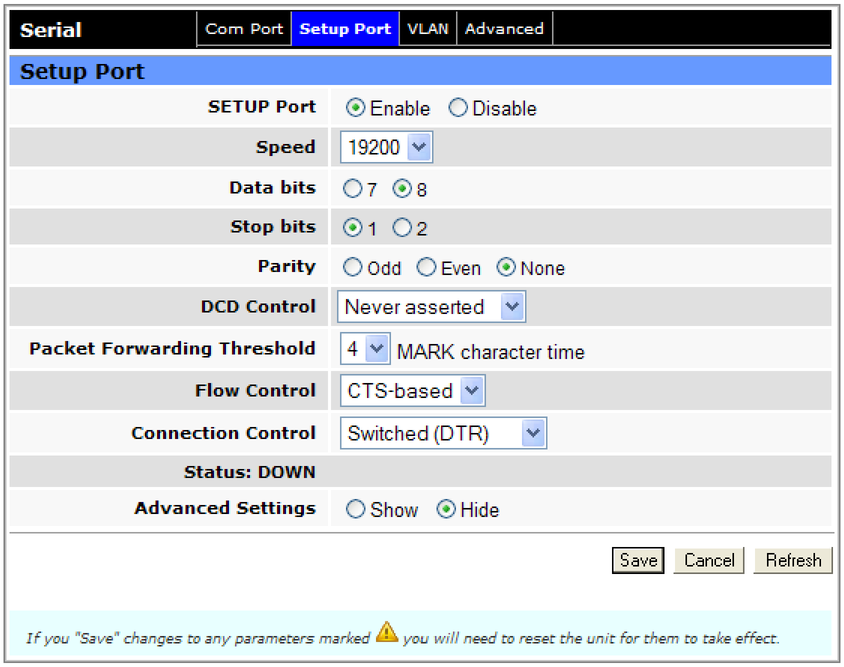


Com Port

COM Port	● Enable ○ Disable
Speed	115200
Data bits	○ 7 ● 8
Stop bits	● 1 ○ 2
Parity	○ Odd ○ Even ● None
DCD Control	Always asserted
Packet Forwarding Threshold	4 MARK character time
Flow Control	CTS-based
Connection Control	Switched (DTR)
Status: DOWN	
Advanced Settings	○ Show ● Hide

If you "Save" changes to any parameters marked ⚠ you will need to reset the unit for them to take effect.

Figure 54 – Serial – Setup Port



Setup Port

SETUP Port	● Enable ○ Disable
Speed	19200
Data bits	○ 7 ● 8
Stop bits	● 1 ○ 2
Parity	○ Odd ○ Even ● None
DCD Control	Never asserted
Packet Forwarding Threshold	4 MARK character time
Flow Control	CTS-based
Connection Control	Switched (DTR)
Status: DOWN	
Advanced Settings	○ Show ● Hide

If you "Save" changes to any parameters marked ⚠ you will need to reset the unit for them to take effect.

COM Port or Setup Port

COM Port or Setup Port: Each port may be enabled or disabled. The default setting is Enabled.

Speed: Select a 300, 1200, 2400, 4800, 9600, 19200, 38400, 56700, or 115200 baud rate for the COM Port.
Note: The Setup Port is limited to 19200. This should be configured to match the settings of the connected device.

- **COM Port**: The default baud rate for the COM Port is 9600.
- **Setup Port:** The default baud rate for the Setup Port is 19200.

Data Bits: Number of bits making up each "word" of data. This is set according to the Host configuration and should be configured to match the settings of the connected device. The default setting is 8.

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

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

DCD Control: The DCD (Data Carrier Detect) line can be set for one of the following: Always Asserted, Never Asserted, or Envelope Mode (the DCD will be asserted only when data is present at the serial port). This should be configured to match the settings of the connected device. The default setting is Envelope Mode.

Packet Forwarding Threshold: Allows you to change the Mark Character time for forwarded packets based on the character length. Possible selections are two (2) through (8), inclusive. The default setting is four (4).

Flow Control: Allows the implementation of RTS/CTS flow control or None. This should be configured to match the setting of the connected device. The default setting is CTS-Based.
Note: Request to Send and Clear to Send flow control will require a five-wire connection to the COM port or Setup port.

Connection Control: Select Permanent (3-wire) when the serial port is always enabled or select Switched (DTR bring up/teardown) when DTR is used to enable or disable the serial connection. This should be configured to match the settings of the connected device. The default setting is Permanent (3-wire)

Status: Displays the status of the serial connection. Whether the connection is ready or down.

Advanced Settings (Show or Hide): Click **Show** to show advanced settings in the lower part of the tab; click **Hide** to hide the advanced settings.

Save: Click Save to save the settings if you have changed any of the settings in this tab.

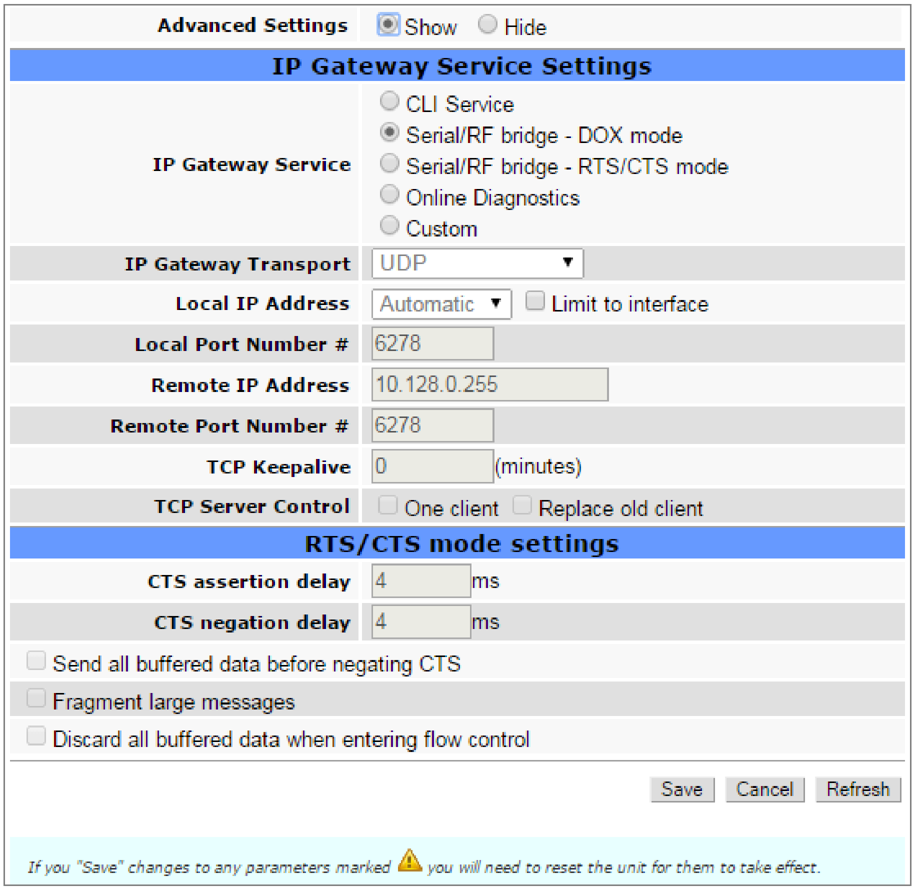
Cancel: Click Cancel to cancel any change you may have made to any of the settings in this tab.

Refresh: Click Refresh to reload the tab with the settings currently in effect.

4.4.10.1. Advanced Settings for Serial » COM Port or Setup Port

When you click **Show** to show the advanced settings in the COM Port or Setup Port tab for the Serial page, the tab expands downward to show the advanced settings. The following figure shows the Advanced Settings section of the Serial » COM Port tab. The Advanced Settings section of the Serial » Setup Port tab contains the same options in the IP Gateway Service Settings section as the COM Port tab, but the Setup Port tab does not have the RTS/CTS mode settings section below.

Figure 55 – Serial – COM Port or Setup Port tab showing Advanced Settings only



Advanced Settings	● Show ○ Hide

IP Gateway Service Settings

IP Gateway Service	○ CLI Service ● Serial/RF bridge - DOX mode ○ Serial/RF bridge - RTS/CTS mode ○ Online Diagnostics ○ Custom
IP Gateway Transport	UDP
Local IP Address	Automatic □ Limit to interface
Local Port Number #	6278
Remote IP Address	10.128.0.255
Remote Port Number #	6278
TCP Keepalive	0 (minutes)
TCP Server Control	□ One client □ Replace old client

RTS/CTS mode settings

CTS assertion delay	4 ms
CTS negation delay	4 ms

□ Send all buffered data before negating CTS

□ Fragment large messages

□ Discard all buffered data when entering flow control

If you "Save" changes to any parameters marked ⚠ you will need to reset the unit for them to take effect.

The Advanced Settings provide options for configuring IP Gateway Service Settings for the COM Port and Setup Port. For the COM Port, options are also provided for configuring RTS/CTS Mode Settings.

IP Gateway Service Settings

IP Gateway Service: Each Serial port can be configured for one of several IP Gateway Services listed.

- The default setting for the COM Port is Serial/RF bridge – DOX mode.
- The default setting for the Setup Port is CLI Service.

CLI (Command-Line Interface) Service: This interface provides a command line interface over an RS-232 connection to a Hose PC. Check with NextGen RF Technical Support for advanced CLI information.

Serial/RF Bridge – DOX mode: This is a three-wire connection. 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.

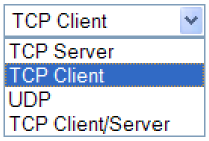
Serial/RF Bridge – RTS/CTS mode : This is a five-wire connection. Data is sent after the device raises the RTS and the Viper returns a CTS signal to the device.

Online Diagnostics: This is a TCP/IP based RF diagnostics mode. Displays the time interval (in seconds) when the Online Diagnostics string will be transmitted.

Custom: Allows you to customize the IP settings by selecting this setting. Choose the socket connection mode from the IP Gateway Transport list and configure the IP settings.

IP Gateway Transport:

Select one of four modes of transport, TCP Server, TCP Client, UDP, or TCP Client/Server. Parameters for each of these modes are defined in Table 15 TCP/UDP Parameter Usage, which follows.



TCP Server Mode: In this mode of operation, the Viper acts as a TCP server. It can accept up to 256 TCP connections from remote endpoints. Data received from any remote endpoint is sent over the serial port. Data received from the serial port is sent to every endpoint connected to the TCP server.

- **Local Port Number** – In TCP Server mode, you must set the local port number parameter. It identifies the port used by the TCP server when accepting connections from the remote endpoints.
- **Remote IP Address** and **Remote Port Number** – These parameters are not used In TCP Server mode.

TCP Client Mode: In this mode of operation, the Viper (local endpoint) tries to establish a TCP connection with a TCP server (remote endpoint). Once the TCP connection is established, any data received from the remote endpoint is sent over the serial interface. Any data received from the serial interface is sent to the remote endpoint.

- **Local Port Number** – This parameter is used to identify the local endpoint. The IP stack automatically decides the value assigned to the local port number. You can let the IP stack decide the value of the local IP address (local IP address = 0.0.0.0) or select a specific local IP address (as long as it is the IP address of one of the interfaces, Ethernet or RF.
- **Remote IP Address** and **Remote Port Number** – These two parameters are used to identify the remote endpoint (TCP Server).

UDP Mode: In this mode of operation, all UDP packets addressed to the Local IP Address and the Local Port Number are sent over the serial interface. Any data received from the serial interface is sent over the serial interface

- **Local Port Number** – The local port number parameters are used in reception to indicate which UDP packets are to be sent to the serial port. The local port number parameters are used in transmission to set the source IP address of the IP header and the source port number of the UDP packet.
- **Remote IP Address** and **Remote Port Number** – The remote port number and remote IP address parameters are used in transmission to set the destination IP address of the IP header and the destination port number of the UDP packet.

TCP Client/Server Mode: In this mode of operation, the Viper acts as both 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.

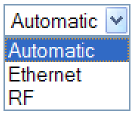
- **Local Port Number** – This parameter is used to define the TCP server.
- **Remote IP Address** and **Remote Port Number** – These parameters are used to define the TCP client. The Viper will try to establish a TCP connection to the remote endpoint defined by these two parameters when there is data received on the serial port AND there are no TCP connections already established.

Table 15 TCP/UDP Parameter Usage

	UDP Mode	TCP Client Mode	TCP Server Mode	TCP Client/Server Mode
Local IP Address	**REQUIRED** **Value** **Automatic** = Let the IP stack decide. **Ethernet** = IP address of the Ethernet interface. **RF** = IP address of the RF interface. **Virtual 1…5** = IP address of the specified virtual interface.	**REQUIRED** **Value** **Automatic** = Let the IP stack decide. **Ethernet** = IP address of the Ethernet interface. **RF** = IP address of the RF interface. **Virtual 1…5** = IP address of the specified virtual interface.	**REQUIRED** **Value** **Automatic** = Let the IP stack decide. **Ethernet** = IP address of the Ethernet interface. **RF** = IP address of the RF interface. **Virtual 1…5** = IP address of the specified virtual interface.	**REQUIRED** **Value** **Automatic** = Let the IP stack decide. **Ethernet** = IP address of the Ethernet interface. **RF** = IP address of the RF interface. **Virtual 1…5** = IP address of the specified virtual interface.
Local Port Number	**REQUIRED** **Value** * 1 - 65535 **Do not use:** 20, 21, 23, 123, 520, or 5002	**UNUSED** **Value** * IP stack decides the value.	**REQUIRED** **Value** * 1 - 65535 **Do not use:** 20, 21, 23, 123, 520, or 5002	**REQUIRED** **Value** * 1 - 65535 **Do not use:** 20, 21, 23, 123, 520, or 5002
Remote IP Address	**REQUIRED** **Value** * Unicast IP address *OR* * Broadcast IP address *OR* * Multicast IP address	**REQUIRED** **Value** * Unicast IP address based on Local IP selection for TCP reply message	**REQUIRED** **Value** N/A	**REQUIRED** **Value** * Unicast IP address based on Local IP selection for TCP reply message
Remote Port Number	**REQUIRED** **Value** * 1 - 65535	**REQUIRED** **Value** * 1 - 65535	**REQUIRED** **Value** * 1 - 65535	**REQUIRED** **Value** * 1 - 65535
TCP Keepalive	**UNUSED**	**OPTIONAL** **Value** ** 0 – 1440 (minutes) (0 = TCP Keepalive is disabled)	**OPTIONAL** **Value** ** 0 – 1440 (minutes) (0 = TCP Keepalive is disabled)	**OPTIONAL** **Value** ** 0 – 1440 (minutes) (0 = TCP Keepalive is disabled)

* Avoid use of reserved port number values. (For example 20, 21, 23, 123, 520, 5002.)

** Setting the value of TCP Keepalive to zero (0) disables the sending of keepalive packets.



Local IP Address: The local IP address for IP Services. The default setting is **Automatic**.

- **Automatic** – The Viper will respond any of the IPs assigned-Ethernet, RF, or virtual.
- **Ethernet** – The Viper will respond only to the Ethernet IP address.
- **RF** – The Viper will respond only to the RF IP address
- **Virtual 1…5** The Viper will respond only to the specified virtual interface.

Limit to Interface: Limit the access to the serial port to only a special class of packets. When this option is selected AND a specific "Local IP Address" is selected, enforce the following rules:

Ingress packets: Destination IP address of packets must be equal to the IP address of the specified interface. If VLAN mode is enabled, the incoming packet must have a VLAN ID matching the interface's PVID.

Egress packets: The source IP address of outgoing packets will be set to the IP address of the specified interface. If the specified interface as a PVID, the VLAN ID set in the packet will be equal to the interface PVID.

TCP Keepalive

The TCP Keepalive feature will transmit a short Keepalive message to test the TCP connection if there is not data transferred through an open TCP connection after the specified number of minutes. If the keepalive message is not received successfully, the Viper will close the existing TCP connection.

To disable this feature, set the TCP keepalive to zero (0). With the TCP keepalive feature disabled, the Viper will leave the TCP connection open indefinitely. An existing TCP connection will only close if the remote endpoint closes the connection, the Viper serial port is disabled, or if the Viper is unable to successfully communicate with the remote endpoint during a data transmission. The default setting is disabled; zero (0) minutes.

TCP Server Control

One client:

Limit the amount of TCP clients to 1. If this option is not checked, the limit of TCP clients is 256.

Replace old client:

When the maximum amount of TCP client is reached, the TCP server can decide to drop an old TCP client in favor of a new TCP client. If this option is selected and there is a new TCP client connecting to the TCP server and the maximum amount of client is already reached, the TCP server will shut down an old TCP client to make room for the new one (otherwise the new one will fail to connect).

RTS/CTS Mode Settings

Note: RTS/CTS Mode Settings apply only to the COM Port and this section does not apply for the Setup Port.

CTS assertion delay: The time in milliseconds (ms) that the data will be displayed after the CTS has been sent. The default setting is 4 milliseconds.

CTS negation delay:

The time in milliseconds (ms) that the CTS will be kept asserted after the last character has been transmitted. The default setting is 4 milliseconds.

Send buffered data before negating CTS: All the data will be sent before the Viper drops the CTS control line.

Fragment large messages: Allows the 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.

Save: Click Save to save the settings if you have changed any of the settings in this tab.

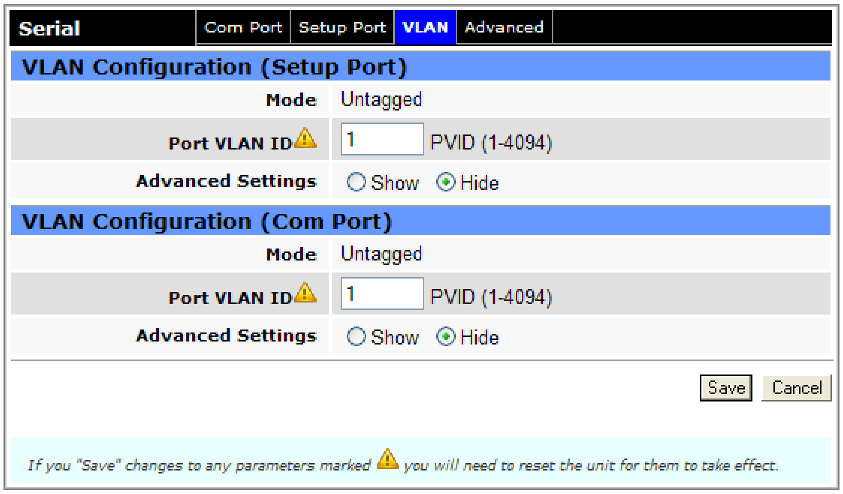
Cancel: Click Cancel to cancel any change you may have made to any of the settings in this tab.

Refresh: Click Refresh to reload the tab with the settings currently in effect.

4.4.11. VLAN

VLAN is the third (from left; second from right) tab in the Serial page. To navigate to this tab, select Serial from the main menu and click VLAN. This tab contains configuration for VLAN set up through either or both of the serial ports (COM or Setup). VLAN configuration settings for both serial ports, Setup and COM, are on this single tab.

Figure 56 – Serial – VLAN



VLAN Configuration (Setup Port)

Mode	Untagged
Port VLAN ID⚠	1 PVID (1-4094)
Advanced Settings	○ Show ● Hide

VLAN Configuration (Com Port)

Mode	Untagged
Port VLAN ID⚠	1 PVID (1-4094)
Advanced Settings	○ Show ● Hide

If you "Save" changes to any parameters marked ⚠ you will need to reset the unit for them to take effect.

VLAN Configuration (Setup Port or COM Port)

Mode: Both serial interfaces, Setup and COM, operate in VLAN Untagged mode only. In Untagged mode, devices on this interface are not using VLAN tags. Incoming (ingress) packets are tagged with the port VLAN ID (PVID). VLAN tags are removed on outgoing (egress) packets. See the Advanced Settings For Serial » VLAN section that follows for more options.

Port VLAN ID: Sets the Port VLAN ID (PVID)

Advanced Settings (Show or Hide): Click **Show** to show advanced settings in the lower part of the tab; click **Hide** to hide the advanced settings.

Save: Click Save to save any changes you have made in this tab. See Note below.

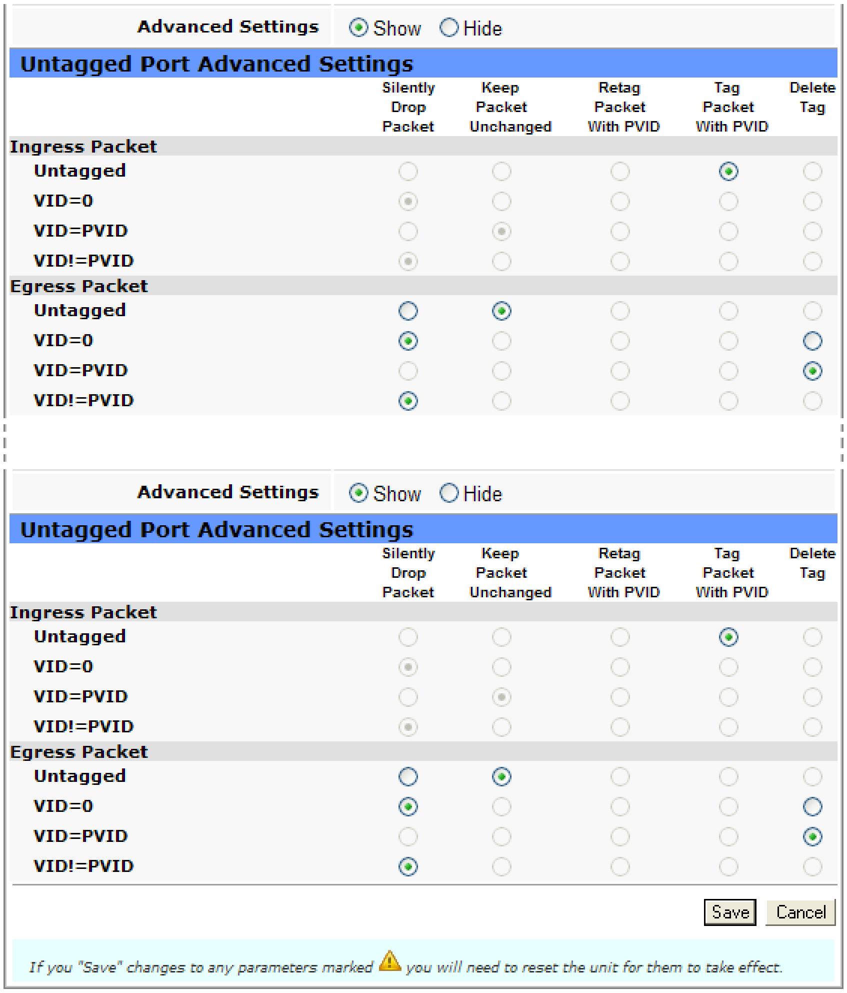
Cancel: Click Cancel to cancel any changes you may have made to any of the settings in this tab.

Note: If you change the Port VLAN ID (PVID) for either serial port, a reset of the Viper is required before the setting will take effect, as indicated by the yellow alert symbol (⚠).

4.4.11.1. Advanced Settings For Serial » VLAN

Advanced Settings are available for both Serial ports (both the Setup and COM port). Advanced settings for VLAN configuration for both serial ports, Setup and COM, are on the same, single tab.

Figure 57 – Serial — VLAN tab Advanced Settings only



Advanced Settings ● Show ○ Hide

Untagged Port Advanced Settings

	Silently Drop Packet	Keep Packet Unchanged	Retag Packet With PVID	Tag Packet With PVID	Delete Tag
Ingress Packet					
Untagged	○	○	○	●	○
VID=0	●	○	○	○	○
VID=PVID	○	●	○	○	○
VID!=PVID	●	○	○	○	○
Egress Packet					
Untagged	○	●	○	○	○
VID=0	●	○	○	○	○
VID=PVID	○	○	○	○	●
VID!=PVID	●	○	○	○	○

Advanced Settings ● Show ○ Hide

Untagged Port Advanced Settings

	Silently Drop Packet	Keep Packet Unchanged	Retag Packet With PVID	Tag Packet With PVID	Delete Tag
Ingress Packet					
Untagged	○	○	○	●	○
VID=0	●	○	○	○	○
VID=PVID	○	●	○	○	○
VID!=PVID	●	○	○	○	○
Egress Packet					
Untagged	○	●	○	○	○
VID=0	●	○	○	○	○
VID=PVID	○	○	○	○	●
VID!=PVID	●	○	○	○	○

If you "Save" changes to any parameters marked ⚠ you will need to reset the unit for them to take effect.

Untagged Port Advanced Settings

Untagged Port Advanced Settings provide options for ingress packets (packets coming into the Viper) and egress packets (packets leaving the Viper) Selections in this section allow you to specify what actions are to be taken with ingress and egress packets, based on their VLAN ID (VID) tag (or absence of a VID tag).

VID is the VLAN ID contained in the packet.
PVID is the Port VLAN ID (the VLAN ID associated with the interface and configured in the Viper Web Interface).

Ingress Packet

Untagged (The packet has no VLAN ID tag): If incoming packets are untagged, you can choose to silently drop these packets, keep them unchanged, or tag the packets with the PVID. The default setting is to tag the packet with the PVID.

VID=0: If incoming packets have a VLAN ID set to zero (0), you can choose to silently drop these packets, keep them unchanged, re-tag the packets with the PVID, or delete their tag. The default setting is to silently drop the packet.

VID=PVID (The packet has a VLAN ID that is the same as the PVID): If incoming packets have a VLAN ID that is the same as the PVID, you can choose to silently drop these packets, keep them unchanged, or delete their tag. The default setting is to keep the packet unchanged.

VID!=PVID (VID is not equal to PVID): If incoming packets have a VLAN ID that is not the same as the PVID, you can choose to silently drop these packets, keep them unchanged, re-tag the packets with PVID, or delete their tag. The default setting is to silently drop the packet.

Egress Packet

Untagged (The packet has no VLAN ID tag): If exiting packets are untagged, you can choose to silently drop these packets, keep them unchanged, or tag them with PVID. The default setting is to keep the packet unchanged.

VID=0: If exiting packets have a VLAN ID set to zero (0), you can choose to silently drop these packets, keep them unchanged, re-tag them with PVID, or delete their tag. The default setting is to silently drop the packet.

VID=PVID (The packet has a VLAN ID that is the same as the PVID): If exiting packets have a VLAN ID that is the same as the PVID, you can choose to silently drop these packets, keep them unchanged, or delete their tag. The default setting is to delete the tag.

VID!=PVID (VID is not equal to PVID) If exiting packets have a VLAN ID that is not the same as the PVID, you can choose to silently drop these packets, keep them unchanged, re-tag the packets with PVID, or delete their tag. The default setting is to silently drop the packet.

Save: Click Save to save any changes you have made in this tab. See the Note that follows.

Cancel: Click Cancel to cancel any changes you may have made to any of the settings in this tab.

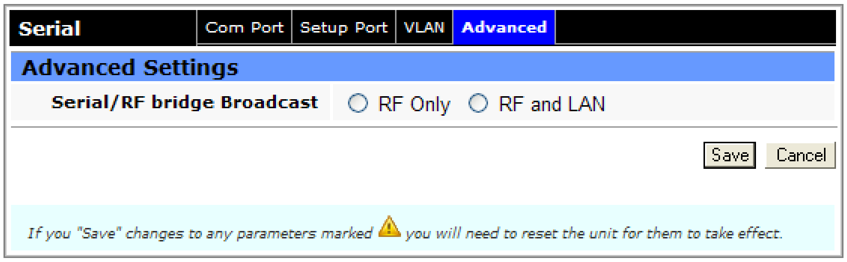
Note: If you change the Port VLAN ID (PVID) for either serial port, a reset of the Viper is required before the setting will take effect, as indicated by the yellow alert symbol (⚠).

4.4.12.ADVANCED

Advanced is the fourth (right-most) tab of the Serial page. To navigate to this tab, select Serial from the main menu and click Advanced. In this tab you can select if Serial/RF bridge Broadcast will be RF Only or RF and LAN.

The parameter in this tab only has meaning when operating in Bridge mode.

Figure 58 – Serial – Advanced



Advanced Settings

Serial/RF bridge Broadcast ○ RF Only ○ RF and LAN

If you "Save" changes to any parameters marked ⚠ you will need to reset the unit for them to take effect.

Advanced Settings

Serial RF Bridge Broadcast: When a serial port is operating in Serial/RF Bridge mode, the packets received by the Viper from the serial port are sent over RF to all remote Vipers so they can pass this data over their corresponding serial port. The sending Viper achieves this by using a broadcast IP address. On reception, the remote Viper will pass this data over its serial port AND optionally send the data over its LAN port.

RF Only:

- When receiving Serial/RF bridge data from a remote Viper over RF, pass it to the corresponding serial port and do not send a copy of the data over the LAN port.
- When transmitting Serial/RF bridge data to remote Vipers over RF, do not send a copy on the LAN port.

RF and LAN:

- When receiving Serial/RF bridge data from a remote Viper over RF, pass it to the corresponding serial port and send a copy of the data over to the LAN port.
- When transmitting Serial/RF bridge data to remote Vipers over RF, send a copy over the LAN port.

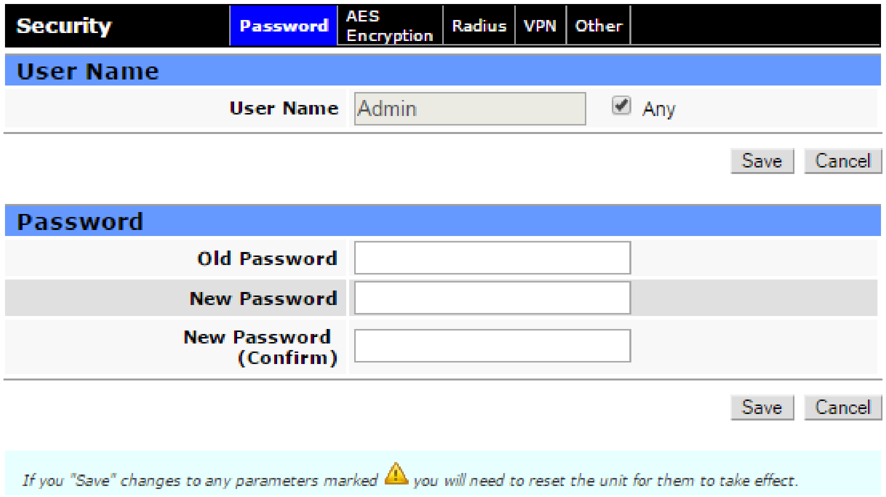
4.5. SECURITY

The Security page contains four tabs: Password, AES Encryption, RADIUS, and VPN.

4.5.1. PASSWORD

Password is the first (left-most) tab of the Security page. To navigate to this tab, select Security from the main menu. This tab allows you to set Usernames and assign and change passwords for users of the Viper to log in to the Viper Web interface.

Figure 59 – Security – Password



User Name

User Name: Admin ☑ Any

Password

Old Password:

New Password:

New Password (Confirm):

If you "Save" changes to any parameters marked ⚠ you will need to reset the unit for them to take effect.

Username

Username: This field allows you to add new usernames for security on the Viper. For initial installation, all Vipers are shipped with the default Username of Admin. If you want the Viper to check the password only at log in and not require a valid username to be entered, click to place a check in the box labeled Any.

Note: If you are using a RADIUS server, the Username will always be required.

Password

Old Password: For initial installation, the default password for the Admin username is ADMINISTRATOR (all uppercase letters). For subsequent access, use the current password.

New Password: Enter a string of any letters or numbers of at least 8 characters and not exceeding 15 characters in length.

CAUTON: Do not lose the new password or you will not be able to gain access to the unit. If you lose your password, you will need to contact NextGen RF for technical support.

New Password (Confirm): Re-enter the new password string you entered above.

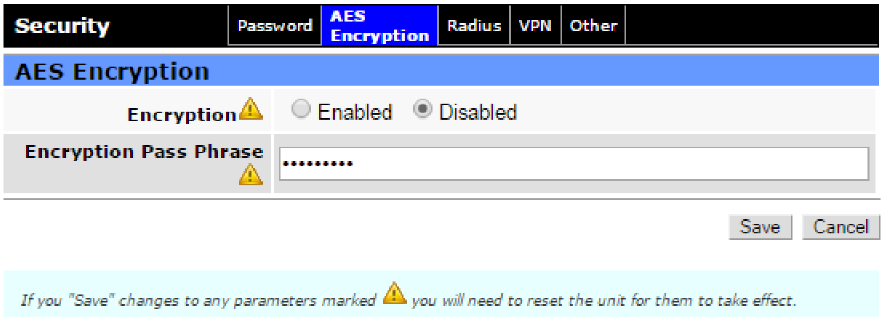
Save: Click Save to save any new username or password changes you have made in this tab. You will need to enter your new password the next time you log in to the Viper.

Cancel: Click Cancel to cancel any changes you may have made in this tab.

4.5.2. AES ENCRYPTION

AES (Advanced Encryption Standard) is the second (from left) tab of the Security page. To navigate to this tab, select Security from the main menu and click AES Encryption. This tab allows you to enable or disable AES Encryption and set the Encryption Pass Phrase.

Figure 60 – Security – AES Encryption



Encryption ⚠ ○ Enabled ● Disabled

Encryption Pass Phrase ⚠ •••••••••

If you "Save" changes to any parameters marked ⚠ you will need to reset the unit for them to take effect.

AES Encryption

Encryption: When enabled, 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 default setting is disabled.

Encryption Pass Phrase: If encryption is enabled, enter a string of characters used to create an AES 128-bit encryption key. The pass phrase can be up to 160 characters long. Using a phrase-length of at least 128 characters should provide an adequate security level for most networks. A good pass phrase mixes alphabetic and numeric characters and avoids easy-to-guess simple names or prose.
Note: The encryption pass phrase and key must be common to all units in each network.

Save: Click Save to save any changes you make in this tab. See the Note that follows.

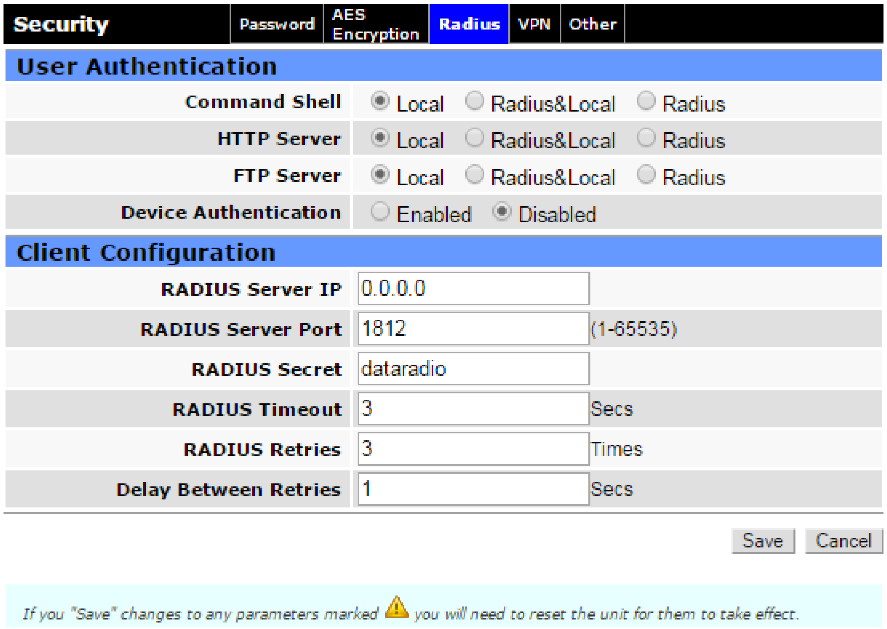
Cancel: Click Cancel to cancel any changes you may have made in this tab.

Note: If you enable or disable encryption or set a new encryption pass phrase, a reset of the Viper is required before any new setting(s) will take effect, as indicated by the yellow alert symbol (⚠).

4.5.3. RADIUS

RADIUS (Remote Authentication Dial In User Service) is the third (from left) tab of the Security page. To navigate to this tab, select Security from the main menu and click RADIUS. This tab allows you to make settings for User Authentication and Client Configuration for RADIUS security.

Figure 61 – Security – RADIUS



User Authentication

Command Shell	● Local ○ Radius&Local ○ Radius
HTTP Server	● Local ○ Radius&Local ○ Radius
FTP Server	● Local ○ Radius&Local ○ Radius
Device Authentication	○ Enabled ● Disabled

Client Configuration

RADIUS Server IP	0.0.0.0	
RADIUS Server Port	1812	(1-65535)
RADIUS Secret	dataradio	
RADIUS Timeout	3	Secs
RADIUS Retries	3	Times
Delay Between Retries	1	Secs

If you "Save" changes to any parameters marked ⚠ you will need to reset the unit for them to take effect.

User Authentication

Command Shell, HTTP Server, and FTP Server: Each of these services (Command Shell, HTTP Server, and FTP Server) can be set for one of three possible options: **Local**, **RADIUS and Local**, or **RADIUS**. Each of these options is explained below.

Local: When accessing the service, check the user credentials (username and password) against credentials stored in the Viper. The user will not be able to access the service if proper credentials are not provided.

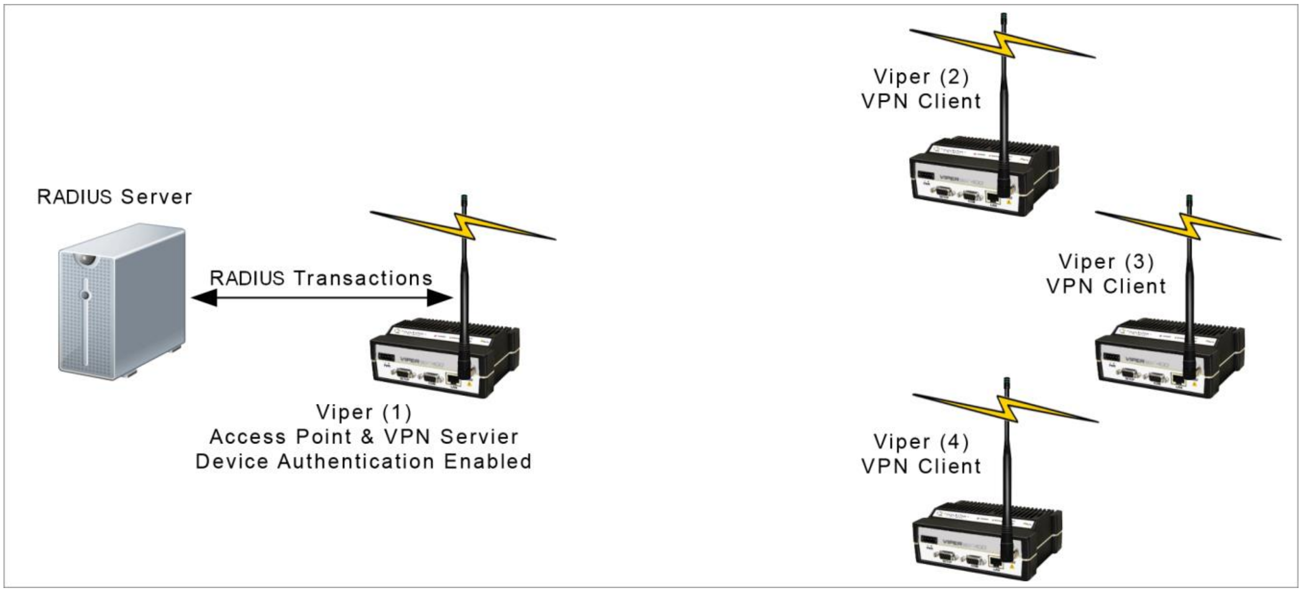
RADIUS And Local: When accessing the service, check the user credentials (username and password) against credentials stored in the Viper. If the credentials fail to match credentials stored in the Viper, check for a match against credentials stored in the RADIUS server database.

RADIUS: When accessing the service, check the user credentials (username and password) against the RADIUS server database. If the user credentials fail to pass with the RADIUS server, access to the service is denied.

Device Authentication: When enabled, Viper performs local and remote device authentication using a RADIUS server. Set the VPN module of the Viper (local) to operate in server mode and set the VPN module of remote devices to operate in client mode. The Viper will authenticate remote devices using the RADIUS server when they are powered on and at regular intervals. The Viper will authenticate itself to the RADIUS server at startup. The default setting is disabled.

The following figure 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 62 – Device Authentication



To utilize device authentication, your network must use the following parameters: The master device (Viper 1) must have Device Authentication Enabled and must be configured as an Access Point (RF Network Settings » RF Network) and a VPN Server (Security » VPN). All remote devices (Vipers 2,3 & 4) must have VPN Enabled and must be configured as VPN Clients (Security » VPN).

Client Configuration

RADIUS Server IP: IP Address of the RADIUS server.

RADIUS Server Port: UDP port number to use when sending authentication requests to the RADIUS server.

RADIUS Secret: Secret key shared between the RADIUS client and RADIUS server. This key is used to encrypt messages exchanged between the client and server application.

RADIUS Timeout: Amount of time (in seconds) to wait for a response when sending an authentication request to the RADIUS server. If the response is not received, the request will be resent as many times as specified by the RADIUS Retries setting.

RADIUS Retries: Number of times the RADIUS client resends the authentication request message to the RADIUS server if it does not respond with an authentication granted or authentication denied message.

Delay Between Retries: Amount of time (in seconds) to wait between retries when sending the RADIUS authentication request to the RADIUS server.

Save: Click Save to save any changes you make in this tab.

Cancel: Click Cancel to cancel any changes you may have made in this tab.

4.5.4. VPN

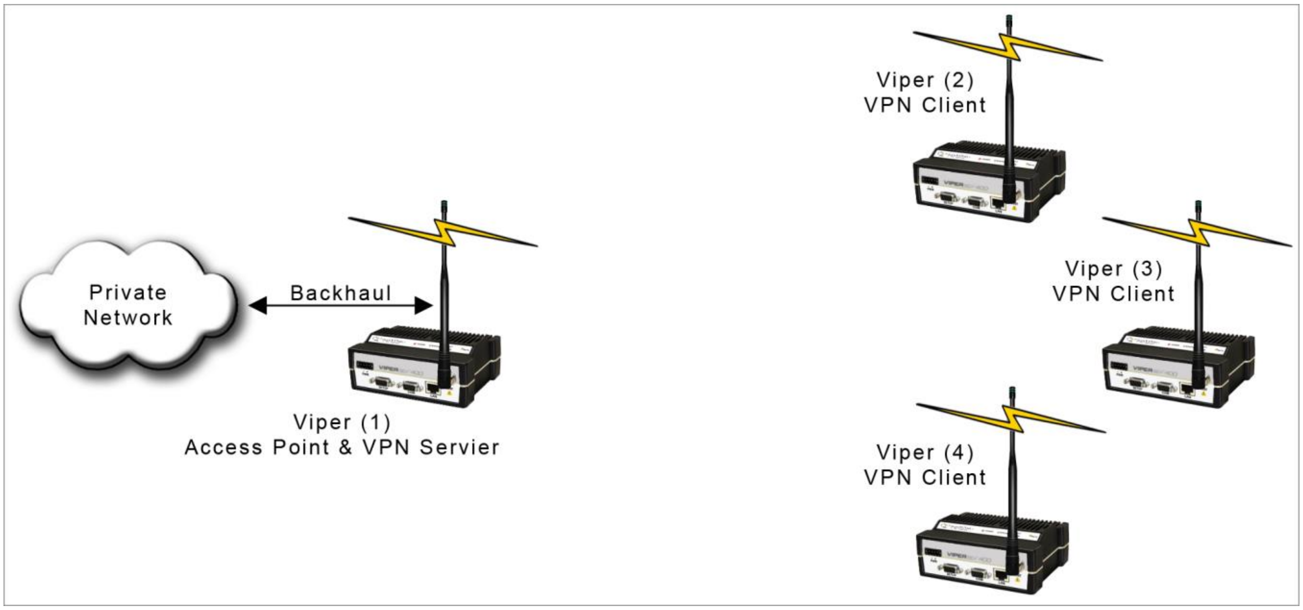
VPN (Virtual Private Network) is the fourth (from left) tab of the Security page. To navigate to this tab, select Security from the main menu and click VPN. This tab allows you to set a password to access VPN settings, enable or disable VPN, and view Status and Statistics for VPN tunnels.

VPN Concepts

A VPN secures network traffic by transporting it within encrypted “tunnels” between two VPN devices. A VPN tunnel ensures data privacy over any type of network. Multiple physical networks can exist between two VPN devices. A VPN tunnel thus provides a virtual “single hop” network connection between two VPN devices.

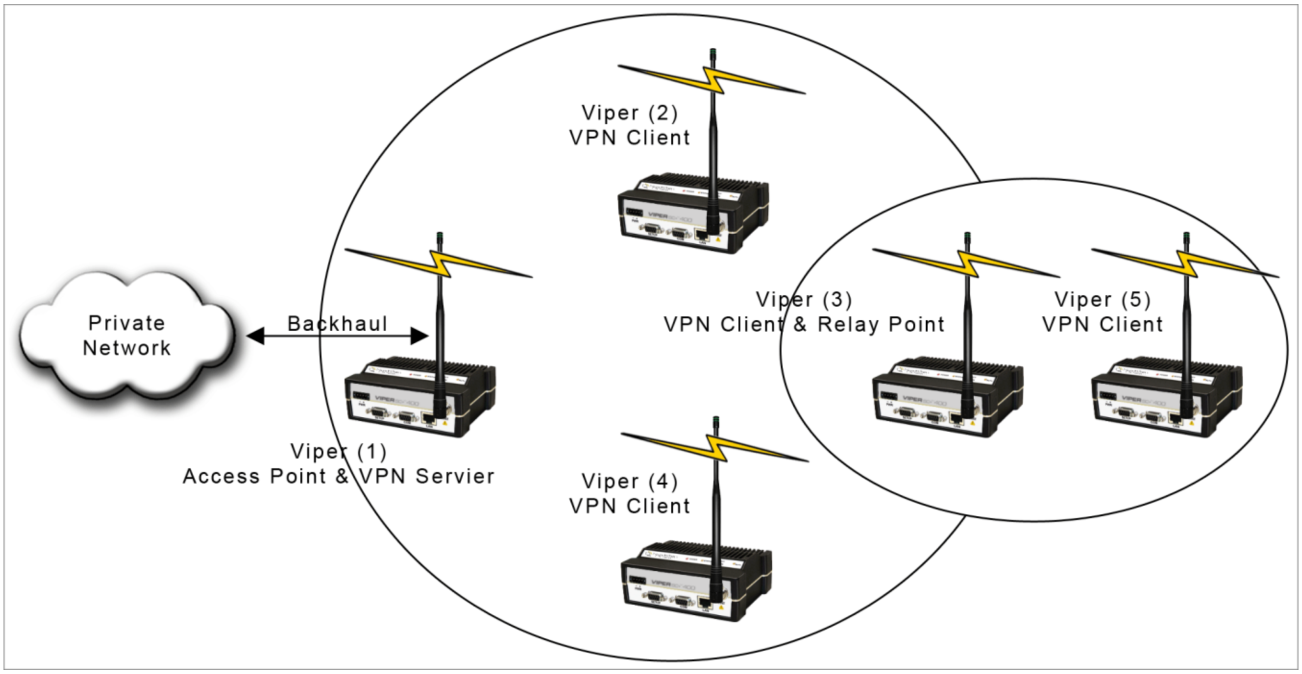
The following figure illustrates a VPN network with one Viper programmed as a VPN server and three remotes set as VPN clients. In this example, a secure connection is established between all Viper remotes and the Access Point. Only a Viper configured as an Access Point can operate as a VPN server.

Figure 63 – Viper VPN Network



This example can be further extended to include a relay point, which allows one unit to relay data from one RF coverage area to another RF coverage area, as shown in the following figure.

Figure 64 – Viper VPN Network with Relay Point



A VPN tunnel is created by a client to a specific server. A server can have tunnels to many clients.
A special shared tunnel is also provided to support a few special traffic types:

- Point-to-multipoint broadcast and multicast packets.
- Telnet, Web, SNMP, and RADIUS packets.
- Device specific IP-service packets (GPS, RSSI, diagnostics, etc.).

The shared tunnel is always available on a device, provided that its VPN service is enabled.

Tunnel Maintenance: Key exchange: Random cipher keys are used to encrypt VPN tunnel traffic. These keys are unique to each tunnel and are generated during VPN client/server key exchange. Tunnel keys are periodically updated to maximize security.

Server Status Advertisement: By default, traffic normally sent via VPN tunnel is blocked if one client/server tunnel endpoint is non-operational. A server therefore advertises its status to ensure that all its tunnels have a very high availability. These are sent whenever the server is enabled or disabled through a reset, device hot-swap, or manual intervention. VPN clients can thus quickly re-establish their tunnels as needed.

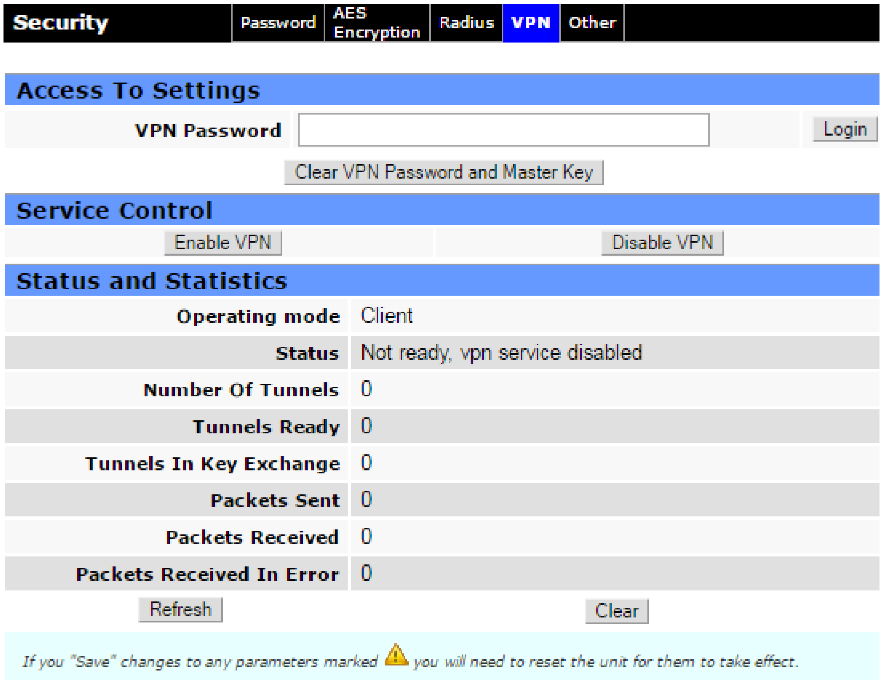
Configuration: Most VPN server configuration settings are sent to each client during key exchange. AVPN server does not send the following settings to VPN clients:

- VPN login password and Master Key.
- Device-specific General settings and IP-filter settings.

Master Key: The VPN Master Key is a configuration item essential to the security of VPN operations. A VPN server's Master Key must also be set on each of its clients. Access to the Master Key (along with other VPN settings) is therefore protected by the VPN login mechanism.

A VPN deployment consisting of multiple isolated VPN servers can employ a different Master Key per server for additional security, since redeploying VPN clients to other servers would require their Master Key to be changed to match the new server's key.

Figure 65 – Security – VPN



Operating mode	Client
Status	Not ready, vpn service disabled
Number Of Tunnels	0
Tunnels Ready	0
Tunnels In Key Exchange	0
Packets Sent	0
Packets Received	0
Packets Received In Error	0

If you "Save" changes to any parameters marked ⚠ you will need to reset the unit for them to take effect.

Access To Settings

VPN Password: Enter the VPN password (leave the field empty if not set) and click Login to be able to access and change VPN-specific configuration settings.

Clear VPN Password Master Key: Permits access to VPN configuration settings when the VPN password is unknown.

Service Control

Enable VPN: Enables the VPN service on the Viper.
Note: For packets to securely pass over the network, the VPN service must be enabled on **both** tunnel endpoints.

Disable VPN: Disables the VPN service on the Viper.
Note: For packets to pass over the network insecurely, the VPN service must be disabled on **both** tunnel endpoints.

Enable VPN Clients (available on VPN servers only): Sends a VPN Enable command to all clients regardless of the VPN server's state.

Notes:

The command is broadcast a few times based on the Network Latency VPN setting. A server can send only one command at a time.

When VPN clients with a user accessing the VPN configuration cannot process commands from the server.

Disable VPN Clients (available on VPN servers only): Sends a VPN Disable command to all clients regardless of the VPN server's state.

Notes:

The command is broadcast a few times based on the Network Latency VPN setting. A server can send only one command at a time.

When VPN clients with a user accessing the VPN configuration cannot process commands from the server.

Status and Statistics

Note: Results of clicking **Enable VPN** or **Disable VPN** are not immediately reflected in the Status and Statistics. Click **Refresh** to update values displayed in this section.

Operating Mode: Displays whether the Viper is operating as a VPN Server or Client. (The Viper must be configured as an Access Point RF device to be a VPN Server; the Viper must be configured as a non-Access Point RF device to be a VPN Client.)

Status: Displays the status of the VPN tunnel service. When the VPN is operational, this will display OK/Ready; if VPN is not operational, this will display Not Ready and the reason it is not operational.

Number of Tunnels: Number of active VPN tunnels originating or terminating in the device. This number is subdivided into tunnels that are ready and tunnels currently undergoing key exchange. One additional shared tunnel is used for special types of traffic. (See VPN for an explanation of this shared tunnel and types of traffic this tunnel is provided for.)

Tunnels Ready: Lists the number of active tunnels that are ready.

Tunnels in Key Exchange: Lists the number of active tunnels in Key Exchange.

Packets Sent: Number of packets sent by the Viper through all VPN tunnels.

Packets Received: Number of packets received by the device from all VPN tunnels.

Packets Received in Error: Number of packets received in error by the Viper from all VPN tunnels.
Possible causes of packets received in error are:

- Reception of non-VPN packets when Block non-VPN Packets is enabled.
- Decryption errors due to key exchange or packet corruption (infrequent).

Password, Key Strength, and Master Key

Note: These settings are not affected by **Set to Defaults**.

VPN Password: This field is used to change the password used to gain access to VPN configuration settings. The password must contain at least eight (8) and no more than fifteen (15) characters using a combination of three out of the following four types of characters.

- Uppercase letters
- Lowercase letters
- Numbers
- Special characters

Notes: The list of supported special characters is displayed after entering an invalid password.
The VPN service cannot be enabled if this field is not set.

Key Strength:

The number of bits used by all VPN keys. The value can be one of the following.

- 128 bits – 16 text characters or 32 hexadecimal digits
- 192 bits – 24 text characters or 48 hexadecimal digits
- 256 bits – 32 text characters or 64 hexadecimal digits

Hexadecimal digits include 0 through 9, and a through f, or A through F.

Master Key:

A key that must be the same for a VPN server and all its clients. This key can be entered as a text string (weaker) or as a binary number (stronger).

- A text string may contain any character. For example, "a 16-byte string" (quotes are optional).
- A numeric value should start with 0x (zero-x) to permit hexadecimal digits. For example, 0x00112233445566778899aabbccddeeff is a 16-byte (128 bit) value.

A numeric value provides a stronger key since each string character contains only 7 bits, but two hexadecimal digits contain 8 bits.

Notes: The length of the key must match the Key Strength setting in bytes (strength in bytes divided by 8).
The VPN service cannot be enabled if this field is not set.

Clear VPN Password and Master Key: Clears the VPN password used to gain access to VPN configuration settings. Also clears the VPN password used t gain access to VPN configuration settings. Also clears the VPN Master Key.

Note: To reset just the Master Key, set the Key Strength to a different value.

VPN Configuration – General Settings

Set Server/Client Defaults; Sets most VPN settings to appropriate values for either server or client mode of operation. Server mode should be selected on devices connected by Ethernet to the backhaul network. Client mode should be selected on all other devices.

Notes: The VPN Password, Key Strength, and Master Key settings are not affected.
It is recommended to select one of these buttons as the first step in configuring the VPN service.

Automatic Start:

The VPN service can be set to start automatically at startup (or not to).

- Enabled — Start the VPN service at startup.
- Disabled — Do not start the VPN service automatically at startup.

The default setting is Enabled.

Operating Mode:

The Viper may be configured to operate as a VPN server or VPN client. (See specific disclaimers below.)

- **Server:** Sets the Viper to operate as a VPN Server. (Viper must be configured as an RF Access Point.)
- **Client:** Sets the Viper to operate as a VPN Client. (Must be configured as a non-Access Point on RF.)

The default setting is Client.

Notes: An Access Point connects to the backhaul via its Ethernet port.
After changing this setting, click **Apply** to apply the new setting and refresh the page.

VPN Configuration – Server Settings

Block non-VPN Traffic (Available on VPN servers only):

The Viper can be set to block or allow non-VPN traffic.

- Enabled — The VPN service blocks all packets from the RF link that were not sent via a VPN tunnel.
- Disabled — Non-matching traffic is not blocked.

The default setting is Enabled.

Notes: This setting is especially useful for blocking devices that are not configured for VPN operation from sending packets to the backhaul network.
A VPN server automatically sets this parameter on its clients during key exchange.

Status Frequency (Available on VPN servers only):

The number of 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 or disabled) and load (0-100% tunnel capacity in use).
A non-zero value permits VPN clients to "discover" servers (they do not need to be preconfigured with server IP addresses). Clients that are aware of more than one server can intelligently select one based on its advertised load.

Notes: This value does not affect the server statuses that are sent whenever a VPN server is enabled or disabled.
Server status packets are broadcast over radio links to minimize traffic. Devices acting as radio-relays must therefore explicitly enable station relay mode to forward server statuses.
A VPN server automatically sets this parameter on its clients during key exchange.
Default = 10 seconds
Minimum = 5 seconds (0 = disabled)
Maximum = 60 seconds (1 minute)

Idle Timeout (Available on VPN servers only):

The number of minutes with no traffic received from a VPN tunnel before attempting an Idle Probe and/or Key Exchange. When Idle Probes are disabled, the Idle Timeout will simply trigger Key Exchange.

Notes: This value affects the time it takes for VPN clients to re-establish their tunnels after a VPN server is restarted.
A VPN server automatically sets this parameter on its clients during key exchange.
Default = 15 minutes
Minimum = 0 minutes (disabled)
Maximum = 60 minutes (1 hour)

Idle Probes (Available on VPN servers only):

On Idle Timeout, this sets the number of Idle Probes to send without receiving a reply. An Idle Probe attempt consists of a 100-byte UDP packet that is sent and received via a VPN tunnel. A successful send and receive prevents premature key exchange for that VPN tunnel.

Notes: The Idle Timeout setting must be non-zero before Idle Probes are sent.
The retry frequency of each probe attempt is determined by the Network Latency setting.
For a Network Latency of 10, the probe frequency is 10 seconds.
Default = 3 seconds
Minimum = 0 seconds (disabled)
Maximum = 10 seconds

Key Timeout (Available on VPN servers only):

Maximum duration of VPN tunnel cipher keys. Key exchange consists of approximately twelve (12) 80–100-byte TCP packets (1 kilobyte), which may take several seconds — or longer when the network is busy.

Notes: The retry frequency of each key exchange attempt is determined by the Network Latency setting.
For a Network Latency of 10, the exchange attempt frequency is 0-70 seconds.
A VPN server automatically sets this parameter on its clients during key exchange.
Default = 6 hours
Minimum = 1 hour
Maximum = 24 hours

Network Latency (Available on VPN servers only):
This parameter is a factor (multiplier) for tuning VPN maintenance operations. It affects the frequency of server status packets, idle probes, and key exchange retries (see explanations of these settings, earlier, for details). This number should be set higher if key exchanges are occurring more frequently than the Key Timeout setting (see the VPN Status and Statistics section.

Notes: Only change this value by small amounts (1-5 seconds).
Default = 10 seconds
Minimum = 2 seconds
Maximum = 30 seconds

VPN Configuration – Client Settings

Server IP Addresses (Available on VPN clients only): The IP address(es) of one or more VPN servers.

Note: When the VPN Server Status Frequency setting is zero (default), each of its clients must be set with that server's RF IP address. Otherwise, this is optional (clients will "discover" the server's IP address.

VPN Configuration – Packet Filter Settings

These filters provide criteria used to select which packets are sent via VPN tunnels. Packets passing inside VPN tunnels are protected with strong encryption. Traffic not matching these filters is discarded when the Block non-VPN Traffic is enabled (default). Otherwise, it is forwarded as-is (unencrypted.

Note: Appropriate filters are automatically set when selecting the Set Client/Server Defaults buttons.

Source/Destination IP Address and **Netmask:** The source and destination IP addresses are used to select which packet are sent via VPN tunnels.

Source IP filter: Controls which traffic from the VPN device or its immediate Ethernet LAN enters the VPN.

Destination IP Filter: Controls which traffic to the given IP address or range enters the VPN.

Examples (with Netmask 255.255.255.255):

- Source IP address 172.30.51.3 allows packets only from the specified LAN IP address into the VPN.
- Source IP address 0.0.0.0 allows packets from any LAN IP address into the VPN. (This is useful when LAN devices sending via the VPN are behind routers, usually the case for a VPN server connected to a backhaul network.)

Note: The Netmask for each IP address controls whether it is a single address or a subnet range.

Examples:
255.255.255.255 restricts the IP address range to the specified value.
255.255.255.0 allows the last part of the IP address to range from 1 to 254 (0 and 255 are reserved)

Source defaults
0.0.0.0 (server, allow any source)
[LAN subnet] (client, allow any local source)

Destination default
0.0.0.0 (allow any destination)

Source/Destination Ports: The source and destination TCP/UDP port number ranges are used to select which packets are sent via the VPN based on application type.

Source Port filter: Controls which traffic from the VPN device or its immediate Ethernet LAN enters the VPN.

Destination Port Filter: Controls which traffic to the given TCP/UDP port or range enters the VPN.

Examples:
Destination ports 0 to 0 allows packets to any port.
Destination ports 5555 to 0 allows packets to only port 5555.
Destination ports 5555 to 6000 allows packets to all ports between 5555 and 6000.

Default = 0 (allow any port)
Minimum = 1
Maximum = 65535

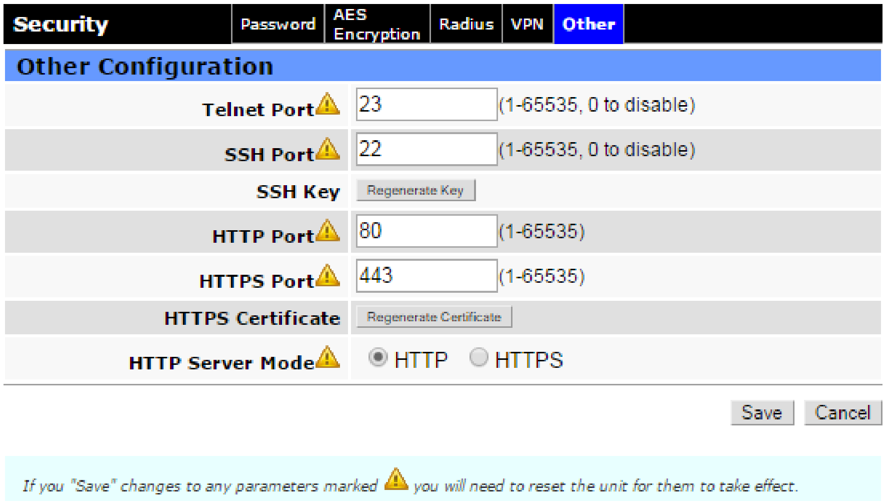
Refresh: Click Refresh to update the status and statistics to show the most current information available.

Clear: Clicking Clear (or cycling power to the Viper) will reset all statistics to zero.

4.5.5. OTHER

This tab allows you to select the preferred method of access to the web pages and the command shell.

Figure 66 - Security - Other



Other Configuration

Telnet Port ⚠	23 (1-65535, 0 to disable)
SSH Port ⚠	22 (1-65535, 0 to disable)
SSH Key	Regenerate Key
HTTP Port ⚠	80 (1-65535)
HTTPS Port ⚠	443 (1-65535)
HTTPS Certificate	Regenerate Certificate
HTTP Server Mode ⚠	● HTTP ○ HTTPS

If you "Save" changes to any parameters marked ⚠ you will need to reset the unit for them to take effect.

Other Configuration

Telnet Port: This parameter lets the user select the TCP port number used by the telnet server on the Viper. Setting it to 0 will disable the server. Make sure to use a port number not used by other applications. Telnet gives you access to the command shell of the Viper over an unencrypted TCP session.

SSH Port: This parameter lets the user select the TCP port number used by the SSH server on the Viper. Setting it to 0 will disable the server. Make sure to use a port number not used by other applications. SSH gives you access to the command shell of the Viper over an encrypted TCP session.

SSH Key: Press to delete the SSH RSA key file currently used by the SSH server. When rebooting, a new RSA key file will be generated.

HTTP Port: This parameters lets the user select the TCP port number used by the HTTP server on the Viper.

HTTPS Port: This parameters lets the user select the TCP port number used by the HTTPS server on the Viper. HTTPS is a secure version of HTTP (the TCP sessions are encrypted to prevent eavesdropping).

HTTPS Certificate: Press to delete the HTTPS certificate currently used by the server. When rebooting, a new certificate will be generated.

HTTP Server Mode: Select the HTTP mode of operation (non-secure: HTTP, secure: HTTPS).

Note: If you change any of the port numbers or select a different HTTP server mode, a reset of the Viper is required before the setting will take effect, as indicated by the yellow alert symbol (⚠).

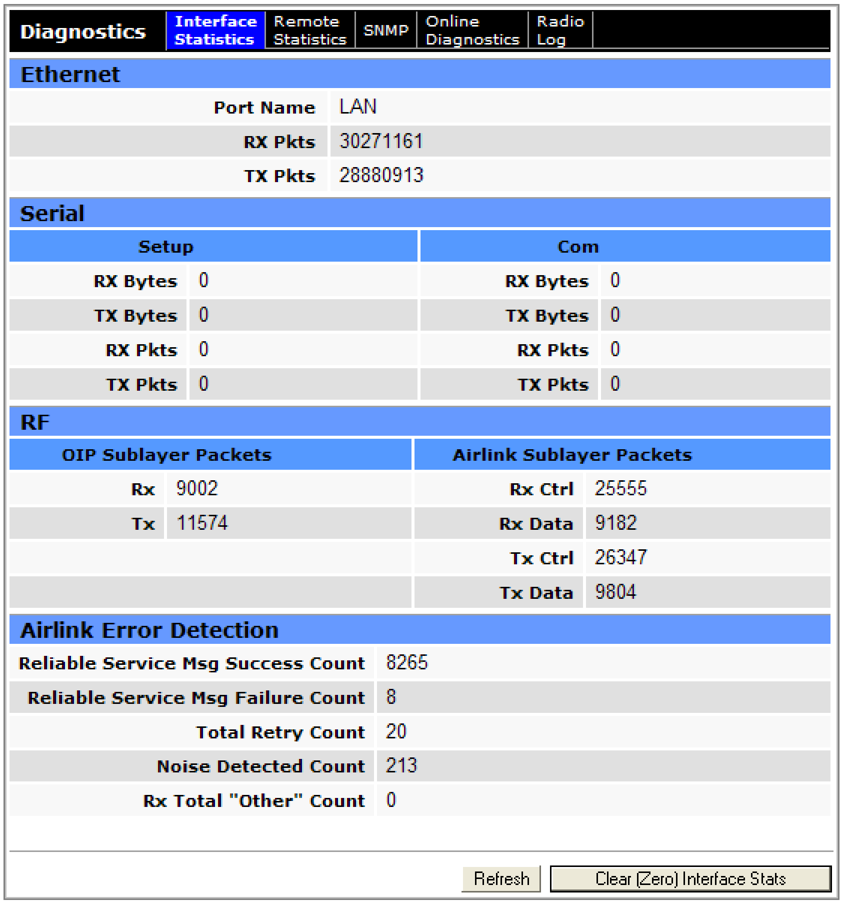
4.6. DIAGNOSTICS

The Diagnostics tab contains five tabs: Interface Statistics, Remote Statistics, SNMP, Online Diagnostics, and Radio Log.

4.6.1. INTERFACE STATISTICS

Interface Statistics is the first (left-most) tab in the Diagnostics page. To navigate to this tab, select Diagnostics from the main menus. This tab provides information about packets sent and received on each of the interfaces (Ethernet, the two serial ports, and RF), and Airlink Error Detection statistics.

Figure 67 – Diagnostics – Interface Statistics



Ethernet

Port Name	LAN
RX Pkts	30271161
TX Pkts	28880913

Serial

Setup		Com	
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

OIP Sublayer Packets		Airlink Sublayer Packets	
Rx	9002	Rx Ctrl	25555
Tx	11574	Rx Data	9182
		Tx Ctrl	26347
		Tx Data	9804

Airlink Error Detection

Reliable Service Msg Success Count	8265
Reliable Service Msg Failure Count	8
Total Retry Count	20
Noise Detected Count	213
Rx Total "Other" Count	0

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

Note: Definitions that follow in this section for use in this tab use the following conventions.

- Rx (or Input) = data received from a lower network layer.
- Tx (or Output) = data transmitted to a lower network layer.

Cycling power to the Viper or clicking Clear (Zero) Interface Stats will reset all statistics to zero.

Ethernet

Port Name: LAN Indicates that statistics in this section are for the port named LAN, the Ethernet port.

Rx Pkts: The total number of incoming packets received by the Ethernet interface (LAN).

Tx Pkts: The total number of outgoing packets transmitted by the Ethernet interface (LAN).

Serial

Bytes and packets statistics for the Serial ports are presented in two columns, left and right, for each of the ports. Statistics listed in the *left* column are for the **Setup** serial port. Statistics listed in the *right* column are for the **COM** port.

Rx Bytes:Total number of incoming bytes received by the Setup or COM port.

Tx Bytes:Total number of outgoing bytes transmitted by the Setup or COM port.

Rx Pkts:Total number of incoming packets received by the Setup or COM port.

Tx Pkts:Total number of outgoing packets transmitted by the Setup or COM port.

RF

Packet statistics in the RF section are presented in two columns, as explained below.

OIP Sublayer Packets: Statistics listed in the left column are for Optimized IP (OIP) sublayer packets.

Rx: Total number of incoming packets received by the RF OIP interface.

Tx: Total number of outgoing packets transmitted by the RF OIP interface.

Airlink Sublayer Packets: Statistics listed in the right column are for physical radio-frequency connection (Airlink) sublayer packets.

Rx Ctrl: Total number of control packets received over the air. These packets may be RTS/CTS messages or RF Acknowledgements.

Rx Data: Total number of data packets transmitted over the air.

Tx Ctrl: Total number of control packets transmitted over the air. These packets may be RTS/CTS messages or RF Acknowledgements.

Tx Data: Total number of output data packets transmitted over the air.

Airlink Error Detection

Airlink error detection statistics provide information about the quality of the RF link.

Reliable Service Message Success Count: Total number of service messages that succeeded. RF Acknowledgements must be enabled to generate a Reliable Service Message.

Reliable Service Msg Failure Count: Total number of service messages that failed.

Total Retry Count: Total number of retries for service messages.

Noise Detected Count: Number of noise (non-Viper carrier) detected above the carrier sense level. If the Noise Detected Count is high, it may be an indication that the Carrier Sense Threshold should be raised.

Rx Total "Other" Count: Total number of messages the Viper overheard that were intended for another station. These messages are discarded.

Refresh: Click Refresh to update the statistics to show the most current information available.

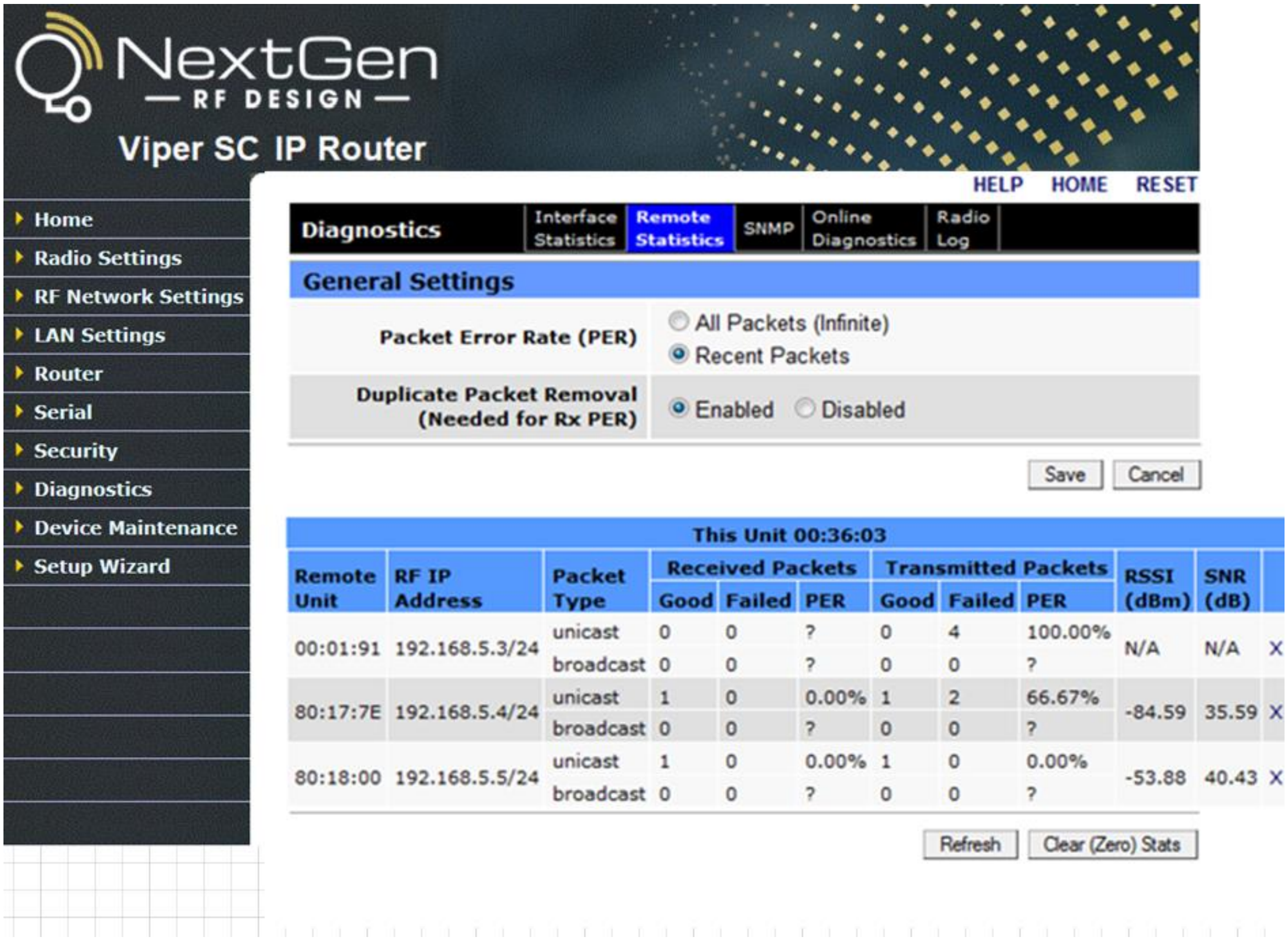
Clear (Zero) Interface Stats: Clicking Clear (Zero) Interface Stats (or cycling power to the Viper) will reset all statistics to zero.

4.6.2. REMOTE STATISTICS

Remote Statistics is the second (from left) tab of the Diagnostics page. To navigate to this tab, select Diagnostics from the main menu and click Remote Statistics. This tab provides information in table form about communication with remote units, including statistics for packets transmitted and received to and from them, received signal strength, and signal-to-noise ratio.

Note: A statistical entry can be deleted by clicking the "X" to the right of the entry.

Figure 68 – Diagnostics – Remote Statistics



General Settings

Packet Error Rate (PER): ○ All Packets (Infinite) ● Recent Packets

Duplicate Packet Removal (Needed for Rx PER): ● Enabled ○ Disabled

This Unit 00:36:03

Remote Unit	RF IP Address	Packet Type	Received Packets Good	Received Packets Failed	Received Packets PER	Transmitted Packets Good	Transmitted Packets Failed	Transmitted Packets PER	RSSI (dBm)	SNR (dB)	
00:01:91	192.168.5.3/24	unicast	0	0	?	0	4	100.00%	N/A	N/A	X
		broadcast	0	0	?	0	0	?			
80:17:7E	192.168.5.4/24	unicast	1	0	0.00%	1	2	66.67%	-84.59	35.59	X
		broadcast	0	0	?	0	0	?			
80:18:00	192.168.5.5/24	unicast	1	0	0.00%	1	0	0.00%	-53.88	40.43	X
		broadcast	0	0	?	0	0	?			

General Settings

Packet Error Rate (PER) — Select how to calculate the PER.

- **All Packets (Infinite)** —The packet error rate is calculated since power cycle or since the last "Clear Stats" event. PER=((total bad packets)/(total bad packets + total good packets))*100.

- **Recent Packets** — The packet error rate is based on the last several hundred packets only. This mode represents the current link quality more accurately than the Infinite mode which calculates PER based on all packets transmitted or received since the last power cycle or "Clear Stats" event."

Duplicate Packet Removal (Needed for Rx PER) — This option must be enabled to calculate the PER. It controls if the packets sent over the air will contain or not the packet sequence number (used by duplicate packet detection and PER calculation). By default, it is disabled to preserve compatibility with firmware versions prior to V3.3_R201109191700. If this option is enabled facing the older firmware versions (prior to V3.3_R201109191700), the RF communication will fail.

Remote Statistics Table

This Unit: Centered at the top of the table provides the RF MAC address of the Viper for reference.
Table columns are as follows.

Remote Unit: The RF MAC address of the neighboring remote unit. This table is updated every time the Viper sends (or receives) data to (or from) the remote unit. If the RF MAC address is prefixed with an asterisk (*, or star), it means this unit was learned of through a Relay Point (RP) unit.

RF IP Address: The RF IP Address of the remote unit.

Received Packets: Number of IP packets sent by the remote unit to this unit and received. A packet is bad, or failed, if at least one of the CRC, the length, or the system identifier is incorrect, or it is simply missing (not received at all by this unit). The Viper can detect missing packets because of the sequence number in each packet.

PER: Packet Error Rate is expressed as a percentage that indicates the percentage of packets that have failed to be successfully transmitted or received over the RF link.

> When the Packet Error Rate is indicated by a question mark (?), it is because the unit cannot determine the value. This is because the sequence number is not included in the packets received over the air or because no IP packet has been received yet. To make sure a remote unit includes a sequence number in its packets, the “OIP duplicate packet removal” feature must be enabled on it.

Transmitted Packets: Total 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 notification was not received from the remote unit of the arrival of the packet.

- The transmit Packet Error Rate (PER) is calculated using the same formula as explained earlier.

- When the Packet Error Rate is indicated by a question mark (?), it is because the unit cannot determine the value. This is because the “RF ACK” feature is not enabled on this unit or no IP packet has been transmitted yet. The “RF ACK” feature lets the unit know that the packet has made it to the remote unit.

RSSI: The most-recent Received Signal Strength Indicator (RSSI) from the remote unit. Each time a new packet is received from the remote unit, the RSSI in this table is calculated and updated.

SNR: The most-recent Signal to Noise Ratio (SNR) from the remote unit. Each time a new packet is received from the remote unit, the SNR in this table is calculated and updated.

Refresh: Click Refresh to update the statistics to show the most current information available.

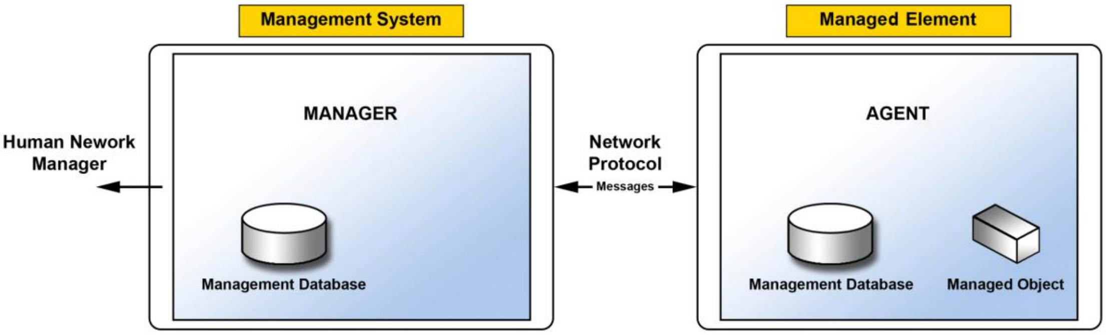
Clear (Zero) Interface Stats: Clicking Clear (Zero) Interface Stats (or cycling power to the Viper) will reset all statistics to zero.

4.6.3. SNMP

SNMP (Simple Network Management Protocol): The third (middle) tab of the Diagnostics page. To enable this feature, select Diagnostics from the main menu and click SNMP to navigate to this tab.

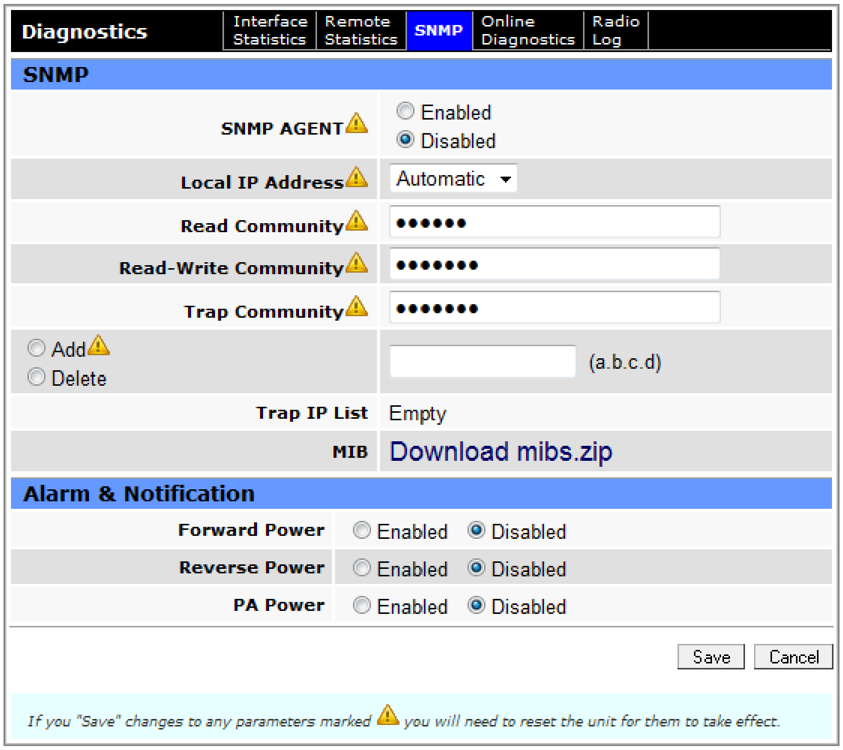
SNMP is used by network management systems to manage and monitor network-attached devices, and provides a means to monitor, collect, and analyze diagnostic information. Viper is compatible with SNMPv2c. SNMP allows you to access IP statistics and diagnostics from the Viper using third-party MIB (Management Information Base) browser software. The Viper can be programmed to respond to SNMP queries to its local IP Address, RF, or Ethernet IP address (Automatic), or respond to its Ethernet IP address (Ethernet), or respond to its RF IP Address (RF). Use the options and settings in this tab to enable or disable the SNMP agent, configure SNMP settings, and enable or disable alarms for power conditions.

Figure 69 – SNMP Model Manager and Agent



Traps (or alarms) will be automatically generated whenever the forward or reverse power goes out of specification. These traps can be sent to a user-specified IP address or addresses.

Figure 70 – Diagnostics – SNMP



SNMP

SNMP AGENT ⚠ ○ Enabled ● Disabled

Local IP Address ⚠ Automatic

Read Community ⚠ ••••••

Read-Write Community ⚠ •••••••

Trap Community ⚠ •••••••

○ Add ⚠ ○ Delete (a.b.c.d)

Trap IP List Empty

MIB Download mibs.zip

Alarm & Notification

Forward Power ○ Enabled ● Disabled

Reverse Power ○ Enabled ● Disabled

PA Power ○ Enabled ● Disabled

If you "Save" changes to any parameters marked ⚠ you will need to reset the unit for them to take effect.

SNMP

SNMP Agent : Enable or disable the internal SNMP agent by selecting the appropriate option. The default setting is Disabled; select Enabled to activate SNMP.

Local IP Address: The Viper can be programmed to respond to SNMP queries to its local IP Address, RF, or Ethernet IP address (Automatic), or respond to its Ethernet IP address (Ethernet), or respond to its RF IP Address (RF). Select either Automatic, Ethernet, or RF. The default setting is Automatic.

Read Community: The password string entered in the Read Community field grants read-only access to external MIB browsers.

Read-Write Community: The password string entered in the Read-Write Community field grants read-write access to external MIB browsers.

Trap Community: The password string entered in the Trap Community field is included in SNMP trap packets.

Trap IP List: This list shows the user-programmed IP addresses where the Viper will send SNMP traps. To add an IP Address to the list, select the Add radio button, enter the IP address into the address field (a.b.c.d), and then click Save (near the bottom of the tab). When the page is refreshed, the IP address you entered will appear in the Trap IP List.

To delete an IP address from the list, select the Delete radio button, enter the IP address to be deleted in the address field (a.b.c.d), and click Save (near the bottom of the tab).

MIB: Three Viper MIB files are bundled with each Viper's firmware. Click the "Download mibs.zip" link to download a .zip file that contains the three MIB files. These files contain links to the SNMP information available in the Viper. The MIB files must be loaded into a third-party MIB browser.

Caution: Certain MIB browsers (standalone or integrated in an SNMP manager) may require you to modify the MIB file's extension (for example, from .MIB to .TXT).

Each Viper firmware package is bundled with three MIB files (found inside the mibs.zip file): (1) nextgenrf-regs.MIB contains a top-level set of managed object definitions aimed at managing products with the NextGenRF brand, (2) 1213.MIB contains a set of managed object definitions aimed at managing TCP/IP-based network devices, and (3) Viper_scx.mib contains a set of managed object definitions aimed at managing Viper radio modems.

For more information about MIB files included with the Viper firmware, see APPENDIX H– MIB File.

Alarm & Notification

Below are the traps that will be sent on an alarm or notification condition to the server that has been added to the Trap IP List. Each of these may be enabled or disabled.

Forward Power: Forward power exceeds minimum or maximum levels. The default setting is Disabled.

Reverse Power: Power exceeds maximum reverse power. The default setting is Disabled.

PA Power: PA power has folded back. The default setting is Disabled.

Save: Click Save to save any changes you have made to settings in this tab. See Note below.

Cancel: Click Cancel to cancel any changes you may have made to any of the settings in this tab.

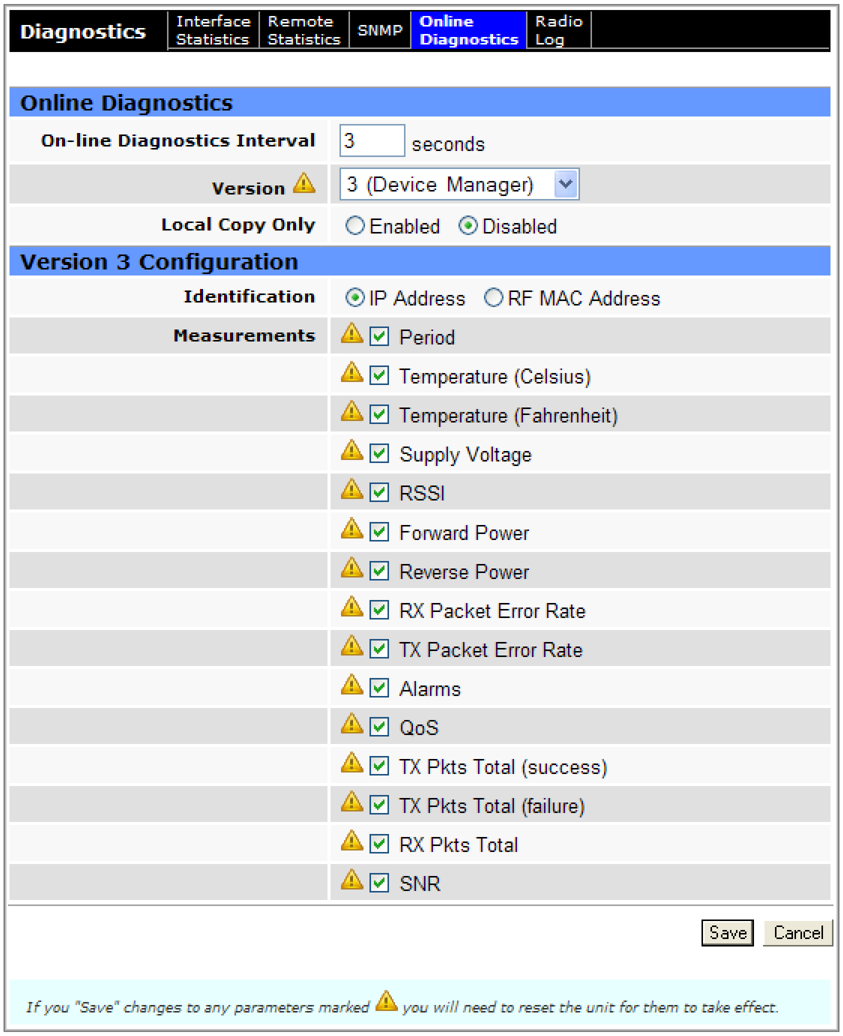
Note: If you enable or disable the SNMP agent or change the Local IP Address, Read Community, Read-Write Community, or Trap Community password string, or add or delete IP addresses in the Trap IP List in this tab, as indicated by the yellow alert symbol (⚠), a reset of the Viper is required before any of these settings will take effect.

4.6.4. ONLINE DIAGNOSTICS

Online Diagnostics is the fourth (from left) tab of the Diagnostics page. To navigate to this tab, select Diagnostics from the main menu and click Online Diagnostics. Settings in this tab allow you to set the interval, configure settings, and save a report containing diagnostic information.

The 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 backhauled. Backhaul adds to network traffic flow and must be considered when designing a network. If a return flow is necessary, it needs to be reduced substantially to have a minimal effect on the network. The Viper can support up to four (4) diagnostic socket connections at once. This may be used, for example, to carry out monitoring at a main office and at up to three separate field locations. It is also possible for one of the four connections to use a serial port instead of enabling it in the Viper Web browser interface.

Figure 71 – Diagnostics – Online Diagnostics



Online Diagnostics

On-line Diagnostics Interval	3 seconds
Version ⚠	3 (Device Manager)
Local Copy Only	○ Enabled ● Disabled

Version 3 Configuration

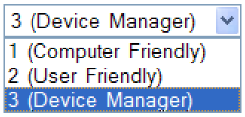
Identification	● IP Address ○ RF MAC Address
Measurements	⚠ ☑ Period
	⚠ ☑ Temperature (Celsius)
	⚠ ☑ Temperature (Fahrenheit)
	⚠ ☑ Supply Voltage
	⚠ ☑ RSSI
	⚠ ☑ Forward Power
	⚠ ☑ Reverse Power
	⚠ ☑ RX Packet Error Rate
	⚠ ☑ TX Packet Error Rate
	⚠ ☑ Alarms
	⚠ ☑ QoS
	⚠ ☑ TX Pkts Total (success)
	⚠ ☑ TX Pkts Total (failure)
	⚠ ☑ RX Pkts Total
	⚠ ☑ SNR

If you "Save" changes to any parameters marked ⚠ you will need to reset the unit for them to take effect.

Online Diagnostics

On-line Diagnostic Interval: The online diagnostic interval is the time interval (in seconds) at which the Viper will broadcast the diagnostic string. Setting the online diagnostic interval to zero (0) disables online diagnostic reporting. The default setting is three (3) seconds.

Version



3 (Device Manager)
1 (Computer Friendly)
2 (User Friendly)
3 (Device Manager)

You can change the version of online diagnostic messages, which affects the format. Three versions are available.

- **Computer Friendly**: This is the “old style.” It is computer-readable, but can be difficult to readily understand
- **User Friendly**: This is the same as Computer Friendly (1), with the exception that all values are “human readable” (with the trade-off that this format is slightly more verbose). An example and explanation are provided in the following section.
- **Local Copy Only:** When this is enabled, the Viper will not piggyback its diagnostic messages over user traffic. The Viper will still output its diagnostic messages over to TCP clients connected to the online diagnostic TCP port.

Version-Specific Configuration

Information in the lower section of the tab will change depending on the Version of online diagnostic messages you have selected above. This section provides options for whether you want the Viper to use the IP Address or RF MAC address for identification

Identification: Select whether to use the IP Address or RF MAC Address of the Viper for identification in online diagnostics reporting. The default setting is to use the IP Address.

Measurements: These are presented as a checklist. Check the items to be included in the online diagnostic reporting; uncheck the items to omit. The default setting is to include all items.

Save: Click Save to save any changes you have made to settings in this tab. See Note below.

Cancel: Click Cancel to cancel any changes you may have made to any of the settings in this tab.

Note: If you change the Version or add or remove any items in the measurements list in the lower section in this tab, as indicated by the yellow alert symbol (⚠), a reset of the Viper is required before any of these settings will take effect.

4.6.4.1. Human-Readable Output Format

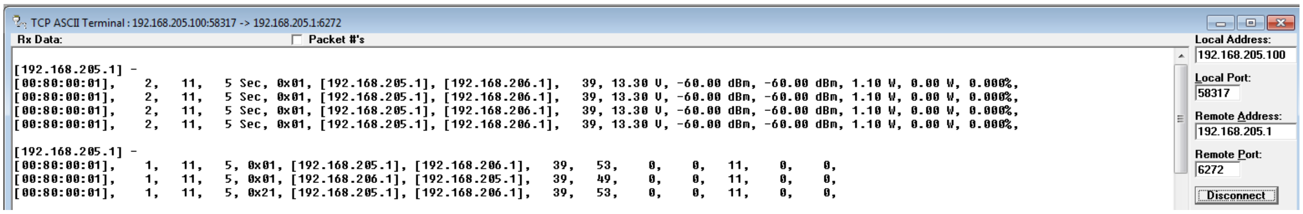
Note: **This section is optional.** For assistance or more specific information, contact support@nextgenrf.com.

With the Online Diagnostics Version set to 2 (User Friendly) and saved, from a Command Prompt window, type telnet nnn.nnn.nnn.nnn.6272 (where nnn.nnn.nnn.nnn represent the Viper's IP address in dot decimal format). The Viper's online diagnostic output will display on your screen. The online diagnostic output is human and machine-readable ASCII, comma-delimited format. Any reader program used (or written) must decode the Version field and check for the type — 1 for "Computer Friendly" or 2 for "User Friendly" — to determine the format.

Note: No overhead is generated in the Viper if no online diagnostic connection is made.

The output looks like the output shown in the following figure.

Figure 72 – Diagnostic Output Sample – Computer readable and Human Readable format



TCP ASCII Terminal : 192.168.205.100:58317 -> 192.168.205.1:6272

Rx Data: □ Packet #'s

```
[192.168.205.1] -
[00:80:00:01],    2,   11,   5 Sec, 0x01, [192.168.205.1], [192.168.206.1],   39, 13.30 V, -60.00 dBm, -60.00 dBm, 1.10 W, 0.00 W, 0.000%,
[00:80:00:01],    2,   11,   5 Sec, 0x01, [192.168.205.1], [192.168.206.1],   39, 13.30 V, -60.00 dBm, -60.00 dBm, 1.10 W, 0.00 W, 0.000%,
[00:80:00:01],    2,   11,   5 Sec, 0x01, [192.168.205.1], [192.168.206.1],   39, 13.30 V, -60.00 dBm, -60.00 dBm, 1.10 W, 0.00 W, 0.000%,
[00:80:00:01],    2,   11,   5 Sec, 0x01, [192.168.205.1], [192.168.206.1],   39, 13.30 V, -60.00 dBm, -60.00 dBm, 1.10 W, 0.00 W, 0.000%,

[192.168.205.1] -
[00:80:00:01],    1,   11,   5, 0x01, [192.168.205.1], [192.168.206.1],   39,   53,    0,    0,   11,    0,    0,
[00:80:00:01],    1,   11,   5, 0x01, [192.168.206.1], [192.168.205.1],   39,   49,    0,    0,   11,    0,    0,
[00:80:00:01],    1,   11,   5, 0x21, [192.168.205.1], [192.168.206.1],   39,   53,    0,    0,   11,    0,    0,
```

Local Address: 192.168.205.100

Local Port: 58317

Remote Address: 192.168.205.1

Remote Port: 6272

Table 16 Diagnostics Output Definitions for Computer-Readable Format

	Output Definitions
Host	MAC address of the station where diagnostic measurements are being collected. The host will collect diagnostic messages from itself and all remote units with IPSD enabled. IPSD can be enabled or disabled in the Advanced Setup options for the port settings.
Ver	Version of the online diagnostics. Different versions may have different parameters. This table describes Version 1.
#	Number of items that follow in the online diagnostic message.
Period	PERIOD (seconds). Specifies the time between generation of online diagnostic messages from the

	Output Definitions
	source station.
Flags	Online Diagnostics Flags. (NextGen RF specific.)
Source	Source Address. In Bridge mode, this address displays the MAC address of the source Viper. In Router mode, this address displays the IP address of the of the source Viper 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. In Router mode, this address displays the IP address of the destination Viper. This is the destination station from the point of view of RSSI measurements.
A	Temperature of the source Viper in Celsius or Fahrenheit. Temperature units can be configured on the source Viper in Home » Basic Settings.
B	Source supply voltage more than 8 volts, shown in tenths (0.1) of volts. Supply voltage = (ODM_reading / 10) + 8.V. A reading of 35, for example, means 11.5 V.
C	RSSI measured at the source Viper for the last message received from the destination Viper. This is also referred to as the Local RSSI. Use the following table to interpret the RSSI value.
D	RSSI measured at the destination Viper for the last message received from the source Viper. This is also referred to as the Remote RSSI. Use the following table to interpret the RSSI value.
E	Radio/antenna forward power measured in tenths (0.1) of watts at the source Viper. A value of 51, for example, means 5.1 W.
F	Radio/antenna reverse power measured in tenths (0.1) of watts at the source Viper. A value of 2, for example, means 0.2 W.
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 maximum value is limited at 255. A reading of 2, for example, means 0.002 % of packets were rejected.

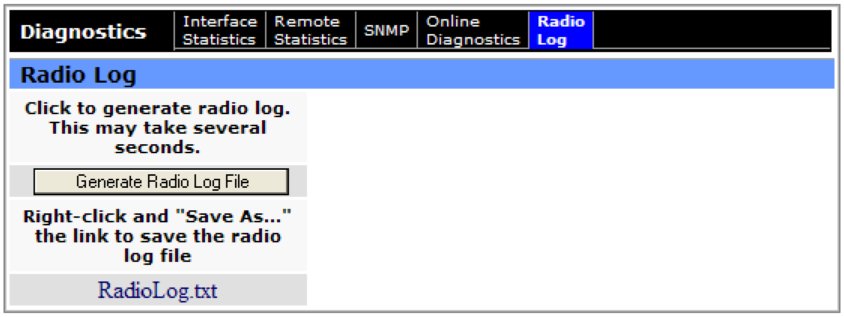
Table 17 Online Diagnostics RSSI Display

Value	RSSI	Notes
0	N/A	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.

4.6.5. RADIO LOG

Radio Log is the fifth (right-most) tab of the Diagnostics page. To navigate to this tab, select Diagnostics from the main menu and click Radio Log. This tab allows you to generate a radio log and save it as a text file.

Figure 73 – Diagnostics – Radio Log



Radio Log

Click to generate radio log. This may take several seconds.

Right-click and "Save As..." the link to save the radio log file

RadioLog.txt

Radio Log

When Generate Radio Log File is clicked, the unit will execute a special script which gathers diagnostic and log information. This information is written to the Radio Log text file named RadioLog.txt. This procedure takes several seconds. When the procedure is complete, you may then extract the Radio Log text file by right clicking the RadioLog.txt link provided near the bottom of the tab and selecting Save As… to navigate to a directory on your PC.

The RadioLog.txt file is an advanced diagnostic tool that should be sent to NextGen RF's technical support for further analysis.

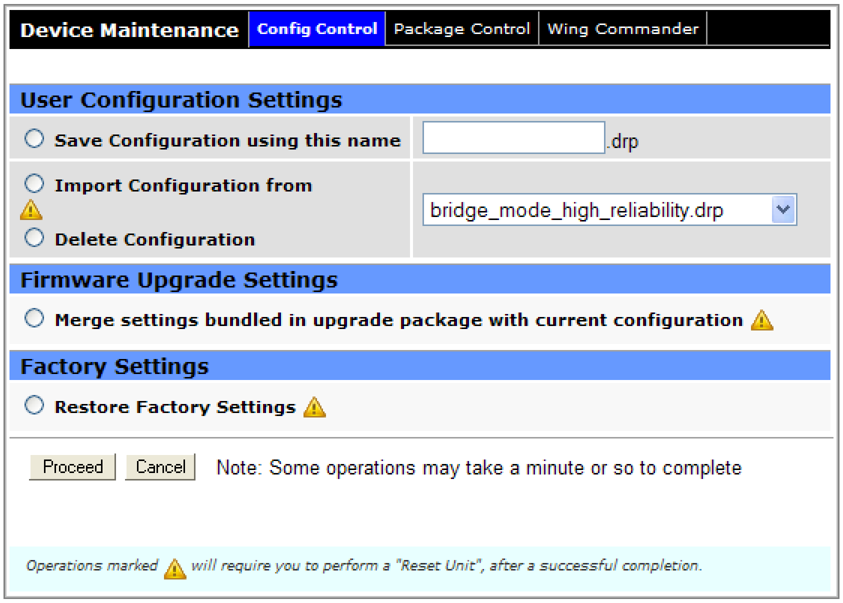
4.7. DEVICE MAINTENANCE

The Device Maintenance page contains three tabs: Config Control, Package Control, and Wing Commander.

4.7.1. CONFIG CONTROL

Config Control is the first (left-most) tab of the Device Maintenance page. To navigate to this tab, select Device Maintenance from the main menu.

Figure 74 – Device Maintenance – Config Control



User Configuration Settings

○ Save Configuration using this name [   ].drp

○ Import Configuration from ⚠

○ Delete Configuration

bridge_mode_high_reliability.drp

Firmware Upgrade Settings

○ Merge settings bundled in upgrade package with current configuration ⚠

Factory Settings

○ Restore Factory Settings ⚠

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

Operations marked ⚠ will require you to perform a "Reset Unit", after a successful completion.

Config Control allows you to save (backup) configuration settings and restore configuration settings from saved or backup configuration files to the Viper. The following chapters about using NextGen RF-provided and cloned Viper configurations and upgrading firmware explain possible additional practical applications for controls in this tab.

User Configuration Settings

Save Configuration using this name: This option saves the current user configuration settings in the Viper to the user-specified file. Valid characters for the file name are a-z, A-Z, 0-9, -, and _. All Viper configuration files must have a **.drp** extension. A missing or invalid file name will cause an Invalid Entry message to pop up. To save the user configuration settings to a file, click the radio button and enter a file name, and then click Proceed.

Import Configuration from or **Delete Configuration:** These two radio buttons allow you to import or delete a stored configuration file. Both options use the same drop-down list to select the configuration file.

To import a configuration file, click the radio button for **Import Configuration**, select the file from the drop-down list, and click **Proceed**.

Note: Do not load more than five (5) separate configuration files onto a single Viper at a time. Loading too many configuration files onto a Viper can use up excessive device memory and can cause the Viper to malfunction.

To delete a configuration file, click the radio button for **Delete Configuration**, select the file from the drop-down list, and click **Proceed**.

Firmware Upgrade Settings

Merge setting bundled in upgrade package with current configuration:

This option merges upgraded settings with the current configuration. Select this radio button and click Proceed to load an upgrade package and merge the current configuration settings. Then, click Save Config and Reset Unit to reset the Viper to operate with the upgraded firmware and current configuration. (See notes below.)

Notes: The Firmware Upgrade process will replace an existing configuration with one that came bundled with the firmware upgrade package.

A reset of the Viper is required for to complete this process, as indicated by the yellow alert symbol (⚠).

Factory Settings

Restore Factory Settings: Use this selection to return the Viper to factory default settings. (See notes below.)

Important: Activating Restore Factory Settings will reset the IP address of the unit to its default value of 192.168.205.1 and reset the Username and Password to defaults of Admin and ADMINISTRATOR.

Have a record of all original Viper factory settings available before proceeding with restoring to factory settings.

Proceed: Click Proceed to apply the settings in this tab.

Cancel: Click Cancel to cancel configuration changes made in this tab.

Note: If you imported or deleted a configuration file in the Viper, or restored factory settings, a reset of the Viper is required for any of these to take effect, as indicated by the yellow alert symbol (⚠).

Note: It is also possible to access the Viper's CLI (Command Line Interface) to restore the factory default values. A terminal emulator program set to 19.2 kbps,N,8,1 can access the CLI via serial cable to the Setup port, then entering the following CLI commands.

```
Login: Admin
Password: current password (or default password ADMINISTRATOR)
default * [Enter] (this will log you out, but log back in as before)
save * [Enter]
stationreset [Enter]
```

The above will reset the Viper and when the Viper is back online, it will have the factory default values including the default Ethernet IP address 192.168.205.1. This will not reset the security parameters, including the password

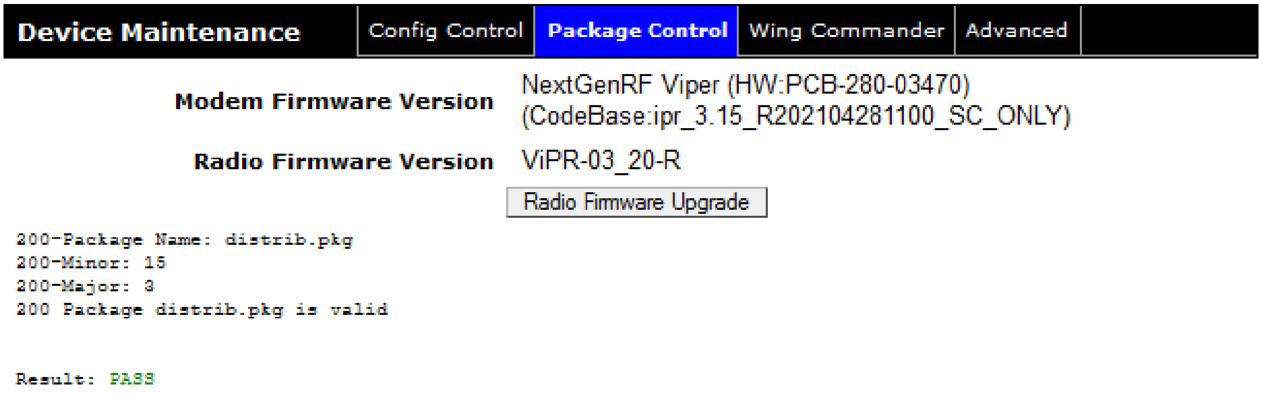
4.7.2. PACKAGE CONTROL

Package Control is the second (middle) tab of the Device Maintenance page. To navigate to this tab, select Device Maintenance from the main navigation menu and click Package Control. From this tab you can view information about installed firmware for the Modem and Radio and upgrade the Radio Firmware if necessary.

Package control is used for verifying a field upgrade of the Viper radio modem firmware. If the installation was successful, the web page will display PASS. If the installation is incomplete or some files are corrupt, the web page will display FAIL and will give an error message specifying which files are missing or corrupt.

If an upgrade problem arises and persists, click the Package Control once more and have the resulting messages available when contacting NextGen RF technical support at support@nextgenrf.com.

Figure 75 – Device Management – Package Control



Modem Firmware Version: NextGenRF Viper (HW:PCB-280-03470) (CodeBase:ipr_3.15_R202104281100_SC_ONLY)

Radio Firmware Version: ViPR-03_20-R

```
200-Package Name: distrib.pkg
200-Minor: 15
200-Major: 3
200 Package distrib.pkg is valid


Result: PASS
```

More information about using the Package Control tab for upgrading firmware is provided in Chapter 6. Upgrading Firmware, which follows.

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

WCP Security

The user must set the WCP security configuration because all WCP communication is encrypted.

WCP Login: Log in using the WCP password before proceeding with the WCP security configuration. Enter the WCP Login in the field provided and click Login.

WCP Password: To set a new password, enter the new password and click Set Passowrd. The password must contain at least three of the following.

- An uppercase alpha character (A-Z).
- A lowercase alpha character (a-z).
- A numeric character (0-9).
- Any other printable character (for example, !@#$%).

Password length must be a minimum of 8 and a maximum of 32 characters.

Data Key Strength: Select the data key strength, either 128, 192, or 256 bits, and click Set Strength.

Data Key: Enter the data key here and click Set Key. This must match the key set in the WCP server database. The key lengthe myst be *exactly* 16, 24, or 32 characters, corresponding to the data key strength values 128, 192, or 256. Click Set Key to set the data key.

Logout and Save: Click to log out and save the new configuration.

Logout and Don’t Save: Click to log out without saving the new configuration. The new configuration will be lost after a unit reset.

WCP Settings

Unit ID: Enter a unique identifier to identify this unit. This can be used when a file upload is targeted to this specific unit.

Group ID: Up to four (4) group IDs may be entered. This unit will participate in a file upload targeting *any* of these Group IDs.

IP Settings

Multicast Group: The WCP server uses multicast messages to target all units simultaneously. Therefore, the multicast group address must match that which is used on the server for a file upload targeting this unit.

Local Port: The IP port number entered here must match that which is used on the server.

Remote IP Address: The destination IP address used when sending WCP messages. (If "auto-response" is enabled, this parameter is not used.)

Remote Port: The destination port number used when sending WCP messages. (If "auto-response" is enabled, this parameter is not used.)

Auto Response: When sending a WCP message (UDP), do not use the remote port and remote IP address configured, but rather send to the IP address and port number of the last WCP message received. When this feature is enabled, drop any message to transmit until at least one message is received.

Note: If you change the Multicast Group or Local Port in the IP Setting section in this tab, a reset of the Viper is required before the setting will take effect, as indicated by the yellow alert symbol (⚠).

General Settings

Forward WC Traffic to RF network: Enable or disable forwarding traffic for the Wing Commander protocol onto the RF network. The default setting is Enabled.

Note: If you change the Forward WC Traffic to RF network Enabled or Disabled, a reset of the Viper is required before the setting will take effect, as indicated by the yellow alert symbol (⚠).

Queued Files Table

The WCP client supports up to five (5) simultaneous file downloads. This table lists the status of each uploaded file.

Server: IP Address of the server uploading the file.

Filename: Filename of the file being uploaded.

Size: Size of the file being uploaded.

Handle: A unique handle with which the server identifies this file.

Blocks: A file upload is broken up into blocks, and the block size is under control for the server. Shown here is the total number of blocks for this file as well as the number of blocks written (received successfully).

Completed: Percent completion of this file upload.

Cmd: Shows the last command received by the WCP client.

Cleanup Files: Click Cleanup Files to clear all entries from the Queued Files Table.

Save: Click Save to save the change if you enable or disable Forward WC Traffic to RF network, or change any of the IP settings in this tab. See Note below.

Cancel: Click Cancel to cancel any change you may have made to any of the settings in this tab.

Note: If you change the Forward WC Traffic to RF network Enabled or Disabled or either of the IP Setting in this tab, a reset of the Viper is required before the setting will take effect, as indicated by the yellow alert symbol (⚠).

5. NETWORK OPTIMIZATION

5.1. MAXIMIZING TCP/IP THROUGHPUT

After optimizing the Viper 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 to how well flow control is implemented in the TCP/IP stack and each application's design. The Viper SC+ has been optimized. 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. LED off periods indicate the application has not presented data to the Viper radio modem.

Using different client/server combinations or applications may show improvements. For example, one FTP server may work 30% faster than another, the buffer management is quicker to respond or has larger message buffers, and 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

5.2.1. USE ROUTER MODE WITH RF ACKNOWLEDGEMENTS ENABLED

Selecting Router mode is highly recommended when running over a weak RF link. This mode ensures that only the necessary packets are passed over the RF interface. Using bridge mode often results in passing more traffic than necessary.

In router mode, you have options to enable Data Retries and enable Collision Avoidance to improve the network performance. The Data Retries and Collision Avoidance mechanisms are also available in bridge mode when communication spans only one RF hop.

Router mode requires some IP route planning to and from Viper units but is well worth the increase in link stability over the simple bridge mode.

5.2.2. REDUCE RF NETWORK BIT RATE

The Viper SC+ has up to four speeds of operation available for each of the five channel bandwidths. The fastest speeds utilize 16-level FSK (frequency shift keying). The slower speeds in each bandwidth utilize 2-, 4-, and 8-level FSK, yielding a higher signal-to-noise level resulting in better sensitivity. When the received RF signal level is strong, the system can utilize 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 slower over-the-air speed for the system's bandwidth. It may result in better overall performance.

5.2.3. USE DATA RETRIES

Increase Data Retries in the Viper Web Interface in the RF Network Settings » RF Bandwidth Management tab.

When data retries are enabled, the receiving Viper will reply with a short RF Acknowledge message each time a unicast data packet is received correctly. The RF Acknowledge allows the transmitting Viper to verify that the packet was received successfully. This does, however, add a small amount of latency to each packet, reducing overall throughput. If the transmitting Viper does not receive an RF Acknowledge, it will retransmit the message again, up to the maximum number of data retries specified.

5.2.4. USE COLLISION AVOIDANCE

Enable Collision Avoidance in the Viper Web Interface in the RF Network Settings » RF Bandwidth Management tab.

When enabled, the Collision Avoidance feature will transmit a short two-way handshake between the transmitting and receiving Viper. This tells any adjacent Vipers that a data transmission will be taking place. Adjacent Vipers will wait until the data transmission is complete before they try to capture the air by sending a new packet.

The two-way handshake reserves airtime from the network for the packet transmission. It will, however, add a small, fixed latency to each packet. The added latency is small relative to the time it takes to transmit a large packet when the chance of collision is greatest. However, when short packets need to be transmitted, it can sometimes take just as long to complete the two-way handshake as it does to send the short packet.

For this reason, the collision avoidance parameter allows the user to specify the packet size threshold, above which the two-way handshake is implemented. For example, if the Collision Avoidance is set for 128, then the Viper will complete a two-way handshake before sending packets that are larger than 128 bytes, reducing potential congestion. The Viper will NOT complete the two-way handshake before sending packets that are smaller than 128 bytes, improving throughput.

5.2.5. USING NEXTGEN RF-PROVIDED AND CLONED VIPER CONFIGURATIONS

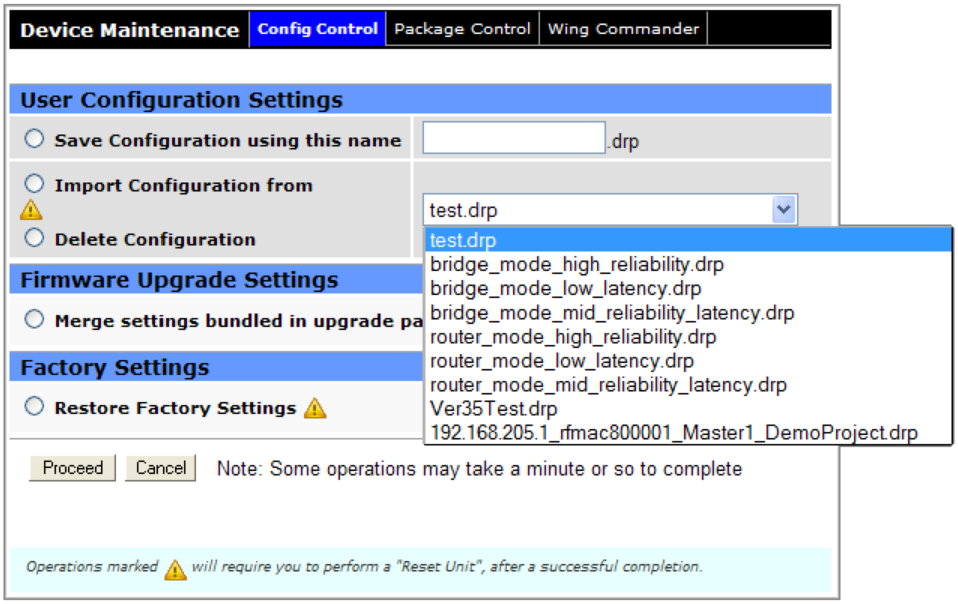
Several configuration files are provided pre-installed, saved in the Viper as shipped. These configuration files can be seen using the drop-down menu in the Config Control tab of the Device Maintenance page of the Viper Web Interface. See the following figure, which shows the list of the sample files.

5.1. USING NEXTGEN RF PRE-PROVIDED (“CANNED”) CONFIGURATIONS

The following figure shows several NextGen RF pre-provided or “canned” configurations. The list you see may differ slightly from the list available at the time of this writing, but the file names should give some insight into the function and purpose for the configuration.

To try any of these pre-installed configurations, select **Device Maintenance** from the Main Menu and then select **Config Control** to navigate to the Config Control tab.

Figure 76 – Drop-down list in Device Maintenance » Config Control Showing Available Sample Configurations


Device Maintenance
Config Control
Package Control
Wing Commander
User Configuration Settings
○ Save Configuration using this name
.drp
○ Import Configuration from
○ Delete Configuration
test.drp
Firmware Upgrade Settings
○ Merge settings bundled in upgrade pa
Factory Settings
○ Restore Factory Settings
Proceed
Cancel

test.drp
bridge_mode_high_reliability.drp
bridge_mode_low_latency.drp
bridge_mode_mid_reliability_latency.drp
router_mode_high_reliability.drp
router_mode_low_latency.drp
router_mode_mid_reliability_latency.drp
Ver35Test.drp
192.168.205.1_rfmac800001_Master1_DemoProject.drp

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

Operations marked ⚠ will require you to perform a "Reset Unit", after a successful completion.

Click the **down-arrow** at the right of the list box to expand the drop-down menu and select the desired canned configuration from the list, and then click **Proceed** near the bottom of the tab.

Note: A reset of the Viper is required before the setting from the imported canned configuration will take effect, as indicated by the yellow alert symbol (⚠).

If desired, you can go through other page tabs to see how the Viper will be configured when restarted.

Important: If you select a configuration that changes the LAN IP Address from the LAN IP Address you entered in your computer's browser address bar, or changes Usernames and Passwords to access the device, you will need to know these to reconnect via the browser after rebooting the Viper.

For assistance with using NextGen RF-provided configurations or cloned configurations (the following topic) contact support@nextgenrf.com.

5.2. CLONING A VIPER

The Viper configuration can also be cloned (copied) from another Viper by importing an existing configuration file from another Viper. An FTP utility is required to transfer the desired configuration from another Viper to the Viper being cloned from the other. After the configuration file has been transferred to the Viper using an FTP utility, the configuration file will appear as a selection in the drop-down menu shown in preceding figure.

Note: An FTP utility is a separate application the customer must install on his or her PC. NextGen RF does not supply an FTP utility.

Notes about Viper Configuration files and file names

- Valid characters that can be used in the file name are a-z, A-Z, 0-9, - and _. File names must not contain a space character. Because many operating systems and file systems see the space character as a delimiter or separator, using a space in a file name is generally a bad idea. Use the underscore character (_) instead as shown in the sample file names.

- File names are case sensitive. Test.drp is not the same as test.drp (nor is Test.drp or other similar combinations), and each may likely contain configuration settings that differ from each other.
- All file names must end with the .drp extension. The cloned configuration file may be renamed, if desired, but (it must not have any space characters in the file name, and) it must keep the .drp extension to be recognized by the Viper as a possible valid configuration file.
- Do not load more than five (5) separate configuration files into a single Viper. Loading many configuration files into a Viper ma use up an excessive amount of memory and may cause the Viper to malfunction.

After saving the configuration file back into the Viper using an FTP client, follow the instructions for on the previous page to select and use the cloned configuration.

Note: A reset of the Viper is required before the setting from the imported cloned configuration will take effect, as indicated by the yellow alert symbol (⚠).

If desired, you can go through other page tabs to see how the Viper will be configured when restarted using the cloned configuration.

Important: If you use a cloned configuration from another Viper, the LAN IP Address is the one setting that you will want to change from the LAN IP Address setting of the Viper you cloned the configuration from, since each unit on a subnet should have a unique IP Address. After you reset the Viper, you will need to enter its IP Address in your computer's browser address bar. If any changes to Usernames or Passwords were affected, you will also need this information to reconnect and access the Viper via your browser after rebooting.

For assistance with using NextGen RF-provided configurations or cloned configurations (the following topic) contact support@nextgenrf.com.

6. UPGRADING FIRMWARE

6.1. FIRMWARE INTRODUCTION

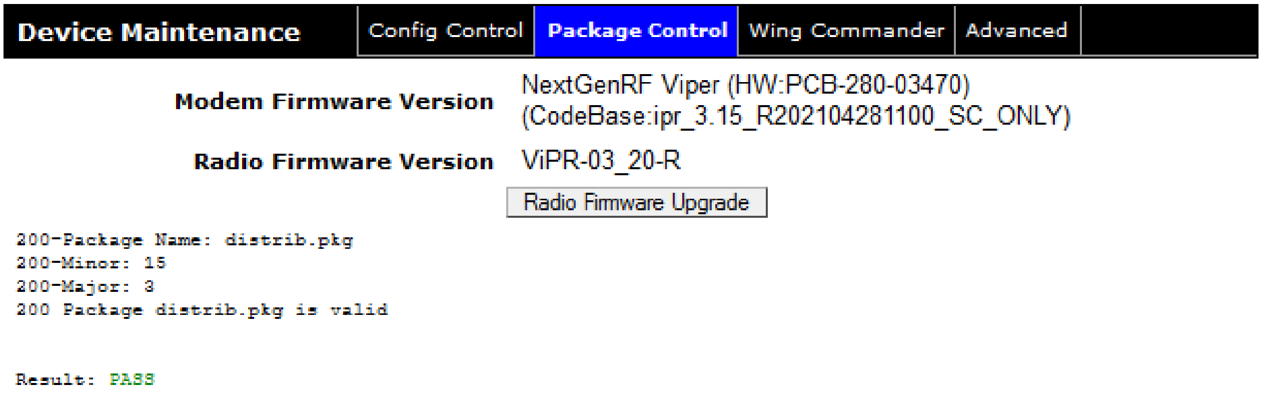
The Viper uses two sets of firmware (code). The Device Maintenance page, shown in the following figure, displays the versions of the Modem and Radio firmware code currently running on the Viper.

Modem Firmware code: This must be updated every time a software upgrade is required.

Radio Firmware code: This code resides on the Viper SC+ transceiver PC board and requires the user to manually perform the upgrade process.

Note: Radio Firmware code does not need to be upgraded each time the Modem Firmware code is upgraded.

Figure 77 – Device Maintenance – Package Control



Modem Firmware Version NextGenRF Viper (HW:PCB-280-03470) (CodeBase:ipr_3.15_R202104281100_SC_ONLY)

Radio Firmware Version ViPR-03_20-R

```
200-Package Name: distrib.pkg
200-Minor: 15
200-Major: 3
200 Package distrib.pkg is valid


Result: PASS
```

6.2. HOW THE VIPER FIRMWARE IS UPGRADED

The Viper firmware code is upgraded by uploading new files into the radio using a FTP (File Transport Protocol) program or by using any FTP utility session. If using FTP, we recommend using a program such as FTP Commander. FTP Commander is available as a demo-version program and can be downloaded from http://www.internet-soft.com/ftpsoftware.htm.

For information on performing an upgrade refer to the applicable Support Bulletins contact support@nextgenrf.com.

6.2.1. UPGRADE THE MODEM FIRMWARE

Very Important – Hardware Versions!

There are earlier hardware versions for the Viper radio: Viper SC and SC+, and pre-SC. Each version requires a different version of the **modem** firmware.

Note: You cannot load modem firmware for the Viper SC or SC+ into a pre-SC Viper.

Upgrade Viper SC and Viper SC+ Modem Firmware

SC Modem firmware version has a Viper 3.X release number. (See the figure above.) This should not be confused with the radio firmware code.

To upgrade the firmware in the modem, refer to the Support Bulletin or our website at http://www. NextGen RF.com/support.

Upgrade Viper Non-SC Modem Firmware

Non-SC modem firmware has a Viper 1.XX release number. This should not be confused with the radio firmware code.

To upgrade the firmware in the modem, refer to the Support Bulletin on our website at http://www. NextGen RF.com/support.

Upgrade Modem Firmware in Older Non-SC Radios

To upgrade the modem firmware in older non-SC radios, refer to the Support Bulletin on our website http://www. NextGen RF.com/support.

6.2.2. UPGRADE THE RADIO FIRMWARE

To upgrade the firmware in the modem, refer to the Support Bulletin on our website at http://www. NextGen RF.com/support.

APPENDIX A – ABBREVIATIONS AND 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.

AES: Advanced Encryption Standard.

Airlink: Physical radio-frequency connection used for communication between units.

ARP: Address Resolution Protocol; maps Internet addresses to physical addresses.

Backbone: The part of a network connecting the bulk of the systems and networks together, handling most of the 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 and Viper SC+ wireless radio modems are COM ports configured as DCE and designed to connect directly to DTE.

CWID: a station identifier or “call sign” broadcast in Morse code at specified periodic intervals to identify the broadcasting radio.

DCE: Data Communication Equipment

Default Gateway: A device forwarding Internet traffic from the Local Area Network (LAN)

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 network 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 in one direction at a time.

HMI: Human Machine Interface. Button panel, keyboard, or touchscreen equipped device that provides a means of human interaction in controlling devices.

HTTP: Hypertext Transfer Protocol; Communications protocol used to connect to servers on the World Wide Web.

Ipconfig: Internet Protocol Configuration; A console application available in Microsoft Windows and Mac OS X that displays all current TCP/IP network configuration values. Displays the IP address for a particular networking device.

LAN: Local Area Network.

MAC: Media Access Control; The unique address a manufacturer assigns to each networking device.

MTU: Maximum Transmission Unit; The largest TCP/IP packet that the 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: Bitrate on the RF link between units in a network.

Node: A network junction or connection point; typically, a computer or workstation.

OIP: Optimized IP; Compresses TCP and UDP headers, and filters unnecessary acknowledgements. 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 (also called a PHYceiver) provides the interface to the 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: A network 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.

PVID: Port VLAN ID.

QoS: Quality of Service; refers to resource reservation control mechanisms.

RADIUS: Remote Authentication Dial in User Service; A networking protocol that provides centralized authentication authorization, and account 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 or performing control operations.

SINAD: Signal-to-Noise and Distortion; a ratio used as a measure of the quality of a signal from a communications device.

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 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 and determining which addresses belong or do not on a specified subnet.

Switch: A device connecting computing devices to host computers, allowing many 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 communication.

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

Terminal Server: Acts as a converter between Ethernet/IP and RS-232 Protocol.

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.

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.

VDC: Voltage Direct Current

VLAN: Virtual Local Area Network

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.

VTS: Virtual Terminal Server

APPENDIX B – VIPER SC+™ SPECIFICATIONS

These specifications are typical and subject to change without notice.

GENERAL SPECIFICATIONS

<table>
<tr><th>Model Number</th><th colspan="2">Frequency Range</th><th colspan="2">Channel Bandwidths Available</th></tr>
<tr><td><b>FCC/IC Certified Models</b></td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td>140-5018-502</td><td colspan="2">136 - 174 MHz</td><td colspan="2">6.25 kHz, 12.5 kHz, 25 kHz, 50 kHz</td></tr>
<tr><td>140-5028-504</td><td colspan="2">215 - 246 MHz*</td><td colspan="2">6.25 kHz, 12.5 kHz, 25 kHz, 50 kHz, 100 kHz</td></tr>
<tr><td>140-5048-302</td><td colspan="2">406.1125 - 470.000 MHz</td><td colspan="2">6.25 kHz, 12.5 kHz, 25 kHz, 50 kHz</td></tr>
<tr><td>140-5048-502</td><td colspan="2">450.000 - 511.975 MHz</td><td colspan="2">6.25 kHz, 12.5 kHz, 25 kHz, 50 kHz</td></tr>
<tr><td></td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td></td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="3"><b>ETSI/ACMA Certified Models</b></td><td colspan="2"></td></tr>
<tr><td>140-5018-600</td><td colspan="2">142 - 174 MHz</td><td colspan="2">12.5 kHz, 25 kHz (ETSI/AS/NZ)</td></tr>
<tr><td>140-5048-400</td><td colspan="2">406.1125 - 470.000 MHz</td><td colspan="2">12.5 kHz, 25 kHz (ETSI/AS/NZ)</td></tr>
<tr><td>140-5048-600</td><td colspan="2">450.000 - 511.975 MHz</td><td colspan="2">12.5 kHz, 25 kHz (ETSI/AS/NZ)</td></tr>
<tr><td>Frequency Stability</td><td colspan="4">1.0 ppm for all models except the models specified below:
0.50 ppm for 140-5028-504,</td></tr>
<tr><td>Modes of Operation</td><td colspan="4">Simplex, Half-Duplex</td></tr>
<tr><td>Frequency Increment</td><td colspan="4">1.25 kHz</td></tr>
<tr><td>Power Source</td><td colspan="4">10-30 V DC, Negative GND
The Viper is UL approved when powered with a listed Class 2 power supply.</td></tr>
<tr><td>RF Impedance</td><td colspan="4">50 Ω</td></tr>
<tr><td>Specified Temperature</td><td colspan="4">- 30° to + 60° C</td></tr>
<tr><td>Operating Temperature</td><td colspan="4">- 40° to + 70° C</td></tr>
<tr><td>Storage Temperature</td><td colspan="4">- 40° to +85°C, non-condensing RH</td></tr>
<tr><td>Operating Humidity</td><td colspan="4">5% to 95% non-condensing RH</td></tr>
<tr><td rowspan="2">Rx Current Drain at 25°C</td><th></th><th>DC Input 10 V</th><th>DC Input 20 V</th><th>DC Input 30 V</th></tr>
<tr><td></td><td>690 mA (max.)
600 mA (typ.)</td><td>345 mA (max.)
300 mA (typ.)</td><td>260 mA (max.)
225 mA (typ.)</td></tr>
<tr><td rowspan="3">Tx Current Drain at 25°C</td><th>Power Out</th><th>DC Input 10 V</th><th>DC Input 20 V</th><th>DC Input 30 V</th></tr>
<tr><td>@ Max. Power</td><td>6.0 A (max.)
3.8 A (typ.)
60 W (max.)</td><td>2.7 A (max.)
2.0 A (typ.)
54 W (max.)</td><td>1.8 A (max.)
1.4 A (typ.)
54 W (max.)</td></tr>
<tr><td>@ 30 dBm (1 W)</td><td>1.8 A (max.)
1.4 A (typ.)</td><td>1.0 A (max.)
0.8 A (typ.)</td><td>0.8 A (max.)
0.6 A (typ.)</td></tr>
<tr><td>Cold start</td><td colspan="4">35 seconds</td></tr>
<tr><td>Nominal Dimensions</td><td colspan="4">5.50 in. W × 2.125 in. H × 4.25 in. D (13.97 cm × 5.40 cm × 10.8 cm) chassis only</td></tr>
<tr><td>Overall Dimensions</td><td colspan="4">6.50 in. W × 2.17 in. H × 4.74 in. D (16.5 cm × 5.51 cm × 12.0 cm) with flat mount plate</td></tr>
<tr><td>Mounting Options</td><td colspan="4">Mounting plate/pattern and DIN Rail</td></tr>
<tr><td>Shipping Weight</td><td colspan="4">2.4 lbs. (1.1 kg)</td></tr>
</table>

Fan Output	5 V DC, 400 mA max.		
Transmitter	**VHF**	**UHF**	
Tx Frequencies	136 - 174 MHz 215 - 240 MHz	406.1125 - 470.000 MHz 450.000 - 511.975 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)		

*Note: Frequencies from 240-246 MHz are for use in Argentina Only.

Receiver						
	Bandwidth Bit Rate	**140-5018-50x**	**140-5028-50x**	**140-5048-30x** **140-5048-50x**		**Units**
Rx Frequencies		136 - 174	215 - 240	406.1125 - 470.000		MHz
				450.000 - 511.975		MHz
Data Sensitivity @ 10^{-6} Bit Error Rate (BER)	**6.25 kHz**					
	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
Typical / Max	**12.5 kHz**					
	8 kbps	-116 / -114	-116 / -114	-116 / -114		dBm
	16 kbps	-109 / -106	-109 / -106	-109 / -106		dBm
	24 kbps	-102 / -98	-102 / -98	-102 / -98		dBm
	32 kbps	-95 / -91	-95 / -91	-95 / -91		dBm
	25 kHz					
	16 kbps	-114 / -111	-114 / -111	-114 / -111		dBm
	32 kbps	-106 / -103	-106 / -103	-106 / -103		dBm
	48 kbps	-100 / -96	-100 / -96	-100 / -96		dBm
	64 kbps	-92 / -88	-92 / -88	-92 / -88		dBm
	50 kHz					
	32 kbps	-111 / -108	-111 / -108	-111 / -108		dBm
	64 kbps	-104 / -101	-104 / -101	-104 / -101		dBm
	96 kbps	-97 / -94	-97 / -94	-97 / -94		dBm
	128 kbps	-88 / -85	-88 / -85	-88 / -85		dBm
	100 kHz					
	64 kbps		-103 / -100			dBm
	192 kbps		-96 / -93			dBm
	256 kbps		-89 / -86			dBm
			-80 / -77			dBm

Receiver						
	Bandwidth Bit Rate	**140-5018-60x**		**140-5048-40x** **140-5048-60x**		**Units**
Rx Frequencies		142 - 174		406.1125 - 470.000 450.000 - 511.975		MHz MHz
ETSI Mode Useable Sensitivity @ 10^{-2} Bit Error Rate (BER)	**12.5 kHz (ETSI)** 8 kbps 16 kbps 24 kbps	 -111 / -108 -104 / -101 -96 / -92		 -111 / -108 -104 / -101 -96 / -92		 dBm dBm dBm
Typical / Max	**25 kHz (ETSI)** 16 kbps 32 kbps 48 kbps	 -110 / -107 -103 / -100 -96 / -92		 -110 / -107 -103 / -100 -96 / -92		 dBm dBm dBm
Adjacent Channel	6.25 kHz	45	45	45		dB
Rejection (min.)	12.5 kHz	60	60	60		dB
	25 kHz	70	70	70		dB
	50 kHz	75	75	75		dB
	100 kHz	—	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	< 15 ms (Band End to Band End)				ms
Receive Input Power	All	17 dBm (50 mW) max.				dBm

Connectors		
Antenna Connector	TNC Female (Tx/Rx)	
Serial Setup Port	DE-9F	
Serial Terminal Server	DE-9F	
Ethernet RJ-45	10 BaseT auto MDIX	
Power – I/O	**Power Header**	**Power Plug**
	NextGen RF P/N 415-7108-113 (Weidmüller P/N 1615550000) 4 Pin, 3.5 mm, Power Header	NextGen RF P/N 897-5008-010 (Weidmüller P/N 1639260000) 4 Pin, 3.5 mm, 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**
	Viper SC+ 200 140-5028-504 140-5028-505	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 128 kbps 192 kbps 256 kbps
Viper SC+						
Viper SC+ ETSI	**Viper SC+ 100 (ETSI AS/NZ)** 140-5018-600 140-5018-601 **Viper SC+ 400 (ETSI AS/NZ)** 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 - 115,200 bps (Default: 19.2 kbps) (100 kHz capable models) Setup Port 300 – 19,200 bps (Default 19.2 kbps) (other models)
	COM Port 300 – 115,200 bps (Default: 9.6 kbps)

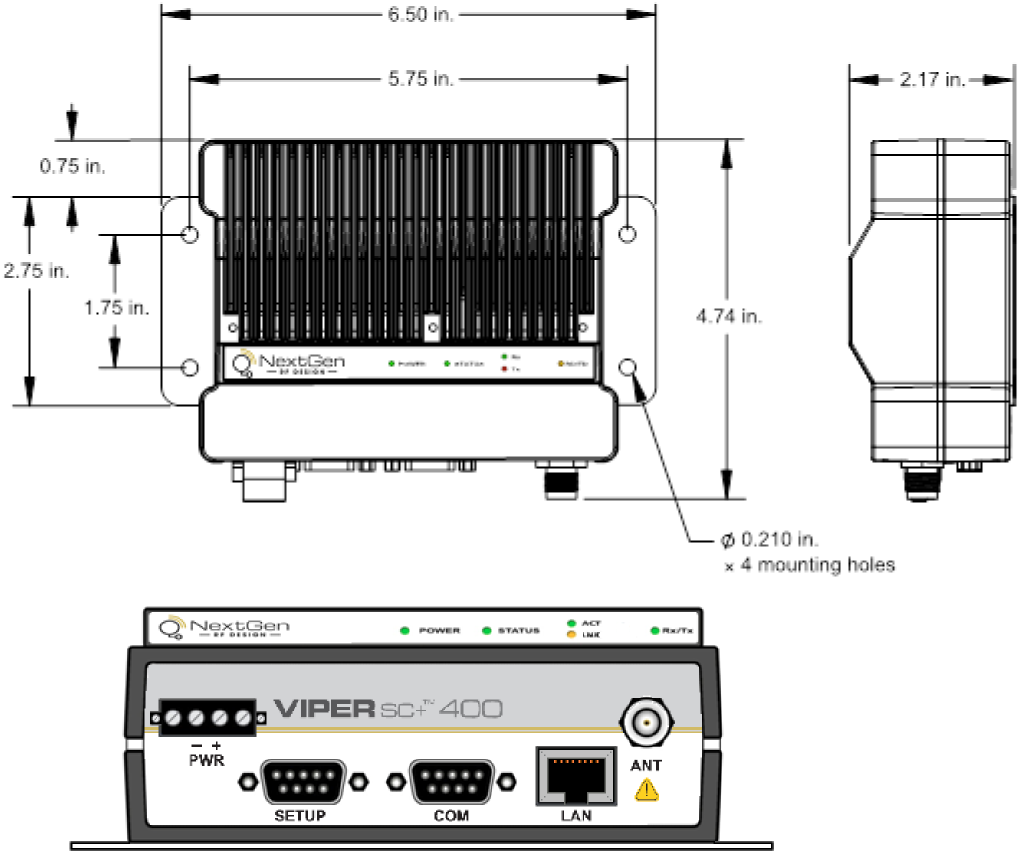
Display	
5 Tri-color status LEDs	Power, Status, Activity, Link, Rx/Tx

Diagnostics	
Message elements	Forward & Reverse Power Temperature Voltage QoS dropped packets Tx & Rx Total Packets

VIPER SC+™ OVERALL DIMENSIONS AND MOUNTING HOLE LOCATIONS

The following figure shows the overall dimensions of the Viper SC+ IP router with mounting plate and locations of mounting holes. The mounting plate allows the Viper to be secured to any surface that can be drilled for this purpose. This drawing may be used for layout reference, but it is advised that an actual physical comparison be made using the Viper and mounting plate before laying out and drilling mounting holes.

Figure 78 – Viper SC+ Chassis and Mounting Plate Overall Dimensions and Mounting Hole Locations



APPENDIX C – VIPER SC+™ REGULATORY CERTIFICATIONS

Domestic and International Certifications					
Model Number	**Frequency Range**	**FCC**	**IC (DOC)**	**European Union EN 300 113**	**Australia / New Zealand**
140-5018-502 140-5018-503	136 - 174 MHz	2AY35-5018-500	27157-5018502		
140-5018-600 140-5018-601	142 - 174 MHz			CE	ACMA AS/NZS 4295-2004 (Spectrum Impact Assessment)
140-5028-504 140-5028-505	215 – 240 MHz	2AY35-5028-504	27157-5028504		
140-5048-302 140-5048-303	406.1125 - 470 MHz	2AY35-5048-300	27157-5048302		
140-5048-400 140-5048-401	406.1125 - 470 MHz			CE	ACMA AS/NZS 4295-2004 (Spectrum Impact Assessment)
140-5048-502 140-5048-503	450 - 512 MHz	2AY35-5048-300	27157-5048302		
140-5048-600 140-5048-601	450 – 512 MHz			CE	ACMA AS/NZS 4295-2004 (Spectrum Impact Assessment)
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
ETSI RED	

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

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

It 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.

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

Language	Declaration
	1999/5/EB Direktyvos nuostatas.
nl Nederlands [Dutch]	Hierbij verklaart NextGen RF dat het toestel radio in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
mt Malti [Maltese]	Hawnhekk, NextGen RF , jiddikjara li dan tar-radju jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
hu Magyar [Hungarian]	Alulírott, NextGen RF nyilatkozom, hogy a rádió megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
pl Polski [Polish]	Niniejszym NextGen RF oświadcza, że radio jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
pt Português [Portuguese]	NextGen RF declara que este rádio está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
sl Slovensko [Slovenian]	NextGen RF izjavlja, da je ta radio v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
sk Slovensky [Slovak]	NextGen RF týmto vyhlasuje, že rádio spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
fi Suomi [Finnish]	NextGen RF vakuuttaa täten että radio tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
sv Svenska [Swedish]	Härmed intygar NextGen RF 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 NextGen RF yfir því að útvarp er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
no Norsk [Norwegian]	NextGen RF 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
Belgium	146 - 174, 406.1 - 430 or 440 - 470 450 - 470	470 - 512
Bulgaria	None	All
Denmark	406.125 - 470, 450 - 511.975	136 - 174
Estonia	None	All
France	Contact Authority	Contact Authority
Germany	Contact Authority	Contact Authority
Greece	142 - 174 421 - 449	406.1250 - 420 450 - 511.975
Hungary	142 - 174 406.125 - 470 450 - 511.975	Contact Authority
Italy	142 - 174	Contact Authority
Latvia	142 - 174 406.125 - 470	450 - 470 470 - 511.975
Lithuania	406.125 - 430 440 - 470	136 - 146 430 - 440 470 - 512
Luxembourg	146 - 156.5125 156.5375 - 156.7625 156.8375 - 169.4	142 - 145 431 - 439 471 - 511.975

Country	Acceptable Frequencies	Prohibited Frequencies
	169.825 - 174 406.1 - 430 440 - 470	
Malta	Contact Authority	Contact Authority
Slovak Republic	146 - 174 410 - 448	142 - 145 406.25 - 409, 449 - 470 450 - 511.975
Slovenia	146 - 174 401.6 - 410, 440 - 470 450 - 470	142 - 145 411 - 439 471 - 511.975
Spain	147 - 174 406.1 - 470	430 - 440
All other EU and EFTA Member States	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.

FCC Emission Designators

Viper SC+ 100 / 400	FCC/IC Type Acceptance – 6.25 kHz / 12.5 kHz / 25.0 kHz					
Model Number	**Channel type**	**Channel Bandwidth**	**Data Rate**	**Baud Rate (kHz)**	**OCBW**	**Emission Designator**
140-5018-502	0	6.25 kHz	4 kbps	4	3.30 kHz	3K30F1D
140-5018-503	1	6.25 kHz	8 kbps	4	3.55 kHz	3K55F1D
140-5048-302	2	12.5 kHz	8 kbps	8	8.20 kHz	8K20F1D
140-5048-303	3	12.5 kHz	16 kbps	8	8.30 kHz	8K30F1D
140-5048-502	4	25.0 kHz	16 kbps	16	16.5 kHz	16K5F1D
	5	25.0 kHz	32 kbps	16	16.8 kHz	16K8F1D
	6	6.25 kHz	12 kbps	4	3.20 kHz	3K20F1D
	7	6.25 kHz	16 kbps	4	3.45 kHz	3K45F1D
	8	12.5 kHz	24 kbps	8	8.50 kHz	8K50F1D
	9	12.5 kHz	32 kbps	8	8.08 kHz	8K08F1D
	10	25.0 kHz	48 kbps	16	17.8 kHz	17K8F1D
	11	25.0 kHz	64 kbps	16	17.0 kHz	17K0F1D

FCC Emission Designators

Viper SC+ 200	FCC Type Acceptance – 6.25 kHz / 12.5 kHz / 25.0 kHz / 50.0 kHz					
Model Number	**Channel type**	**Channel Bandwidth**	**Data Rate**	**Baud Rate (kHz)**	**OCBW**	**Emission Designator**
140-5028-502	0	6.25 kHz	4 kbps	4	3.30 kHz	3K30F1D
140-5028-503	1	6.25 kHz	8 kbps	4	3.55 kHz	3K55F1D
	2	12.5 kHz	8 kbps	8	8.20 kHz	8K20F1D
	3	12.5 kHz	16 kbps	8	8.30 kHz	8K30F1D
	4	25.0 kHz	16 kbps	16	16.5 kHz	16K5F1D
	5	25.0 kHz	32 kbps	16	16.8 kHz	16K8F1D
	6	6.25 kHz	12 kbps	4	3.20 kHz	3K20F1D
	7	6.25 kHz	16 kbps	4	3.45 kHz	3K45F1D
	8	12.5 kHz	24 kbps	8	8.50 kHz	8K50F1D
	9	12.5 kHz	32 kbps	8	8.08 kHz	8K08F1D
	10	25.0 kHz	48 kbps	16	17.8 kHz	17K8F1D
	11	25.0 kHz	64 kbps	16	17.0 kHz	17K0F1D
	12	50.0 kHz	32 kbps	32	33.3 kHz	33K3F1D
	13	50.0 kHz	64 kbps	32	34.3 kHz	34K3F1D
	14	50.0 kHz	96 kbps	32	36.0 kHz	36K0F1D
	15	50.0 kHz	128 kbps	32	33.0 kHz	33K0F1D

FCC Emission Designators

Viper SC+ 200	IC Type Acceptance – 12.5 kHz					
Model Number	**Channel type**	**Channel Bandwidth**	**Data Rate**	**Baud Rate (kHz)**	**OCBW**	**Emission Designator**
140-5028-502	2	12.5 kHz	8 kbps	8	8.20 kHz	8K50F1D
140-5028-503	3	12.5 kHz	16 kbps	8	8.30 kHz	8K50F1D
	8	12.5 kHz	24 kbps	8	8.50 kHz	8K50F1D
	9	12.5 kHz	32 kbps	8	8.08 kHz	8K50F1D

Viper SC+ 200	FCC / IC Type Acceptance – 6.25 kHz / 12.5 kHz / 25.0 kHz / 100 kHz					
Model Number	**Channel type**	**Channel Bandwidth**	**Data Rate**	**Baud Rate (kHz)**	**OCBW**	**Emission Designator**
140-5028-504	0	6.25 kHz	4 kbps	4	3.30 kHz	3K30F1D
140-5028-505	1	6.25 kHz	8 kbps	4	3.55 kHz	3K55F1D
	2	12.5 kHz	8 kbps	8	8.20 kHz	8K20F1D
	3	12.5 kHz	16 kbps	8	8.30 kHz	8K30F1D
	4	25.0 kHz	16 kbps	16	16.5 kHz	16K5F1D
	5	25.0 kHz	32 kbps	16	16.8 kHz	16K8F1D

Viper SC+ 200	FCC / IC Type Acceptance – 6.25 kHz / 12.5 kHz / 25.0 kHz / 100 kHz					
Model Number	Channel type	Channel Bandwidth	Data Rate	Baud Rate (kHz)	OCBW	Emission Designator

FCC Emission Designators

FCC Emission Designators

Viper SC+ 100 / 400	ETSI Type Acceptance – 12.5 kHz / 25.0 kHz					
Model Number	**Channel type**	**Channel Bandwidth**	**Data Rate**	**Baud Rate (kHz)**	**OCBW**	**Emission Designator**
140-5018-600	16	12.5 kHz	8 kbps	8	6.30 kHz	6K30F1D
140-5018-601	17	12.5 kHz	16 kbps	8	6.10 kHz	6K10F1D
140-5048-400	18	12.5 kHz	24 kbps	8	6.00 kHz	6K00F1D
140-5048-401	19	25.0 kHz	16 kbps	16	13.8 kHz	13K8F1D
140-5048-600	20	25.0 kHz	32 kbps	168	13.2 kHz	13K2F1D
140-5048-601	21	25.0 kHz	48 kbps	16	12.9 kHz	12K9F1D

APPENDIX D – UL INSTALLATION INSTRUCTIONS

UL acceptance requires the following installation instructions. These installation instructions are available and may be downloaded from the www.NextGenRF.com website listed on the NextGen RF Product Information Card provided with each unit and include the following:

1. This equipment is suitable for use in Class I, Division 2, Groups A, B, C, and D or non-hazardous locations only.

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

⚠ 2. **WARNING** — EXPLOSION HAZARD — Substitution of components may impair suitability for Class I, Division 2.

3. The unit is to be powered with a Listed Class 2 or LPS power supply rated at 10 to 30 VDC or equivalent.

4. Device must be installed in an end-use enclosure.

5. All wiring routed outside the housing, except for the antenna, must be installed in grounded conduit, following acceptable wiring methods based on installation location and electrical code.

6. The USB and SIM connectors are for temporary connection only during maintenance and setup of the device. Do not use, connect, or disconnect unless the area is known to be non-hazardous. Connection or disconnection in an explosive atmosphere could result in an explosion.

7. Do not operate reset switch unless area is known to be non-hazardous.

APPENDIX E – VIPER SC+™ SITE INSTALLATION AND SETUP GENERAL GUIDELINES

This appendix addresses best-practices instructions for installing and setting up Viper SC+ IP Routers.

There are three areas that need to be reviewed for each site to ensure that the Vipers will perform at a high level. If these areas are thoroughly inspected and any issues found corrected, then the Vipers will perform extremely well. It is important to record the commissioning information to make future troubleshooting simple, even for individuals who have little RF or data protocol knowledge or expertise.

These procedures assume that a basic system Viper configuration (router or bridge mode) has been decided upon by the customer and is known to technical personnel commissioning the sites.

PHYSICAL INSTALLATION

1. Viper power supply
   a. Ensure 60 watts for remote Vipers. 10 – 30 VDC, red and white are positive, black is negative.
   b. Ensure 90 watts for base station Vipers. 10 – 30 VDC, terminals are marked + for positive and – for negative.
   c. Ensure a good connection. White must be tied (shorted) to + positive voltage if not using low-power feature.
   d. Watch the Viper's LEDs to determine if the Viper is resetting when transmitting. This *may* be a sign of inadequate power supply capacity or poor power regulation.

2. Physical mounting
   a. **Remote Vipers**.
      i. Remote Vipers should be mounted in a weather-tight housing. No ventilation is required. Radio operating temperature range is -30° C to 60° C (-22° F to 140° F). When possible, a temperature-controlled environment is recommended.
      ii. When mounting the Viper in a NEMA enclosure, care must be taken to mount the radio in such a way so that the coaxial feedline cables are not kinked or have tight bends. Kinks or tight bends can cause SWR issues and damage the cable.

   b. Viper base stations
      i. Rack-mount base stations should allow for easy access to the top and rear (when practical) for ease of maintenance.
      ii. The base station should be mounted in such a way that prevents the feedline coaxial cable from kinking or having tight bends in the cables. Kinks or tight bends can cause SWR issues and damage the cable.

3. PolyPhaser® (lightning surge protection)
   a. It is extremely important to ensure that the correct type of lightning surge protector device is used. This will be based on the type of antenna being used: grounded or not grounded. Although the antenna specification sheet may indicate the antenna is grounded, this may not be completely true. **Please refer to Section 2.4 Selecting Antenna and Lightning Arrestor combinations, earlier in this Viper SC+ User Manual for the recommended combination of antenna and surge protection devices to use**. Failure to install the correct type of lightning protection device may result in the failure of the Viper's transmitter RF driver and final power devices.
   b. All lightning protection devices must be grounded for the device to provide protection for the equipment. Please refer to the manufacturer's recommended grounding instructions.
   c. For remote Vipers, ensure the device is installed correctly and securely to the housing unit. Water should not be allowed in through this bulkhead mount.

4. Feedline to PolyPhaser® (lightning surge protection device)

   Remote Vipers

   i. All cable connectors should be installed using manufacturer's guidelines.
   ii. Ensure all RF connections at the Viper and at the surge protector are hand-tightened. It is **not recommended** to use pliers or wrenches to tighten RF connectors. TNC male matches to TNC female; N male matches to N female, etc. **Do not crossmatch TNC to N!**
   iii. Ensure there are no tight bends in the cable. Do not kink the cable.

5. Antenna feedline cable to antenna (from PolyPhaser)

   a. At the tower site, NextGen RF recommends that the cable and antenna be analyzed to determine return loss. A low return loss (lower than 15 dB) should be inspected and corrected.
   b. At the remote site, NextGen RF recommends that the cable and antenna be analyzed to determine return loss. A low return loss (lower than 15 dB) should be inspected and corrected.

6. Site grounding

   All sites should have a system ground. The base station or tower ground might be more intricate than at the remote sites. The base station might have a grounding bed outside that the inside grounding network connects to. In all cases, the following devices should have their own grounding cable connecting to the system ground.

   i. Viper (via the back panel or cabinet ground).
   ii. PolyPhaser or an isolated grounding bus.
   iii. Antenna feedline cable shield.
   iv. Power supply.

7. Antenna mounting and alignment

   a. Tower site antennas

   i. Ensure the correct model was installed and record.
   ii. Ensure the antenna is mounted in the vertical, straight up and down.
   iii. Ensure there is the recommended standoff from the tower leg if applicable.
   iv. Ensure there is no other antenna mounted directly across from the antenna.

   b. Remote site antennas

   i. Ensure antenna is mounted at least 12 inches from any obstacle.
   ii. If yagi, ensure yagi is aligned back to the tower location. Check with GPS.
   iii. Ensure yagi is mounted for vertical polarization and is level or slightly angled to the tower if extremely close.

8. Weatherproofing connections

   a. All connections exposed to the weather should be weatherproofed after the site has been tested and verified to pass valid data. Weatherproofing kits are available for outside RF connections. This includes all shield grounds as well.
   b. Follow the manufacturer's recommended installation methods when applying weatherproofing.

VIPER CONFIGURATION (RADIO AND CONTROLLER BOARD FOR BASE STATION)

1. Ensure the latest Viper firmware is installed.
2. Ensure the Viper is configured correctly for each tower group.
    a. Frequencies
    b. Power
    c. Bandwidth and over-the-air data rate
    d. Wing Commander parameters set
    e. Serial port data format correct
    f. Security has the same phrase in all Vipers
3. Ensure unique IP addresses and record for each location.
4. Ensure the base station has been configured correctly and can communicate to the internal Vipers.
    a. Ensure the default gateway has been set in the base station controller.
    b. Ensure it is in auto mode (if redundant base).
    c. Ensure two remote Vipers' IPs have been configured (if redundant base).

RF CONNECTIVITY AND PROTOCOL TESTING

1. Check and record forward and reverse power in Viper.
    a. Key the Viper via the web page RF test and check forward and reverse power readings under RF status.
    b. Correct any power issues if required. If the reverse power is greater than 1.2 watts, verify with a watt meter.
2. Ping the master Viper (from remote).

    Use a ping utility (NextGen RF recommends Integra-TR ping utility; use random data 128 bytes, 200 pings). Ping success rate should be 97% or greater.
3. Check and record RSSI and SNR values.
    a. At the master, record all remotes' RSSI and SNR values.
    b. At the remote, record the master's RSSI and SNR values.
4. Ensure the SCADA host control center can send commands and poll to end devices.

    Verify with the SCADA host control center that commands and responses are sent to and received from remote locations.

APPENDIX F – VIPER SC+™ POWER-SAVE MODE

Viper has offered a Power-Save Mode (PSM) since the release of version 3.4 firmware. The normal power consumption is as follows.

Table 18 Normal Power Consumption for Viper SC+

Rx Current Drain at 25° C		DC Input 10 V	DC Input 20 V	DC Input 30 V
	Maximum	690 mA	345 mA	260 mA
	Typical	600 mA	300 mA	225 mA
Tx Current Drain at 25° C		**DC Input 10 V**	**DC Input 20 V**	**DC Input 30 V**
@ Maximum Power Out	Maximum	6.0 A	2.7 A	1.8 A
	Typical	3.6 A	2.0 A	1.4 A
@ 30 dBm (1 W) Out	Maximum	1.8 A	1.0 A	0.8 A
	Typical	1.4 A	0.8 A	0.6 A

Using a 20 V DC input as an example, typical Rx current drain is 240 mA. Power consumption at this level is 4.8 W. With the PSM enabled, power consumption will drop to less than 2 W, providing a power saving of greater than 40%.

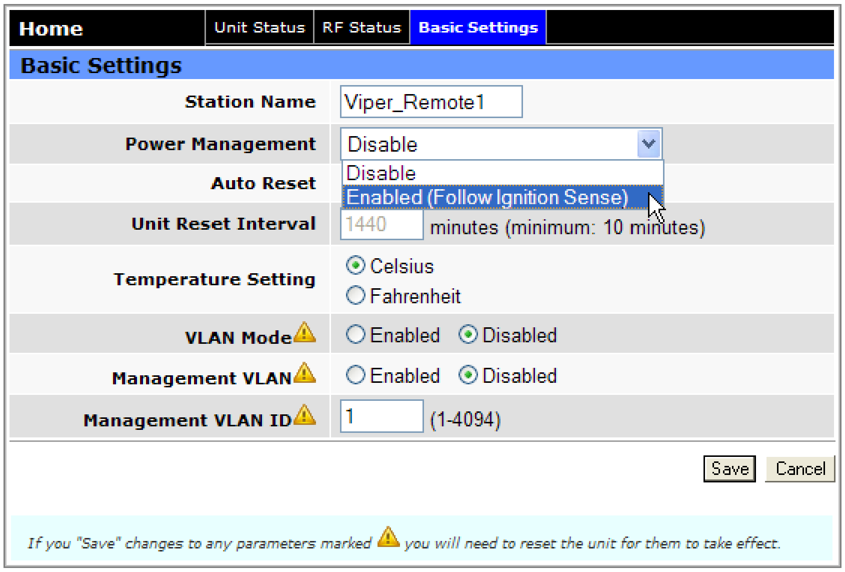
PSM allows for much faster startup (wake-up) time. Normally wake-up time is approximately 30 seconds from a cold start (power off). With PSM, wake-up time is between two to five seconds (2–5 sec.) for full operation.

The following functions are turned off during PSM:

- Transmit and receive; the radio will not receive nor transmit a message while in PSM.
- Communication ports are inactive; the Ethernet and serial ports are not functioning during PSM.

PSM is enabled by programming the Power Management feature of the Viper SC+ in the Basic Settings tab of the Home page by setting the Auto Reset option to Enabled (Follow Ignition Sense), as shown in the following figure.

Figure 79 – Enable Power Management Using the Auto Reset menu in Home » Basic Settings



Basic Settings

Station Name	Viper_Remote1
Power Management	Disable Disable Enabled (Follow Ignition Sense)
Auto Reset	
Unit Reset Interval	1440 minutes (minimum: 10 minutes)
Temperature Setting	● Celsius ○ Fahrenheit
VLAN Mode ⚠	○ Enabled ● Disabled
Management VLAN ⚠	○ Enabled ● Disabled
Management VLAN ID ⚠	1 (1-4094)

If you "Save" changes to any parameters marked ⚠ you will need to reset the unit for them to take effect.

To set up the Viper SC+ to enable or disable PSM using the command-line interface (CLI), use either of the following two commands:

```
set low.power.mode=0    ;(disables PSM.)
set low.power.mode=1    ;(enables psm, follows the state of the “ignition sense” signal)
save                    ;(when selecting either mode, enter save to save your setting.)
```

Selecting Power Management to Enable (follow ignition sense) as shown above, allows the white Ignition Sense line to control the PSM of the Viper SC+.

Normally the White ignition sense line or “Enable” line is tied to the B+ supply along with the Red B+ wire. When used for PSM, the white wire is connected to a line that will toggle from B+ to OFF. When B+ is applied, the Viper SC+ will be powered up as normal. When B+ is removed, the PSM sleep mode is enabled in less than 500 milliseconds (500 ms, or 0.5 sec).

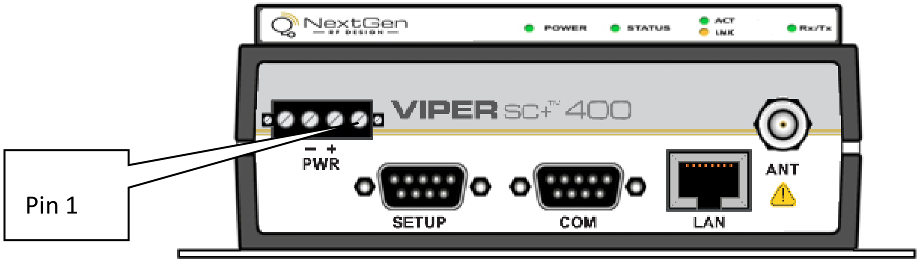
When B+ is reapplied to the White wire, the Viper SC+ will wake up and be in full operation mode in approximately one second (1 s) if VPN is not used. If VPN is used, wake-up time will be less than or equal to five seconds (5 s). Wake-up time may increase if the system is congested since VPN requires the keys to be updated from the VPN server.

The following table shows the maximum current drain used by the White wire. Input voltage is from +10 V DC to +30 V DC. This will allow the user to size the DC switching line to control this feature.

Enable Ignition Sense		
Input Voltage	**Current (Max.)**	**Current (Typ.)**
10 V DC	0.3 mA (max.)	0.2 mA (max.)
20 V DC	0.5 mA (max.)	0.4 mA (max.)
30 V DC	0.7 mA (max.)	0.6 mA (max.)

The following figure shows the Viper SC+ power connector and identifies the location of Pin 1 used for ignition sense.

Figure 80 – Viper SC+ Power Connector Pin 1



The amount of current drain will vary for each radio. Initial testing has shown a current drain of approximately 130 mA at +12 V DC input. This is a power consumption of less than 1.6 W. These are average readings and are not a guaranteed specification. Please Contact NextGen RF Technical Support with any questions. Technical Support can be reached at:

Email: support@NextGenRF.com

Phone: 1.507.514.6245

POWER SAVE MODE FAQS

Q: Is PSM currently available in the Viper product line?

A: Yes. PSM has been supported since the version 3.4 firmware release and all units leaving the factory have version 3.4 or newer firmware installed.

Q: Can I put PSM into a Viper that is not an SC or SC+?

A: No. The Viper must have the Viper SC or Viper SC+ designation to have PSM.

Q: Where can I obtain firmware at the most-current version for my Viper SC+ and for Viper SC units already implemented in the field?

A: Contact NextGen RF technical support by e-mail at support@NextGenRF.com or by phone at 1.507.514.6245.

Q: Can I use my RTU/PLC to control PSM?

A: Yes. A possible scenario might be for the remote PLC to activate the Enable line of the power connector, wait a few seconds, and then send and receive data. Once the response or poll is completed, it places the Viper back into sleep mode by removing B+ from the White wire.

Q: Can I have the Viper SC+ listen for RF carrier to wake up the radio?

A: No. In this case the remote Viper will not wake up since the Viper radio is asleep and does not listen to incoming RF messages. The Ignition Sense line must be toggled from Off to B+ to wake up the radio.

Q: Are there any other power-save modes available in the Viper that I can utilize in my system?

A: No. Currently there are no other power-save modes available.

Q: Can I use PSM on a "Report by Exception" system?

A: Yes. A report by exception polling routine is an excellent opportunity to take advantage of PSM. The Viper SC+ can be allowed to sleep until a condition occurs that triggers the PLC to send a response. The radio can be awakened, message sent, response received, and then PSM enabled again.

Q: My system polling is based on strict controlled timed poll responses. Is PSM of any advantage in this application?

A: Yes. As an example, each remote is polled every 60 minutes. At the end of a polling cycle, the SCADA server could issue a command to the PLC telling it to put the Viper radio to sleep for 55 minutes. The Viper will go to sleep for 55 minutes, then wake up again just before the next poll request is scheduled.

Email: support@NextGenRF.com

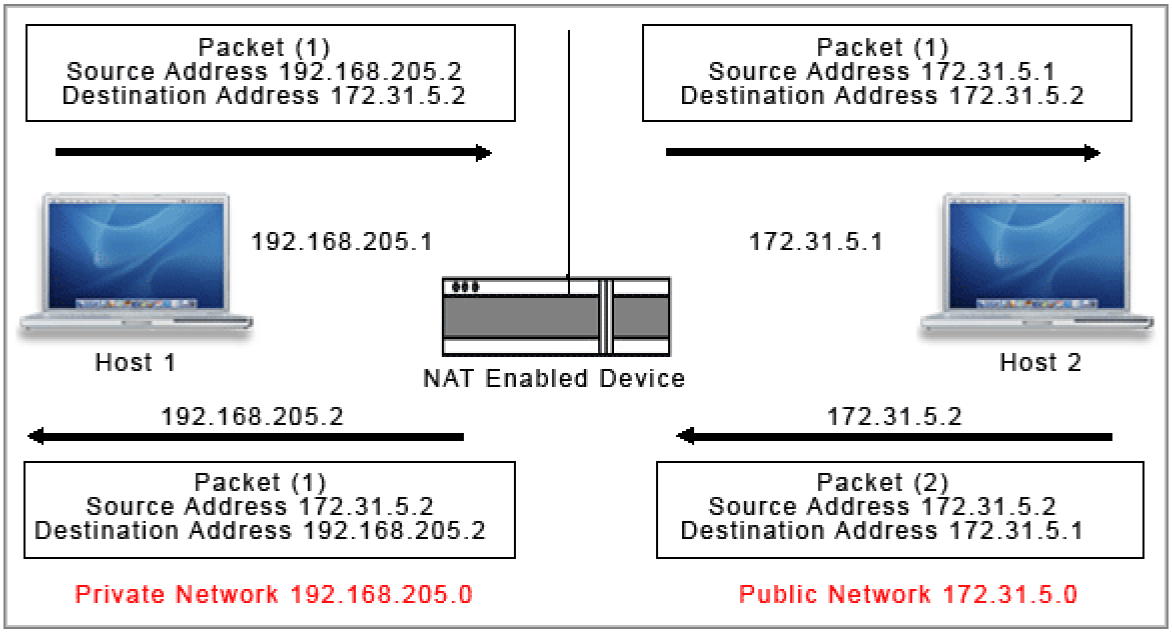
Phone: 1.507.514.6245

APPENDIX G – NAT OVERVIEW

NAT (Network Address Translation) 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 masquerading 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 81 – Basic NAT Operation


Packet (1)
Source Address 192.168.205.2
Destination Address 172.31.5.2
Packet (1)
Source Address 172.31.5.1
Destination Address 172.31.5.2
192.168.205.1
172.31.5.1
Host 1
NAT Enabled Device
Host 2
192.168.205.2
172.31.5.2
Packet (1)
Source Address 172.31.5.2
Destination Address 192.168.205.2
Packet (2)
Source Address 172.31.5.2
Destination Address 172.31.5.1
Private Network 192.168.205.0
Public Network 172.31.5.0

In the above 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, as shown in the preceding figure.

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).

NAT ON VIPER

The purpose of the NAT (Network Address Translation) 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. In a Viper, it is normally used on the WAN side of an IP network to hide local IP addresses from an external IP network.

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 creates an address translation table that is used when traffic is coming back from the public network to the private network.

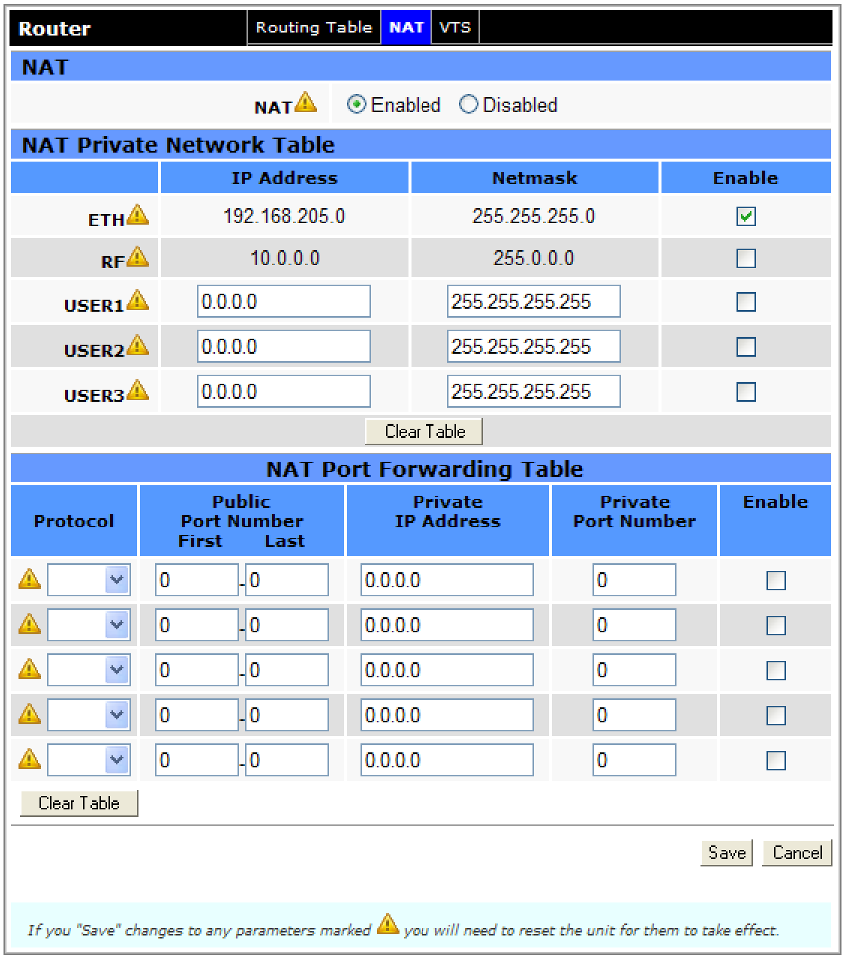
The user can select which of two interfaces (Ethernet or RF) will be considered private. The following examples illustrate how to configure the Vipers. The examples use a private network of

192.168.205.x and a public network of 172.31.5.x.

ETHERNET INTERFACE PRIVATE

The following figure shows NAT enabled for the Ethernet interface.

Figure 82 – NAT Enabled, Ethernet Interface (Private)



NAT

NAT⚠ ● Enabled ○ Disabled

NAT Private Network Table

	IP Address	Netmask	Enable
ETH⚠	192.168.205.0	255.255.255.0	☑
RF⚠	10.0.0.0	255.0.0.0	□
USER1⚠	0.0.0.0	255.255.255.255	□
USER2⚠	0.0.0.0	255.255.255.255	□
USER3⚠	0.0.0.0	255.255.255.255	□

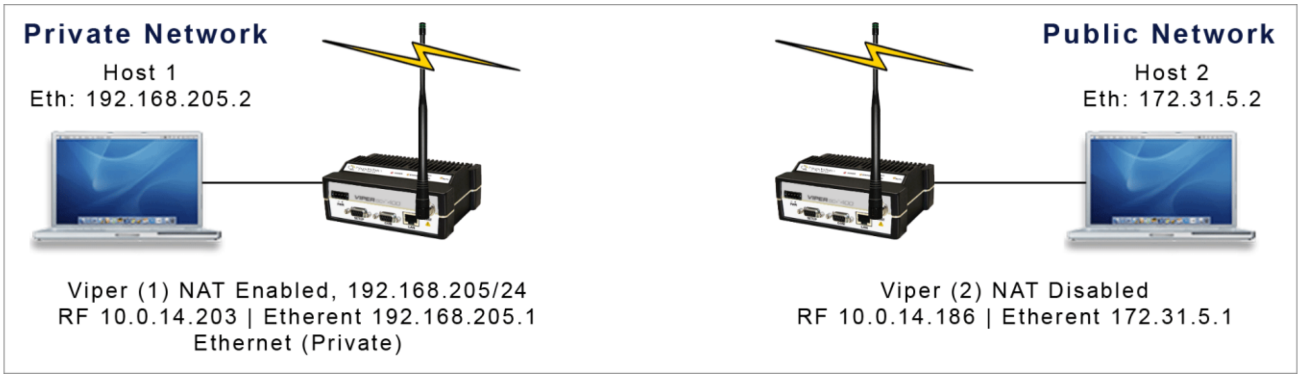
NAT Port Forwarding Table

Protocol	Public Port Number First	Public Port Number Last	Private IP Address	Private Port Number	Enable
⚠	0	0	0.0.0.0	0	□
⚠	0	0	0.0.0.0	0	□
⚠	0	0	0.0.0.0	0	□
⚠	0	0	0.0.0.0	0	□
⚠	0	0	0.0.0.0	0	□

If you "Save" changes to any parameters marked ⚠ you will need to reset the unit for them to take effect.

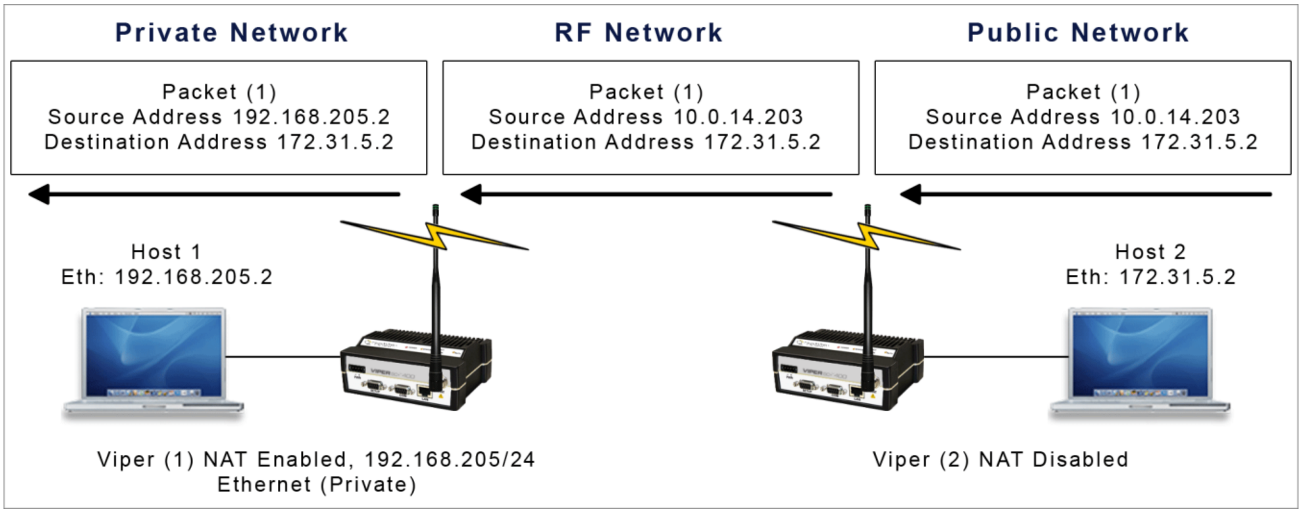
The preceding figure shows the Viper configured protect the Viper (1) Ethernet interface IP address from hosts located on a public network. The following figure shows what this looks like.

Figure 83 – 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 the Viper (1) as shown in the following figure.

Figure 84 – Private to Public Packet Flow

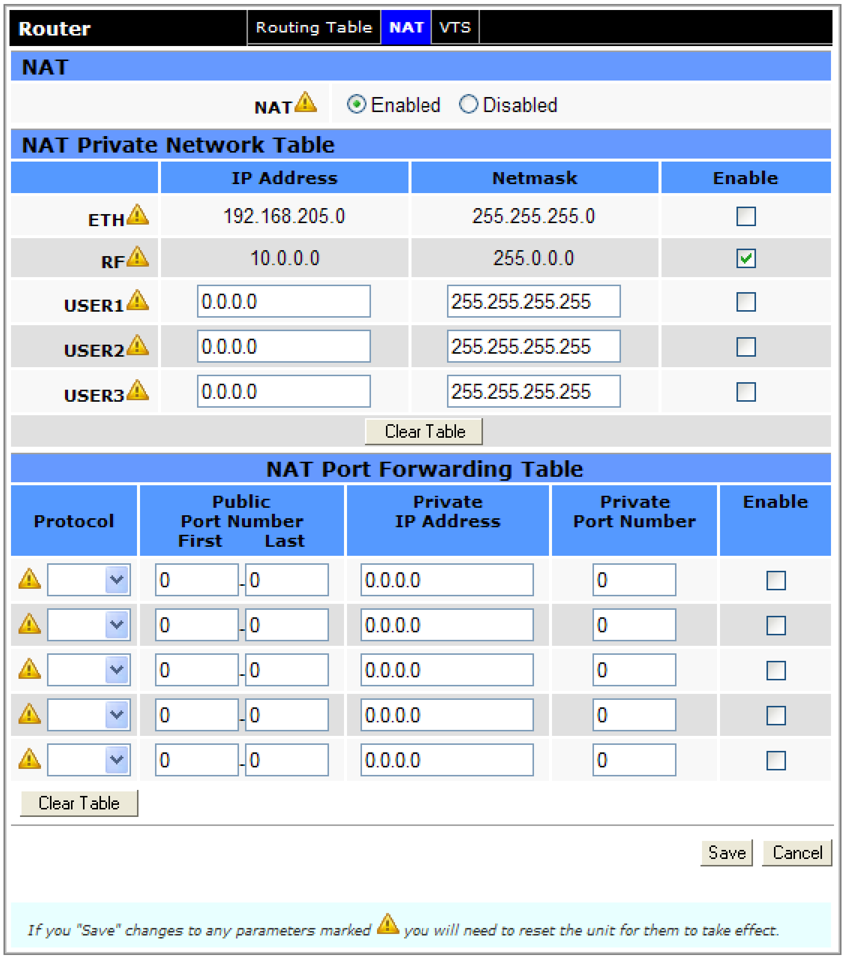

Private Network
RF Network
Public Network
Packet (1)
Source Address 192.168.205.2
Destination Address 172.31.5.2
Packet (1)
Source Address 10.0.14.203
Destination Address 172.31.5.2
Packet (1)
Source Address 10.0.14.203
Destination Address 172.31.5.2
Host 1
Eth: 192.168.205.2
Host 2
Eth: 172.31.5.2
Viper (1) NAT Enabled, 192.168.205/24
Ethernet (Private)
Viper (2) NAT Disabled

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 with NAT Eth enabled.

RF INTERFACE PRIVATE

The following figure shows NAT enabled for the RF interface.

Figure 85 – NAT Enabled, RF Interface (Private)



NAT

NAT⚠ ● Enabled ○ Disabled

NAT Private Network Table

	IP Address	Netmask	Enable
ETH⚠	192.168.205.0	255.255.255.0	□
RF⚠	10.0.0.0	255.0.0.0	☑
USER1⚠	0.0.0.0	255.255.255.255	□
USER2⚠	0.0.0.0	255.255.255.255	□
USER3⚠	0.0.0.0	255.255.255.255	□

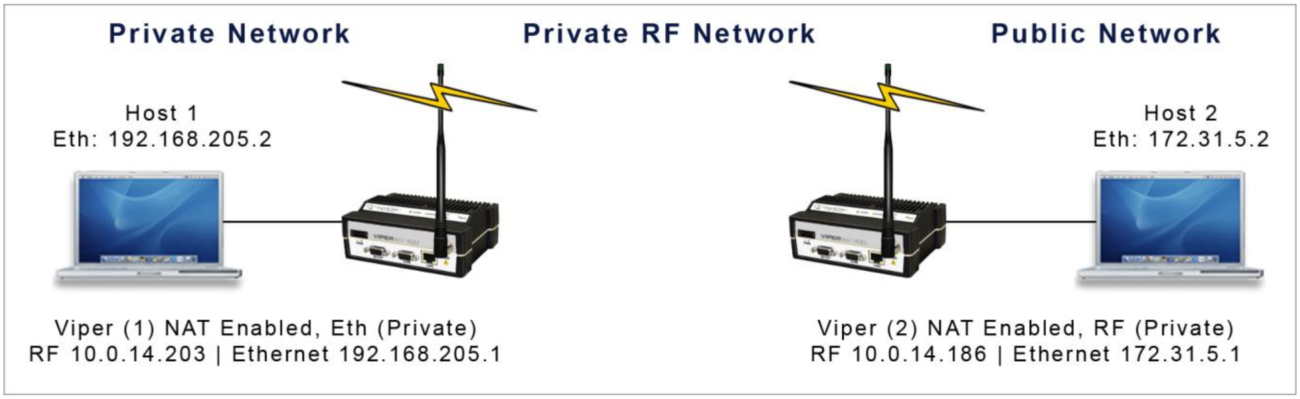
NAT Port Forwarding Table

Protocol	Public Port Number First	Public Port Number Last	Private IP Address	Private Port Number	Enable
⚠	0	0	0.0.0.0	0	□
⚠	0	0	0.0.0.0	0	□
⚠	0	0	0.0.0.0	0	□
⚠	0	0	0.0.0.0	0	□
⚠	0	0	0.0.0.0	0	□

If you "Save" changes to any parameters marked ⚠ you will need to reset the unit for them to take effect.

The preceding figure shows the Viper configured to protect the Viper (2) RF interface and Viper (1) Ethernet interface from hosts located on a public network. The following figure shows what this looks like.

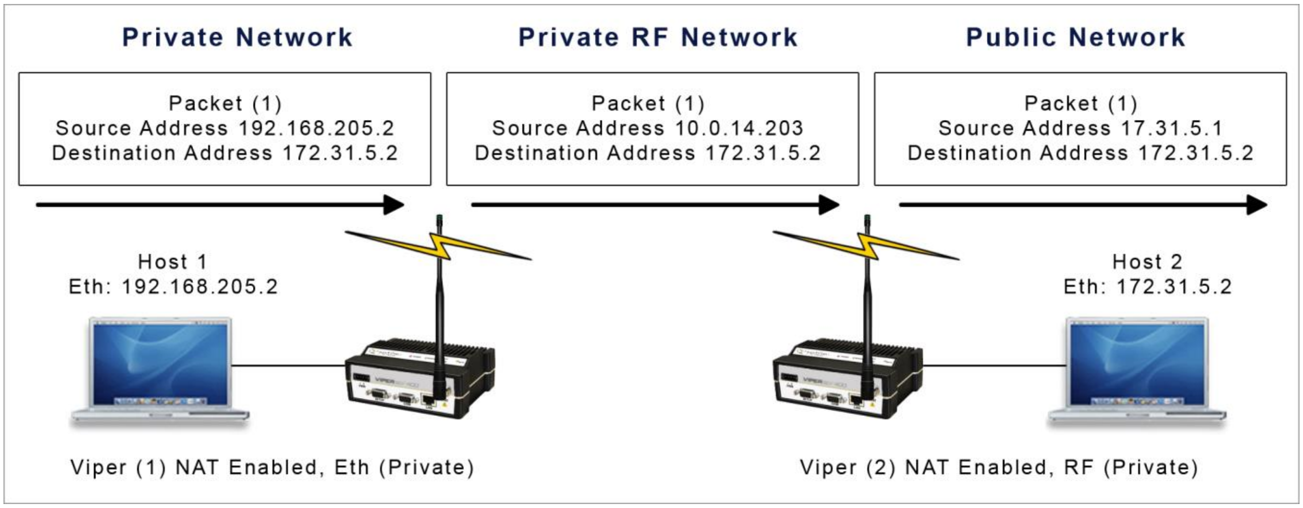
Figure 86 – NAT Enabled, RF (Private), Ethernet (Private)



Private Network
Private RF Network
Public Network
Host 1
Eth: 192.168.205.2
Host 2
Eth: 172.31.5.2
Viper (1) NAT Enabled, Eth (Private)
RF 10.0.14.203 | Ethernet 192.168.205.1
Viper (2) NAT Enabled, RF (Private)
RF 10.0.14.186 | Ethernet 172.31.5.1

An IP packet whose source IP address originates from the RF network and is sent towards the Ethernet network will shows how packets will be modified as the packets pass through the network.

Figure 87 – Packet Flow, Ethernet and RF (Private)


Private Network
Private RF Network
Public Network
Packet (1)
Source Address 192.168.205.2
Destination Address 172.31.5.2
Packet (1)
Source Address 10.0.14.203
Destination Address 172.31.5.2
Packet (1)
Source Address 17.31.5.1
Destination Address 172.31.5.2
Host 1
Eth: 192.168.205.2
Host 2
Eth: 172.31.5.2
Viper (1) NAT Enabled, Eth (Private)
Viper (2) NAT Enabled, RF (Private)

In the following figure, 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 88 – RF Interface (Private)

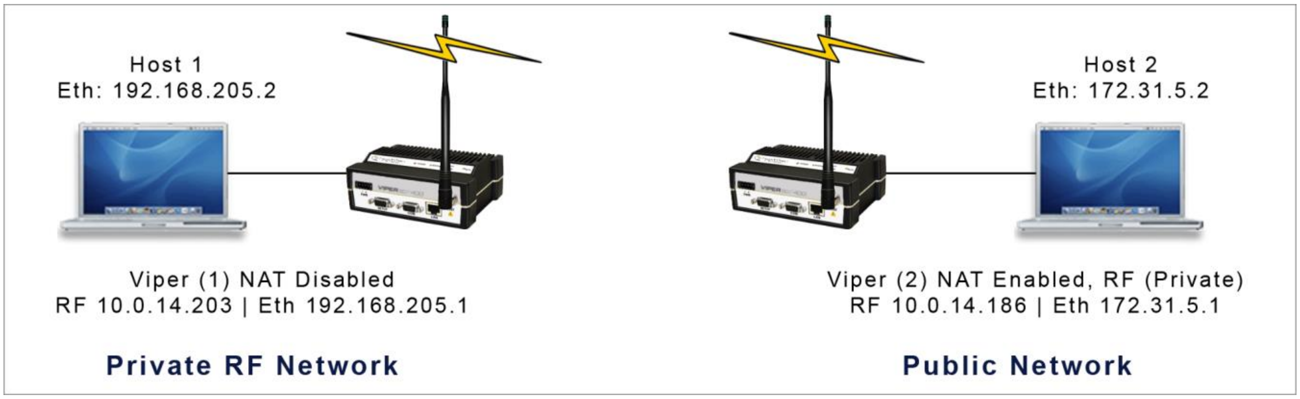
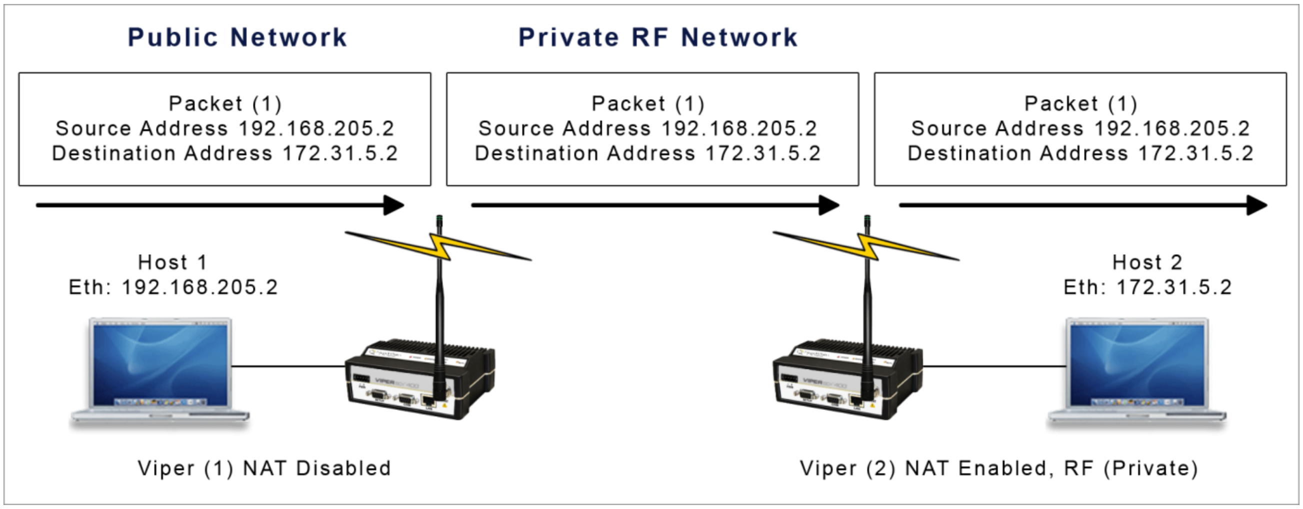

Host 1
Eth: 192.168.205.2
Host 2
Eth: 172.31.5.2
Viper (1) NAT Disabled
RF 10.0.14.203 | Eth 192.168.205.1
Viper (2) NAT Enabled, RF (Private)
RF 10.0.14.186 | Eth 172.31.5.1
Private RF Network
Public Network

Figure 89 – Packet Flow, RF Interface (Private)


Public Network
Private RF Network
Packet (1)
Source Address 192.168.205.2
Destination Address 172.31.5.2
Packet (1)
Source Address 192.168.205.2
Destination Address 172.31.5.2
Packet (1)
Source Address 192.168.205.2
Destination Address 172.31.5.2
Host 1
Eth: 192.168.205.2
Host 2
Eth: 172.31.5.2
Viper (1) NAT Disabled
Viper (2) NAT Enabled, RF (Private)

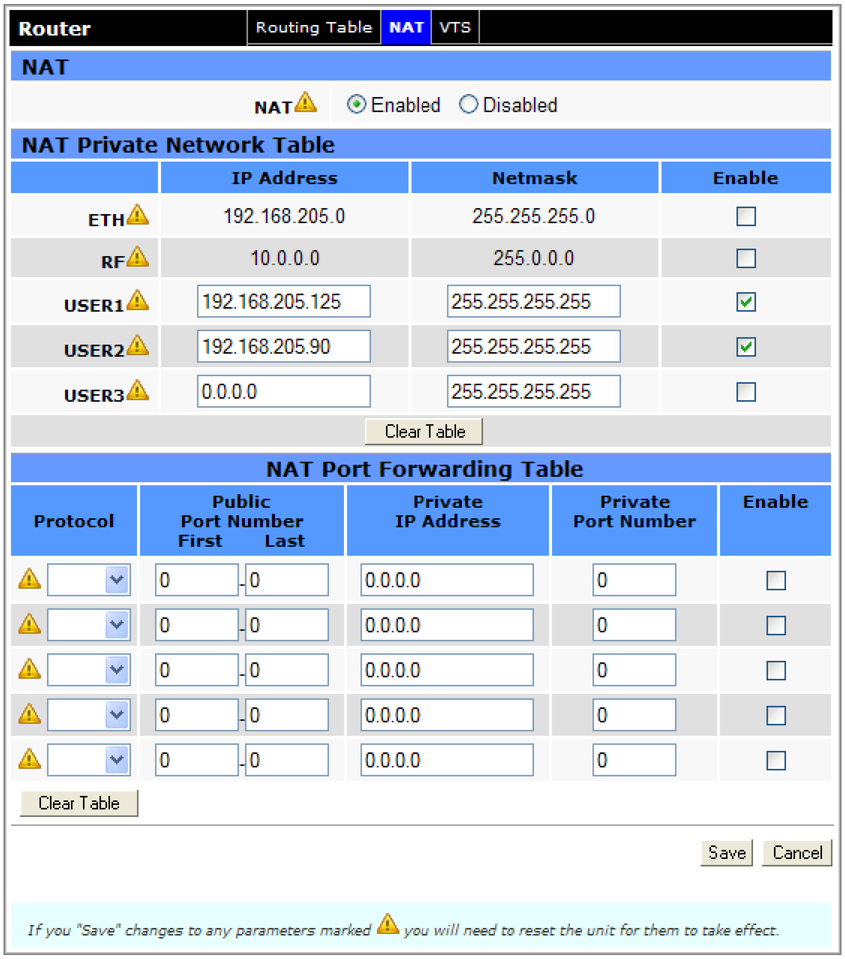
The above figure shows that when Host 1 sends a packet, the source IP address is not changed by Viper (2) because the source does not originate from the private RF network.

USER NAT ENTRIES

The user can add three (3) User IP addresses that will be considered private.

The following figure shows User1 IP address 192.168.205.125 and User 2 IP address 192.168.205.90 will be considered private. If User 3, whose IP address is 192.168.205.87, is connected to the Viper, but not added to the table, User 3 192.168.205.87 would not be considered private.

Figure 90 – User 1 and User 2 (Private)



NAT

NAT⚠ ● Enabled ○ Disabled

NAT Private Network Table

	IP Address	Netmask	Enable
ETH⚠	192.168.205.0	255.255.255.0	□
RF⚠	10.0.0.0	255.0.0.0	□
USER1⚠	192.168.205.125	255.255.255.255	☑
USER2⚠	192.168.205.90	255.255.255.255	☑
USER3⚠	0.0.0.0	255.255.255.255	□

Clear Table

NAT Port Forwarding Table

Protocol	Public Port Number First	Public Port Number Last	Private IP Address	Private Port Number	Enable
⚠	0	0	0.0.0.0	0	□
⚠	0	0	0.0.0.0	0	□
⚠	0	0	0.0.0.0	0	□
⚠	0	0	0.0.0.0	0	□
⚠	0	0	0.0.0.0	0	□

Clear Table

Save Cancel

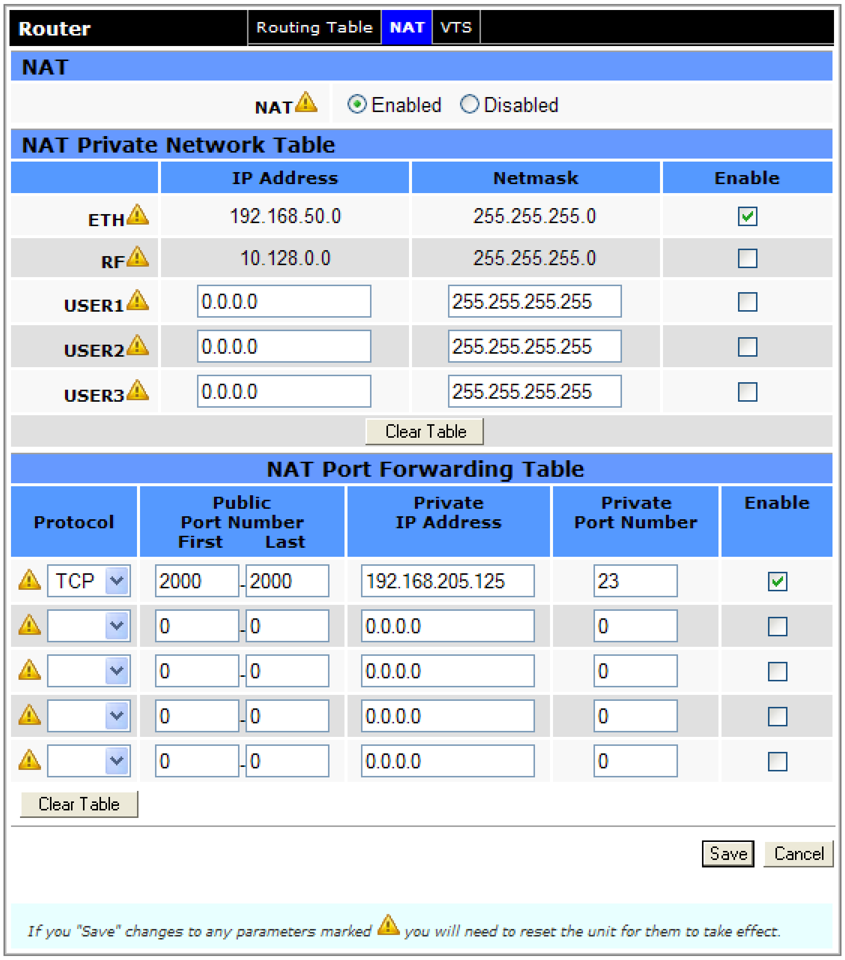
If you "Save" changes to any parameters marked ⚠ you will need to reset the unit for them to take effect.

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.

The following figure 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 Forwarding Table.

Figure 91 – NAT Port Forwarding, Port 2000 is redirected to 192.168.205.125:23



NAT

NAT⚠ ● Enabled ○ Disabled

NAT Private Network Table

	IP Address	Netmask	Enable
ETH⚠	192.168.50.0	255.255.255.0	☑
RF⚠	10.128.0.0	255.255.255.0	□
USER1⚠	0.0.0.0	255.255.255.255	□
USER2⚠	0.0.0.0	255.255.255.255	□
USER3⚠	0.0.0.0	255.255.255.255	□

Clear Table

NAT Port Forwarding Table

Protocol	Public Port Number First	Public Port Number Last	Private IP Address	Private Port Number	Enable
⚠ TCP	2000	2000	192.168.205.125	23	☑
⚠	0	0	0.0.0.0	0	□
⚠	0	0	0.0.0.0	0	□
⚠	0	0	0.0.0.0	0	□
⚠	0	0	0.0.0.0	0	□

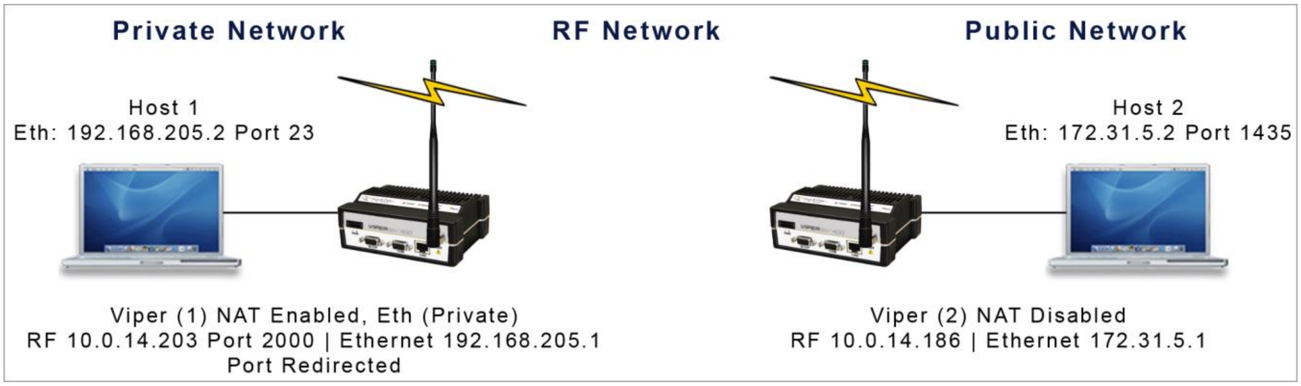
Clear Table

Save Cancel

If you "Save" changes to any parameters marked ⚠ you will need to reset the unit for them to take effect.

The following figure 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 that the IP packets are coming from 10.0.14.203.

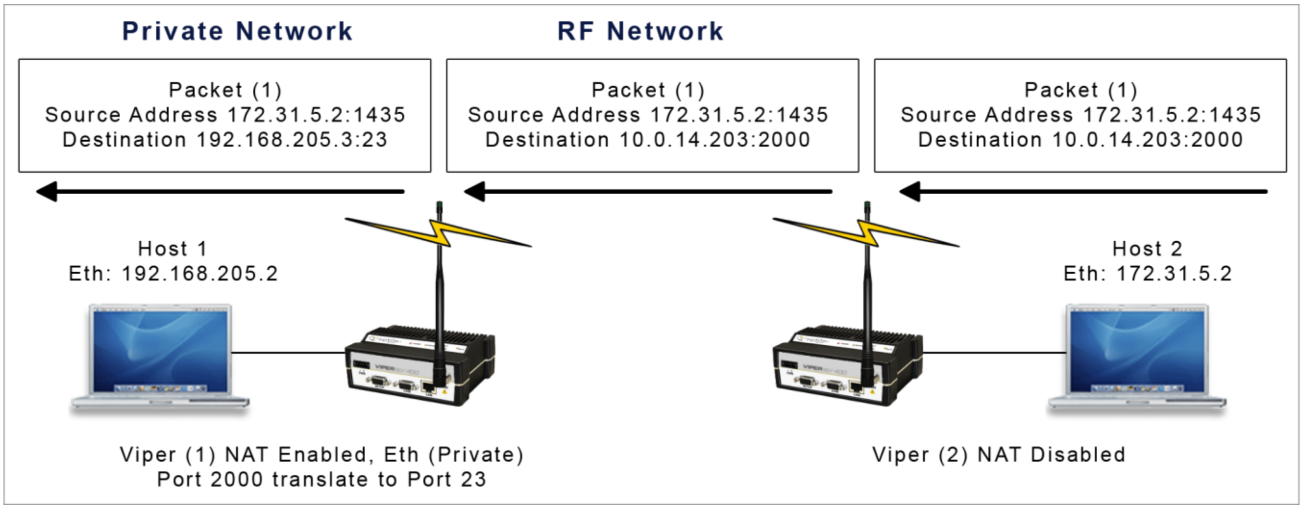
Figure 92 – Port 2000 is redirected to 192.168.205.125:23


Private Network
RF Network
Public Network
Host 1
Eth: 192.168.205.2 Port 23
Host 2
Eth: 172.31.5.2 Port 1435
Viper (1) NAT Enabled, Eth (Private)
RF 10.0.14.203 Port 2000 | Ethernet 192.168.205.1
Port Redirected
Viper (2) NAT Disabled
RF 10.0.14.186 | Ethernet 172.31.5.1

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 1325) to send TCP packets to 192.168.205.5:23 (port 23) by sending the packets to 10.0.14.203:2000 (port 2000).

The following figure shows how the packets would be modified as they moved through the network.

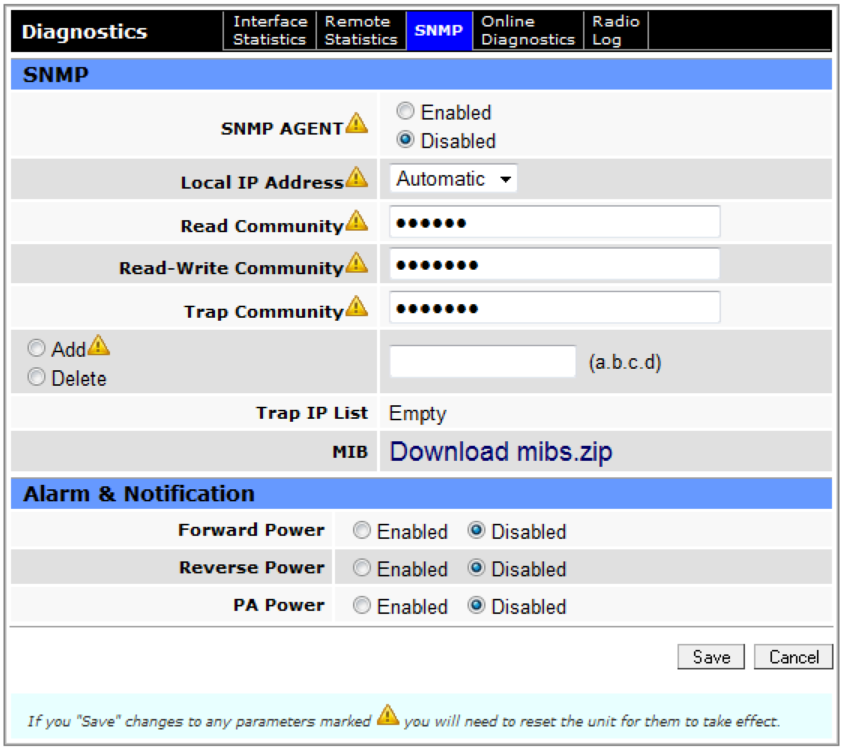
Figure 93 – Packet Flow, Port Redirection


Private Network
RF Network
Packet (1)
Source Address 172.31.5.2:1435
Destination 192.168.205.3:23
Packet (1)
Source Address 172.31.5.2:1435
Destination 10.0.14.203:2000
Packet (1)
Source Address 172.31.5.2:1435
Destination 10.0.14.203:2000
Host 1
Eth: 192.168.205.2
Host 2
Eth: 172.31.5.2
Viper (1) NAT Enabled, Eth (Private)
Port 2000 translate to Port 23
Viper (2) NAT Disabled

APPENDIX H – MIB FILE OVERVIEW

Note: The SNMP feature (and the SNMP tab shown below) is available when enabled in the Diagnostics menu. Three MIB files are bundled with the Viper's firmware. In the Diagnostics » SNMP tab, click the "Download mibs.zip" link to download a .zip file that contains the three MIB files. These files contain links to the SNMP information available in the Viper. The MIB files must be loaded into a third-party MIB browser.

Figure 94 – Viper SNMP tab with Download mibs.zip link



SNMP

SNMP AGENT ⚠ ○ Enabled ● Disabled

Local IP Address ⚠ Automatic

Read Community ⚠ ••••••

Read-Write Community ⚠ •••••••

Trap Community ⚠ •••••••

○ Add ⚠ ○ Delete (a.b.c.d)

Trap IP List Empty

MIB Download mibs.zip

Alarm & Notification

Forward Power ○ Enabled ● Disabled

Reverse Power ○ Enabled ● Disabled

PA Power ○ Enabled ● Disabled

If you "Save" changes to any parameters marked ⚠ you will need to reset the unit for them to take effect.

Caution: Certain MIB browsers (standalone or integrated in an SNMP manager) may require you to modify the MIB file's extension (for example, from .MIB to .TXT).

The three MIB files (found inside the mibs.zip file) are:

(1) nextgenrf-regs.MIB contains a top-level set of managed object definitions aimed at managing products provided under the NextGen RF brand,

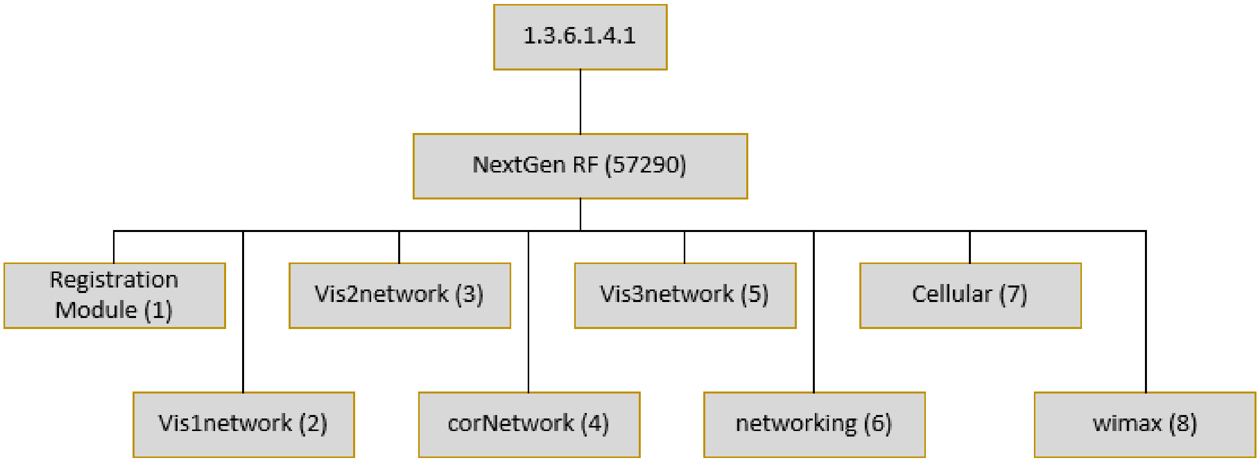
(2) 1213.MIB contains a set of managed object definitions aimed at managing TCP/IP-based network devices, and

(3) Viper_scx.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 form a tree-like structure. The following figure illustrates this tree-like structure for the nextgenrf-regs.MIB, which comes bundled with the Viper firmware. A path to any object can be traced starting from the root (top of the tree). For example, the object titled “NextGenRF” has a unique OID 1.3.6.1.4.1. 57290. The MIB associates each OID with a label (in this example, “NextGenRF”) and various other parameters. When an SNMP manager wants to obtain information on an object, it will assemble a specific message (for example, 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 95 – NextGenRF-REGS MIB tree



Viewing MIB Files

To view the hierarchy of SNMP variables in the form of a tree and view additional information about each node, open each of the MIB files with an MIB browser. In a MIB browser, each object (or node) can be selected, and its properties (including OID) can be viewed. For simple networks, any MIB browser supporting SNMP v2c can 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 Vipers. The same password can be used for both read and read/write. This password is not the same password used to access the Viper Web Interface.

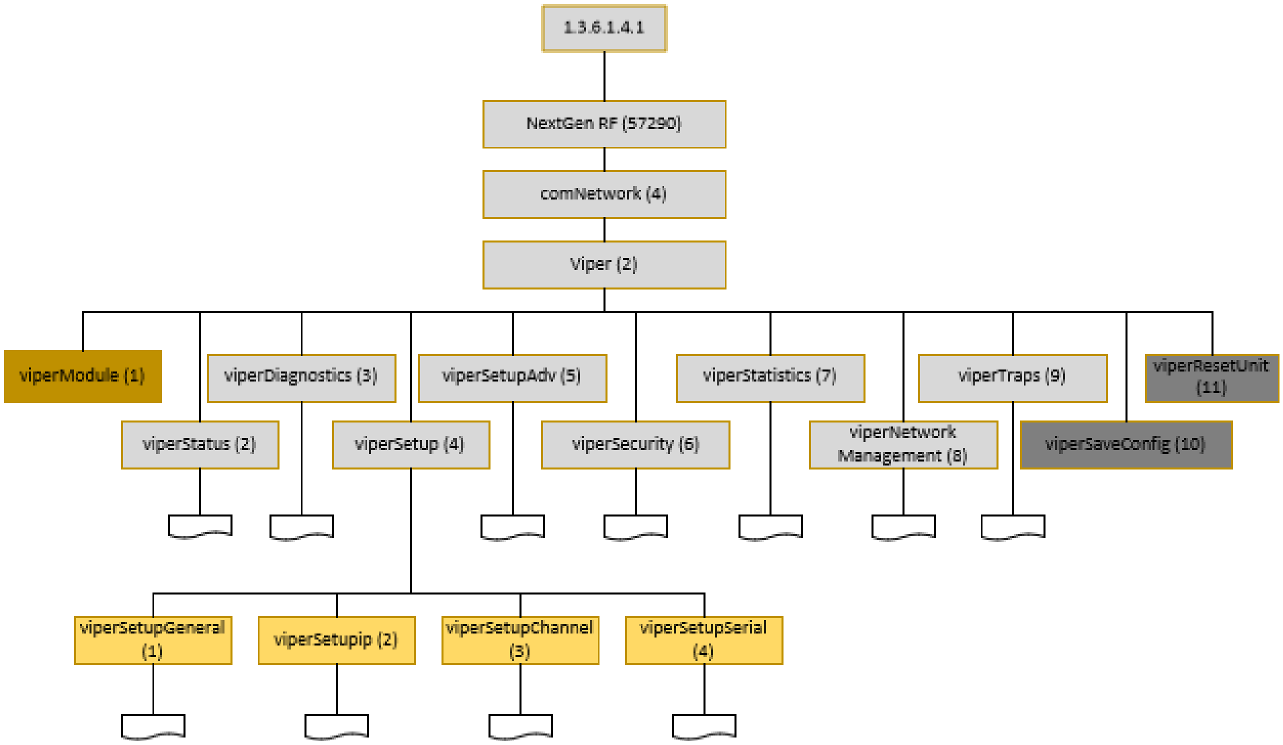
The following figure shows top-level objects of the Viper_scx.mib file. It includes eight branches (b) and three nodes or leaves (l).

- *ViperModule (l)*
- *ViperStatus (b)*
- *ViperDiagnostics (b)*
- *ViperSetup (b)*
- *ViperSetupAdv (b)*
- *ViperStatistics (b)*

- *ViperSecurity (b)*
- *ViperNetworkManagement (b)*
- *ViperTraps (b)*
- *ViperSaveConfig (l)*
- *ViperResetUnit (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 SCx MIB objects can be accessed through an MIB browser.

Figure 96 – Viper OID Tree



APPENDIX I – VLAN INTRODUCTION

When VLAN is enabled, the Viper can perform certain actions based on the interface configuration and the content of packets' VLAN identifiers or "tags." Actions the Viper can perform include adding or removing, or replacing VLAN tags, and filtering or not filtering packets, based on their VLAN tag.

VLAN TAGGING AND UNTAGGING

Adding a VLAN header to an Ethernet packet is called "tagging," and removing a VLAN header from an Ethernet packet is called "untagging."

Packets with a VLAN header can be recognized by looking at the Ethernet type field.

Some common Ethernet types:

```
0x0800 :  Ethernet data is an IP packet.
0x0806 :  Ethernet data is an ARP packet.
0x8100 :  Ethernet data is preceded by a VLAN header.
```

VLAN TAGGING

Reception of an untagged Ethernet packet.

An untagged Ethernet packet is structured like the following.

ETHERNET HEADER			ETH DATA
MAC DST	MAC SRC	TYPE (0x0800)	IP PACKET

Adding a VLAN header to an untagged Ethernet packet.

The VLAN Header is added following the Ethernet Header and before the Ethernet data, as indicated highlighted in beige in the following figure.

ETHERNET HEADER			VLAN HEADER (4 bytes)		ETH DATA
MAC DST	MAC SRC	TYPE (0x8100)	PRIO:0 CFI:0 ID:100	TYPE(0x0800)	IP PACKET

VLAN UNTAGGING

Reception of a tagged Ethernet packet.

The Viper may receive a tagged Ethernet packet structured like the following. (The VLAN header is highlighted.)

ETHERNET HEADER			VLAN HEADER (4 bytes)		ETH DATA
MAC DST	MAC SRC	TYPE (0x8100)	PRIO:0 CFI:0 ID:100	TYPE(0x0800)	IP PACKET

Removing the VLAN header from the tagged Ethernet packet.

The Viper (when configured to remove VLAN tags) removes the VLAN header from the Ethernet packet and it becomes an untagged Ethernet packet.

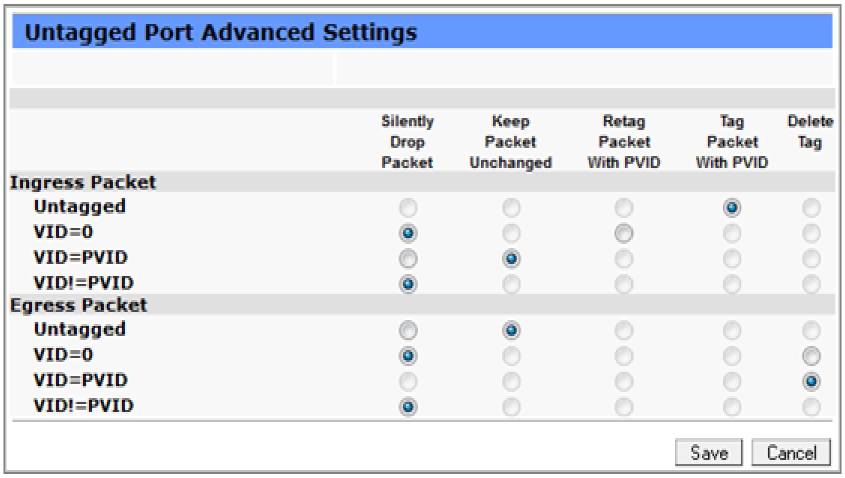
ETHERNET HEADER			ETH DATA
MAC DST	MAC SRC	TYPE (0x0800)	IP PACKET

INTERFACE MODES

When VLAN is enabled (bridge mode only), Viper interfaces can operate in one of two modes: Untagged mode or Tagged mode. (The RF interface is limited to Tagged mode.) Each interface (called a port) is assigned a VLAN ID called a VLAN ID (VID) or Port VLAN ID (PVID).

UNTAGGED MODE

Ingress (incoming) and egress (exiting) packets on an interface operating in Untagged mode will typically be updated using the following rules (available in the VLAN tab for the interface in the Viper Web Interface).



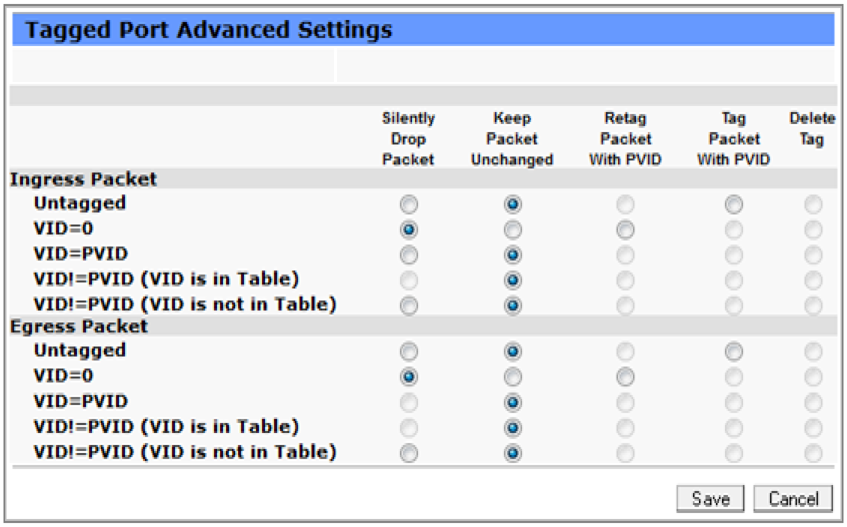
Untagged Port Advanced Settings

	Silently Drop Packet	Keep Packet Unchanged	Retag Packet With PVID	Tag Packet With PVID	Delete Tag
Ingress Packet					
Untagged	○	○	○	●	○
VID=0	●	○	○	○	○
VID=PVID	○	●	○	○	○
VID!=PVID	●	○	○	○	○
Egress Packet					
Untagged	○	●	○	○	○
VID=0	●	○	○	○	○
VID=PVID	○	○	○	○	●
VID!=PVID	●	○	○	○	○

VID is the VLAN ID contained in the packet.
PVID is the Port VLAN ID (the VLAN ID associated with the interface and configured through the Web browser).

TAGGED MODE

Ingress and egress packets on an interface operating in Tagged mode will typically be updated using the following rules (available in the VLAN tab for the interface in the Viper Web interface).



Tagged Port Advanced Settings

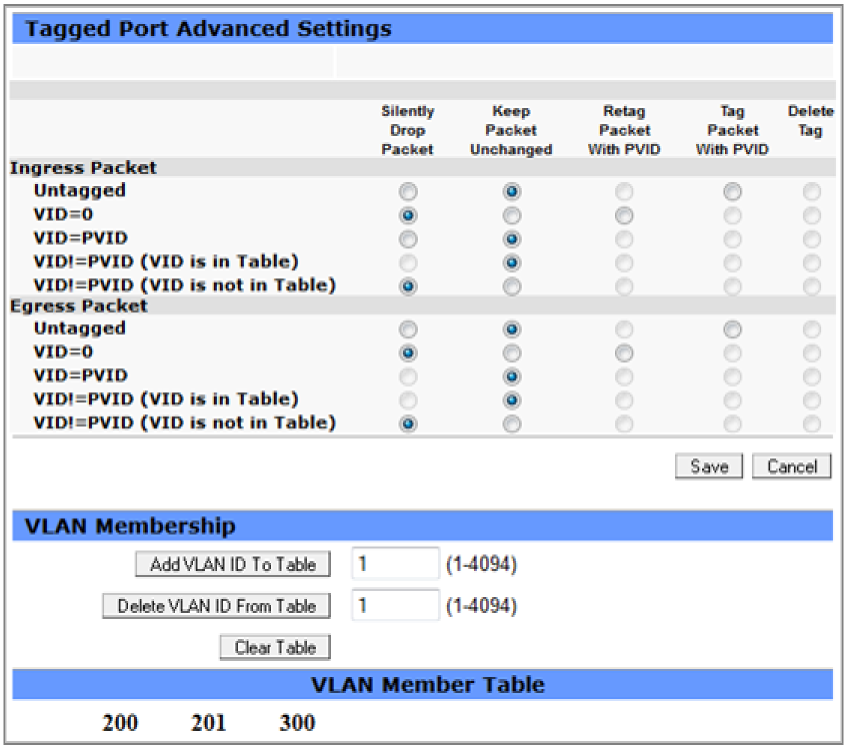
	Silently Drop Packet	Keep Packet Unchanged	Retag Packet With PVID	Tag Packet With PVID	Delete Tag
Ingress Packet					
Untagged	○	●	○	○	○
VID=0	●	○	○	○	○
VID=PVID	○	●	○	○	○
VID!=PVID (VID is in Table)	○	●	○	○	○
VID!=PVID (VID is not in Table)	○	●	○	○	○
Egress Packet					
Untagged	○	●	○	○	○
VID=0	●	○	○	○	○
VID=PVID	○	●	○	○	○
VID!=PVID (VID is in Table)	○	●	○	○	○
VID!=PVID (VID is not in Table)	○	●	○	○	○

VID is the VLAN ID contained in the packet.
PVID is the Port VLAN ID (the VLAN ID associated with the interface and configured through the Web browser).

The Viper Web interface allows you to configure a VLAN Member table to help handle packets with VLAN IDs different than the VLAN ID associated with the interface.

VLAN MEMBER TABLE

The VLAN member table is used for interfaces operating in Tagged mode only. It is used to select the behavior of the Viper when it processes packets with VLAN IDs that are different from the interface VLAN ID (PVID).



Tagged Port Advanced Settings

	Silently Drop Packet	Keep Packet Unchanged	Retag Packet With PVID	Tag Packet With PVID	Delete Tag
Ingress Packet					
Untagged	○	●	○	○	○
VID=0	●	○	○	○	○
VID=PVID	○	●	○	○	○
VID!=PVID (VID is in Table)	○	●	○	○	○
VID!=PVID (VID is not in Table)	●	○	○	○	○
Egress Packet					
Untagged	○	●	○	○	○
VID=0	●	○	○	○	○
VID=PVID	○	●	○	○	○
VID!=PVID (VID is in Table)	○	●	○	○	○
VID!=PVID (VID is not in Table)	●	○	○	○	○

VLAN Membership

Add VLAN ID To Table: 1 (1-4094)

Delete VLAN ID From Table: 1 (1-4094)

VLAN Member Table

200 201 300

You can maintain a list of VLAN IDs used when processing packets where the packet VLAN ID (VID) is not equal to the interface VLAN ID (PVID).

Example:

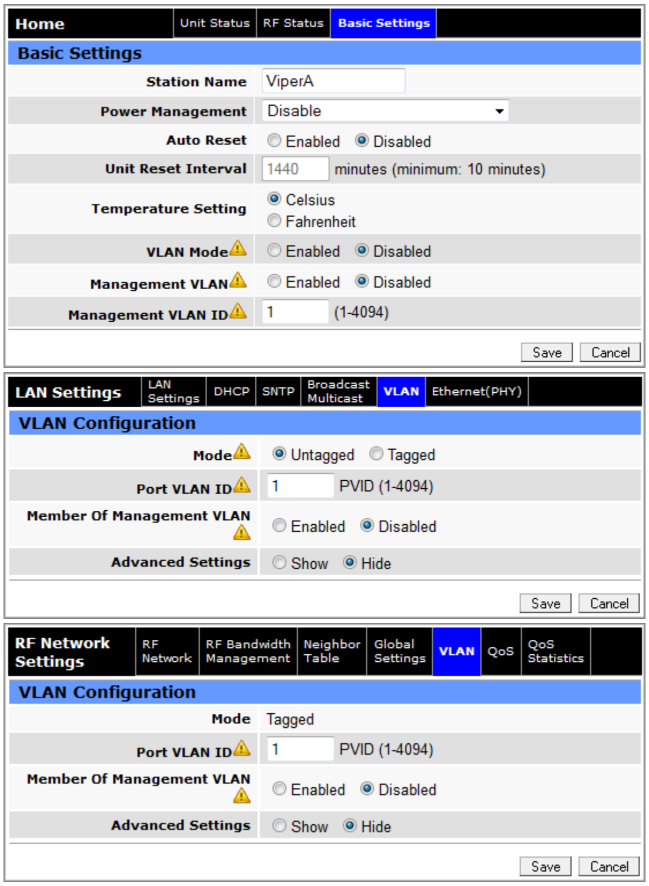
1) LAN interface is operating in Tagged mode.
2) LAN interface PVID = 100.
3) LAN interface contains the advanced configuration shown in the previous figure.
4) The Viper receives a (ingress) packet with VID = 400.
   - ➢ The Viper silently drops the packet because the VID is not equal to the PVID and the VID is not in the Member table.
5) The Viper receives a (ingress) packet with VID = 200.
   - ➢ The Viper keeps the packet unchanged because the VID is not equal to the PVID, but the VID is in the Member table.

EXAMPLES

The following examples show how packets are processed in Bridge mode with VLAN disabled, in Bridge mode with VLAN enabled, and in Router mode.

BRIDGE MODE (VLAN DISABLED)

Viper A Configuration



Home | Unit Status | RF Status | Basic Settings

Basic Settings

Station Name	ViperA
Power Management	Disable
Auto Reset	○ Enabled ● Disabled
Unit Reset Interval	1440 minutes (minimum: 10 minutes)
Temperature Setting	● Celsius ○ Fahrenheit
VLAN Mode ⚠	○ Enabled ● Disabled
Management VLAN ⚠	○ Enabled ● Disabled
Management VLAN ID ⚠	1 (1-4094)

Save Cancel

LAN Settings | LAN Settings | DHCP | SNTP | Broadcast Multicast | VLAN | Ethernet(PHY)

VLAN Configuration

Mode ⚠	● Untagged ○ Tagged
Port VLAN ID ⚠	1 PVID (1-4094)
Member Of Management VLAN ⚠	○ Enabled ● Disabled
Advanced Settings	○ Show ● Hide

Save Cancel

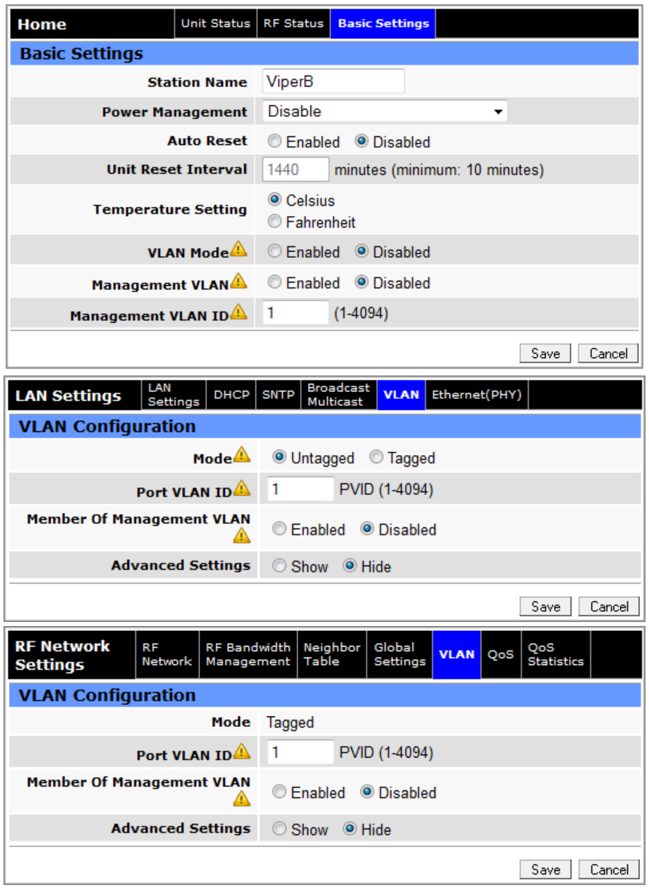
RF Network Settings | RF Network | RF Bandwidth Management | Neighbor Table | Global Settings | VLAN | QoS | QoS Statistics

VLAN Configuration

Mode	Tagged
Port VLAN ID ⚠	1 PVID (1-4094)
Member Of Management VLAN ⚠	○ Enabled ● Disabled
Advanced Settings	○ Show ● Hide

Save Cancel

Viper B Configuration



Home | Unit Status | RF Status | Basic Settings

Basic Settings

Station Name	ViperB
Power Management	Disable
Auto Reset	○ Enabled ● Disabled
Unit Reset Interval	1440 minutes (minimum: 10 minutes)
Temperature Setting	● Celsius ○ Fahrenheit
VLAN Mode ⚠	○ Enabled ● Disabled
Management VLAN ⚠	○ Enabled ● Disabled
Management VLAN ID ⚠	1 (1-4094)

Save Cancel

LAN Settings | LAN Settings | DHCP | SNTP | Broadcast Multicast | VLAN | Ethernet(PHY)

VLAN Configuration

Mode ⚠	● Untagged ○ Tagged
Port VLAN ID ⚠	1 PVID (1-4094)
Member Of Management VLAN ⚠	○ Enabled ● Disabled
Advanced Settings	○ Show ● Hide

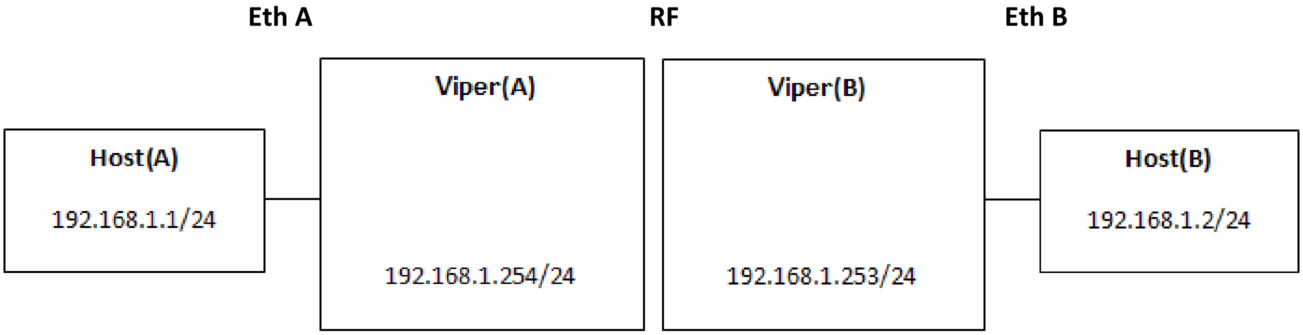
Save Cancel

RF Network Settings | RF Network | RF Bandwidth Management | Neighbor Table | Global Settings | VLAN | QoS | QoS Statistics

VLAN Configuration

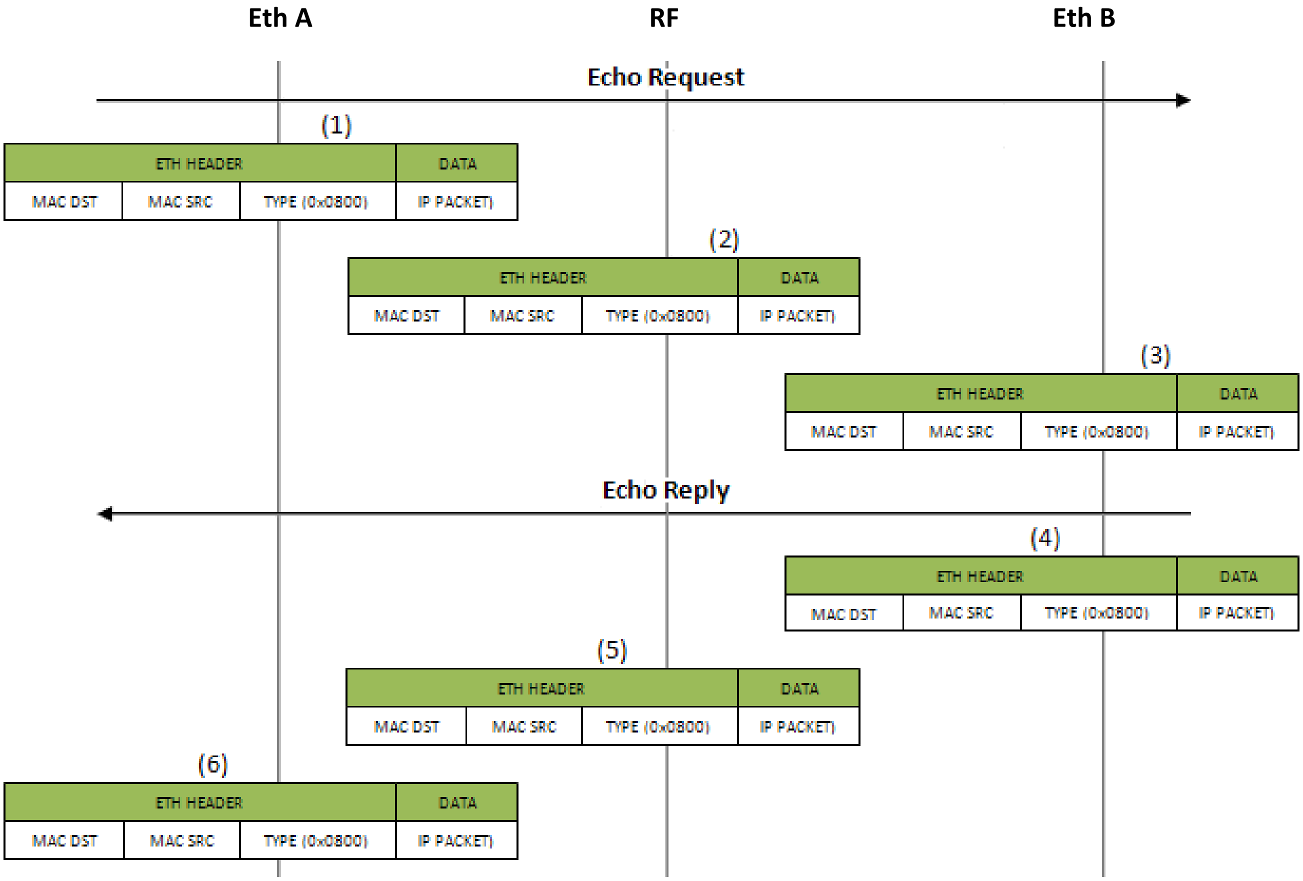
Mode	Tagged
Port VLAN ID ⚠	1 PVID (1-4094)
Member Of Management VLAN ⚠	○ Enabled ● Disabled
Advanced Settings	○ Show ● Hide

Save Cancel



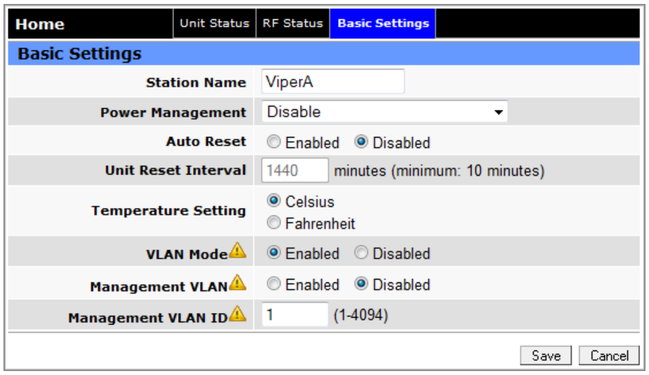
Example:

```
Host(A) C:\> ping 192.168.1.2
```


Eth A
RF
Eth B
Echo Request
(1)
ETH HEADER
DATA
MAC DST
MAC SRC
TYPE (0x0800)
IP PACKET)
(2)
ETH HEADER
DATA
MAC DST
MAC SRC
TYPE (0x0800)
IP PACKET)
(3)
ETH HEADER
DATA
MAC DST
MAC SRC
TYPE (0x0800)
IP PACKET)
Echo Reply
(4)
ETH HEADER
DATA
MAC DST
MAC SRC
TYPE (0x0800)
IP PACKET)
(5)
ETH HEADER
DATA
MAC DST
MAC SRC
TYPE (0x0800)
IP PACKET)
(6)
ETH HEADER
DATA
MAC DST
MAC SRC
TYPE (0x0800)
IP PACKET)

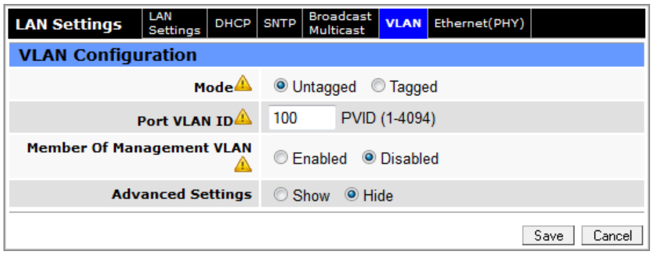
BRIDGE MODE (VLAN ENABLED)

Viper A Configuration



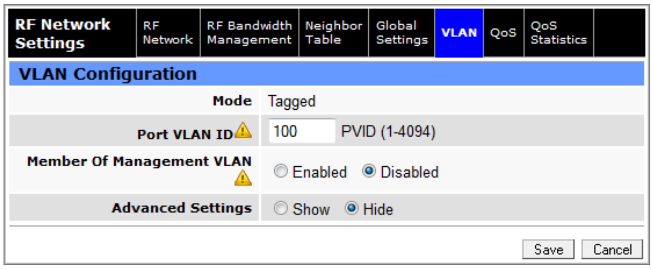
Basic Settings

Station Name	ViperA
Power Management	Disable
Auto Reset	○ Enabled ● Disabled
Unit Reset Interval	1440 minutes (minimum: 10 minutes)
Temperature Setting	● Celsius ○ Fahrenheit
VLAN Mode⚠	● Enabled ○ Disabled
Management VLAN⚠	○ Enabled ● Disabled
Management VLAN ID⚠	1 (1-4094)



VLAN Configuration

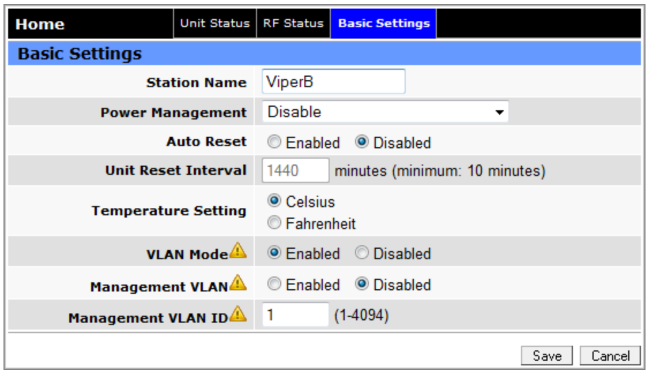
Mode⚠	● Untagged ○ Tagged
Port VLAN ID⚠	100 PVID (1-4094)
Member Of Management VLAN⚠	○ Enabled ● Disabled
Advanced Settings	○ Show ● Hide



VLAN Configuration

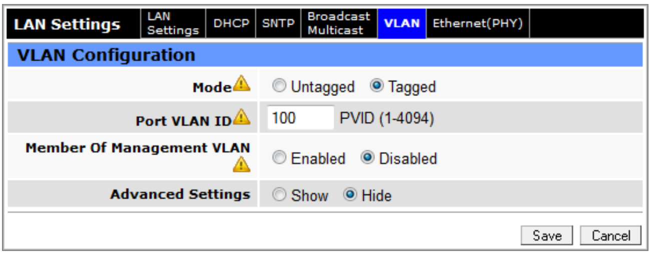
Mode	Tagged
Port VLAN ID⚠	100 PVID (1-4094)
Member Of Management VLAN⚠	○ Enabled ● Disabled
Advanced Settings	○ Show ● Hide

Viper B Configuration



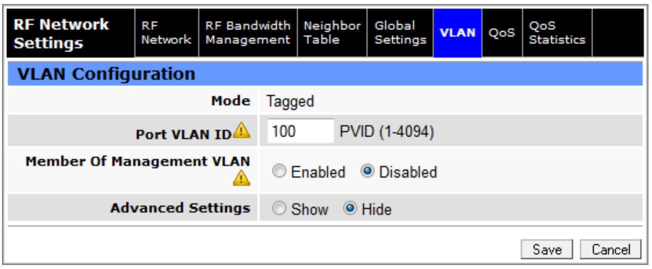
Basic Settings

Station Name	ViperB
Power Management	Disable
Auto Reset	○ Enabled ● Disabled
Unit Reset Interval	1440 minutes (minimum: 10 minutes)
Temperature Setting	● Celsius ○ Fahrenheit
VLAN Mode⚠	● Enabled ○ Disabled
Management VLAN⚠	○ Enabled ● Disabled
Management VLAN ID⚠	1 (1-4094)



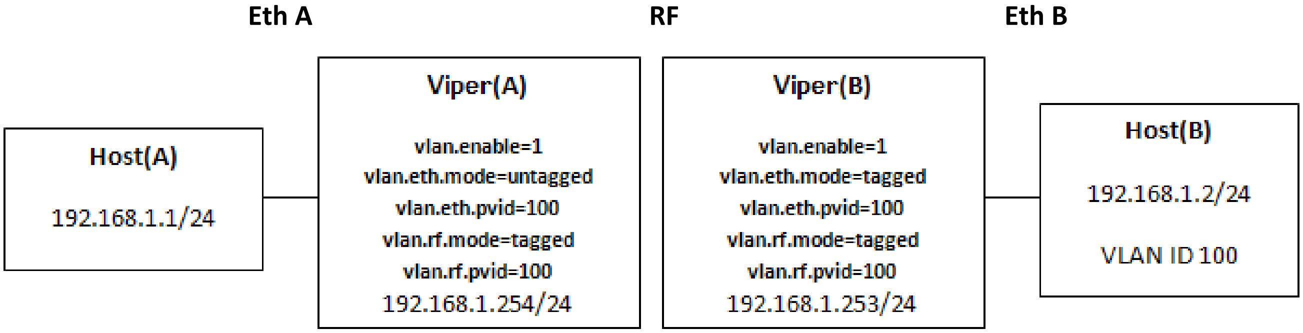
VLAN Configuration

Mode⚠	○ Untagged ● Tagged
Port VLAN ID⚠	100 PVID (1-4094)
Member Of Management VLAN⚠	○ Enabled ● Disabled
Advanced Settings	○ Show ● Hide



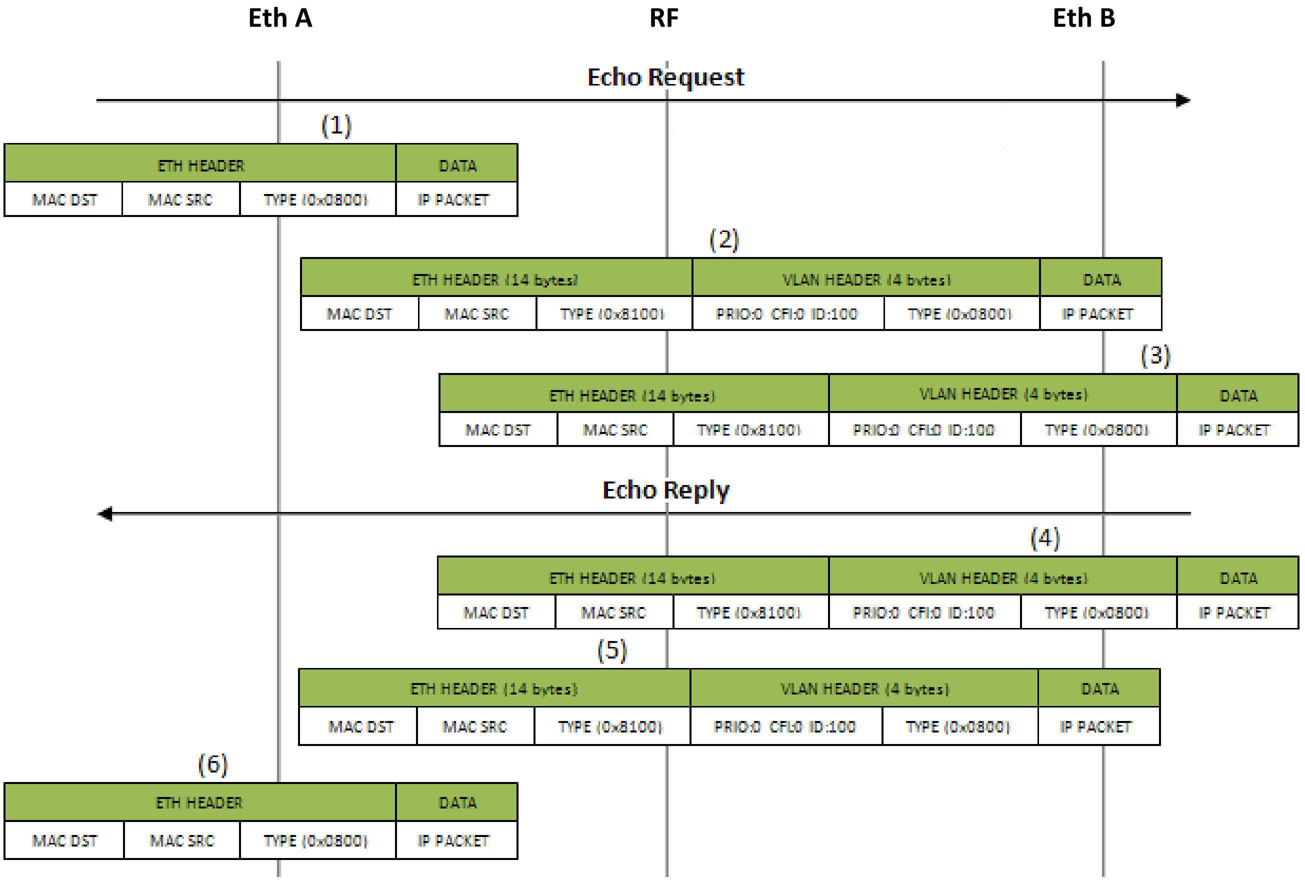
VLAN Configuration

Mode	Tagged
Port VLAN ID⚠	100 PVID (1-4094)
Member Of Management VLAN⚠	○ Enabled ● Disabled
Advanced Settings	○ Show ● Hide



Example:

```
Host(A) C:\> ping 192.168.1.2
```


Eth A
RF
Eth B
Echo Request
(1)
ETH HEADER
DATA
MAC DST
MAC SRC
TYPE (0x0800)
IP PACKET
(2)
ETH HEADER (14 bytes)
VLAN HEADER (4 bytes)
DATA
MAC DST
MAC SRC
TYPE (0x8100)
PRIO:0 CFI:0 ID:100
TYPE (0x0800)
IP PACKET
(3)
ETH HEADER (14 bytes)
VLAN HEADER (4 bytes)
DATA
MAC DST
MAC SRC
TYPE (0x8100)
PRIO:0 CFI:0 ID:100
TYPE (0x0800)
IP PACKET
Echo Reply
(4)
ETH HEADER (14 bytes)
VLAN HEADER (4 bytes)
DATA
MAC DST
MAC SRC
TYPE (0x8100)
PRIO:0 CFI:0 ID:100
TYPE (0x0800)
IP PACKET
(5)
ETH HEADER (14 bytes)
VLAN HEADER (4 bytes)
DATA
MAC DST
MAC SRC
TYPE (0x8100)
PRIO:0 CFI:0 ID:100
TYPE (0x0800)
IP PACKET
(6)
ETH HEADER
DATA
MAC DST
MAC SRC
TYPE (0x0800)
IP PACKET

APPENDIX J – VIPER PLC SETUP

PLC AND LADDER LOGIC SETUP

The general information in this section is designed to assist PLC and system setup and for ladder logic program setup. The focus is on TCP communication. UDP is often friendlier to on-air networks since it requires less handshaking or overhead, but often TCP is the only choice available on PLCs. PLC communication via serial lines or serial terminal server is not covered here, nevertheless the general information provided here may apply.

POLLING REMOTE PLCS WITHOUT UNSOLICITED MESSAGES

When polling multiple PLCs from a master PLC over the RF network, the polling method used has an important influence. To minimize on-air congestion and collision, it is best to sequentially time the polling to each remote and have remotes generating none or few unsolicited inbound messages and making few remote-to-remote PLC messages or none.

The master should be set up as follows.

- Sequentially poll next remote PLC when detecting the ladder logic “done” bit or equivalent message-complete operation or on the later logic “error” bit or equivalent (could be timeout or other).
- Wait for example, 200 milliseconds before polling the next remotes. This allows TCP handshaking to complete. For some systems it may be more or less, and therefore may require tuning afterwards.

POLLING REMOTE PLCS WITH UNSOLICITED MESSAGES AND REMOTE-TO-REMOTE PLC MESSAGES

Polling using unsolicited messages is less preferable than polling sequentially each remote from the master only.

In this case more on-air collisions can occur since messages from the master PLC destined for the remote PLC and messages from any remote destined for the master could have been sent on-air at the same time. These messages will be retried by the Viper (in router mode) and if successful all is fine. If the system traffic is loaded by many remotes and masters sending messages, then many message retries are made and throughput goes down. The Viper protocol also has mechanisms to handle contention, but sometimes there is just too much to handle.

When unsolicited or remote-to-remote PLC messaging is required, then it is important to time or limit the amount of these messages.

For example, the master sequential poll could be set up to give some free airtime between each poll to allow unsolicited messages from remotes or between remotes to use the free airtime to exchange messages. The time to wait between messages depends on overall network load and may only be adjusted once the system is running. Maybe start by using a one-second gap between polls, or derive a value based on the project traffic load.

There are different ways to achieve freeing-up airtime to allow others to communicate. Other ways could also be okay if free on-air time gaps are accomplished often. For example, it may not be good to have a gap every 30 seconds only.

Note: Sometimes polling less often helps to reduce traffic and improve response.

POLLING REMOTE PLCS NON SEQUENTIALLY

Polling messages non-sequentially, where several poll requests are initiated asynchronously overlapping each other, is not recommended since it is less efficient. But if the system cannot be converted or designed with sequential polling, then some of the approaches used above for unsolicited messaging control (adding free on-air time) may need to be applied.

MESSAGING WITH TCP AND TCP CONNECTION TIMEOUT

TCP is a stream protocol where lost parts of the data stream are being retried by the low-level TCP driver of the PLC.

Often the higher-level application of the PLC can function with TCP, UDP, or other. These applications therefore have message timeouts to allow retransmission of a presumed lost or delayed message. With TCP this is not really required since the low-level driver will keep on trying and will only terminate the connection when tries are exhausted.

It is important to set the application message timeout long enough to minimize the application retrying above the TCP driver retries. For example, if the reply for message 1 was not received in time due to temporarily network congestion or outage, and the TCP low-level driver keeps on trying, then the application could end-up sending additional messages (2, 3, and so on). During this congestion or temporarily short network outage period, the retried messages by the application could result in a backlog of outstanding messages and then on recovery resulting in a temporary sort of network storm that may take some time to recover or sometimes turns into a TCP connection failure or termination.

For this case it is better for the application to wait longer than trying to resend the message too quickly resulting in possible multiple responses or connection problems.

The application message timeout should not be made way too long since it may be used by the PLC application to terminate the connection.

A good value for TCP connections timeout that seems to work well is 20 seconds. This gives 20 seconds time to make a new TCP connection. On busy or temporarily congested / multi hop system, 25 or 30 seconds works better. These settings are required for master PLC and remote PLCs.

For message timeout 10 seconds is often good, but on busy or temporarily congested / multi hop system, 15 seconds works better. These settings are required for master PLC and remote PLCs.

If the system is often overloaded, then monitoring is required to determine the cause and the delays. Traffic could be reduced, or timeout needs to be increased.

OPENING A NEW CONNECTION WHILE PREVIOUS TCP CONNECTION IS STILL IN PROGRESS

The PLC should not re-open a new connection while the last one for the same remote PLC is still in progress.

When a TCP connection is attempted by the application the low-level TCP driver will perform several retries to achieve the connection. Often the original TCP connection SYN message is sent then two more are retried using exponential backoff timeouts. This often results in 21 seconds (3 +6+12) for all 3 tries. If the PLC application or sometimes the TCP driver does not wait for the timeout to occur before starting a new connection, then multiple connections to the same destination could be in progress. If the PLC only accepts responses from the last connection attempted, all previous delayed SYN-ACK responses are ignored or terminated.

Note: Making a TCP connection or connection attempt is the initial process to open a TCP connection between two PLCs (also called Endpoints). Once the initial connection message exchanges are completed, the connection is open and ready for data message exchange use.

The above re-open connection scenario can easily occur at one of the following:

- Startup of PLC polling
- A remote not responding
- When temporarily network outage occurs

Having the PLC retrying new connections too quickly, and on multiple remotes at the same time, results in a sort of "message storm," resulting in more congestion.

The PLC application, ladder logic and/or TCP driver should set to wait for the complete connection timeout before starting a new one. Depending on the on-air bandwidth and the number of PLC remotes, only one or a few connection-attempts should be outstanding.

If this cannot be accomplished, then extend the TCP connection timeout to 20 or even 25 seconds. Verify that no other adverse impact occurs.

CLOSING OLD TCP CONNECTION

The PLC should close old TCP connections if no longer required.

When a TCP connection is no longer required, without response, or determined not usable, then the PLC should close it. Leaving these unused TCP connections open consumes Viper internal resources (limited) that could have been used for new connections (Viper TCP proxy buffer resource).

SENDING FRAGMENTED MESSAGES

For best performance, the PLC should use single request message and the response from the remote should also be a single message.

Sending multiple small or fragmented TCP messages over the on-air network is less efficient than grouping the responses for example into a larger single message. Due to TCP/IP message overhead and radio on-air overhead, a small user message with its overhead is much less efficient than multiple small user messages grouped into a single slightly larger message. Also, the on-air protocol often must negotiate the on-air medium to be able to transmit a message, depending on collision retries and traffic, the performance is further affected.

HEARTBEAT MESSAGES

Sending heartbeat messages is generally not recommended. Heartbeat messages should be disabled where possible. If this is not possible then heartbeat messages should only be sent from one endpoint. Their interval should be 4 minutes and start 4 minutes after connection idle time (no data sent in either direction).

If heartbeats are used, depending on the number of connections using them and their interval, the resulting traffic load needs to be evaluated to assess their impact on the on-air network traffic.

AVOID UNNECESSARY TRAFFIC OVER THE AIR NETWORK

Monitoring Remote PLCs with Monitoring Application Tools

Continuously monitoring remote PLCs for monitoring purposes only via the on-air network adds additional traffic. This should be avoided unless required. Some of these software tools are made to run on local networks (high bandwidth) rather than over the air. If used set their timeouts as described above in Messaging with TCP and TCP Connection Timeout.

Some applications when closed still leave their TCP communication layer running. So even if the main display is closed background monitoring still occurs. If this is suspected, use Wireshark to capture whether communication persists, or turn the monitoring PC off temporally to view any impact this has.

Remote Alive Check

Sometimes the PLC could perform pings in parallel to the communication connection. The ping result may be used to determine the presence of the remote or the master. This should be disabled where possible. If required, change ping interval to every 5 or 10 minutes. Check with PLC manufacturer for advice.

MESSAGING WITH TCP – OPENING AND CLOSING TCP CONNECTION FOR EACH POLL

Opening and closing TCP connection for each poll is not recommended. Opening and closing a TCP connection requires 2-3 times more in and out messages then messages for a simple poll. This increases the on-air traffic and adds extra delays for the polling.

It is best to open all the TCP connections at the beginning when starting the poll and closing the TCP connection when poll is stopped. Unsolicited messages done at non-regular intervals and more than 4 minutes apart for the same remote should open and close the TCP connection for each message group.

Having a polling interval of more than 4 minutes for the same remote PLC or having a mixed (more than 4 minutes and less than 4 minutes) interval for unsolicited messages, the TCP connection should be opened and closed each time. With the Viper in proxy mode, after 5 to 10 minutes of inactivity, the Viper will remove the internal proxy context and resume the connection without proxy. Therefore, the benefit for proxy is lost.

When opening and closing is required than the additional traffic load for TCP open and closing needs to be planned into the system design.

SAFE LADDER LOGIC – SUGGESTION

When a PLC remotely controls important operations of another PLC, it would be good to have ladder logic protection in case of communication failure with remote.

For example, one PLC is at the pump station and the other is at the tank station. To avoid tank overflow in case of communication loss, it could be possible to design the logic for the pump PLC to detect that if no data message were received for over 10 minutes from the tank PLC, to turn its pumps off if they were running.

For example, the remote PLC inactivity timeout could trigger this or some other method of detection.

PLC LADDER LOGIC ON RESTART OPENS ALL CONNECTIONS AT ONCE INSTEAD OF SEQUENTIALLY

When the PLC ladder program is set up to have at startup all write message rungs set to true, all TCP connections are triggered “simultaneously.” This creates an overload of TCP SYNs and somewhat could congest the on-air traffic depending on the system.

It is recommended to setup the ladder write message rungs not to start up simultaneously. Write messages should be setup to open the TCP connection sequentially. For more information it may be required to contact your PLC provider.

VIPER GENERAL SETUP WITH PLCS

SET UP VIPER IN ROUTER MODE INSTEAD OF BRIDGE MODE

Note: Viper Bridge Mode cannot filter keep-alive and cannot operate in TCP proxy mode.

If the system has very few units and few messages Viper Bridge mode could be used. But for larger systems and PLC doing many keep-alive, or on-air network being contentious, it may be required to use router mode. Router mode allows retransmission of messages lost due to on-air contention. Bridge mode only does broadcasts without retries. In Bridge mode the application needs to retry lost messages.

FILTERING TCP KEEP-ALIVE WITH VIPER TCP PROXY MODE

When using TCP protocol and having PLCs where the TCP keep-alive rate cannot be controlled, it is important to enable Viper TCP (OIP proxy) mode. This requires that all Vipers be configured in router mode (Viper Bridge mode cannot filter keepalive and cannot operate in TCP proxy mode).

Note: For PLCs where the keep-alive can be controlled and are required, set keep-alive to 4 minutes.

One of the Viper's TCP proxy mode usages allows filtering of keep-alive messages and prevents them to be sent over the air. Without this filtering, several PLCs sending keep-alive messages could easily load the on-air network.

If TCP Proxy mode is not enabled, see documentation earlier in this user manual about using the Viper Web interface to enable it. By default, Viper proxy mode is enabled. See the » RF Bandwidth Management tab. Also see » Neighbor Table (Connectivity Status) to make sure that neighbors are configured with the proxy attribute.

REPLACING OR RESETTING A VIPER USING PROXY MODE WITHOUT RESTARTING POLLING

When replacing or resetting: a remote Viper, a Viper used as a repeater, or even a master Viper connected through a switch, the Viper proxy context is lost. The Viper will reestablish proxy automatically.

ALLEN-BRADLEY PLC FOR VIPER SYSTEM

This guide is intended to assist with Allen-Bradley MicroLogix 1400 and 1100 communication setup between master PLC and remote PLC using an Allen-Bradley TCP protocol between PLCs. Some information may apply for the Allen-Bradley SLC 5 PLC.

PLC communication via serial lines or serial terminal server is not covered here. Nevertheless, some of the information could apply.

Note: Please consult information about general PLC setup presented earlier in this appendix for background information about systems with PLC setup.

ALLEN-BRADLEY MICROLOGIX 1100 OR 1400 (MAY ALSO APPLY TO SLC 5)

Following are important settings recommended to improve communication when used with a limited bandwidth Viper network. This provides more specific information that supplements the general PLC communication information presented earlier in this appendix.

Note: When required, contact your PLC provider or Allen-Bradley or Rockwell Automation support.

PLC Ladder Logic on Restart Opens All Connections at Once Instead of Sequentially

When the PLC ladder program is set up to have at startup all write message rungs set to true, all TCP connections are triggered “simultaneously.” This creates an overload of TCP SYNs and somewhat could congest the on-air traffic depending on the system.

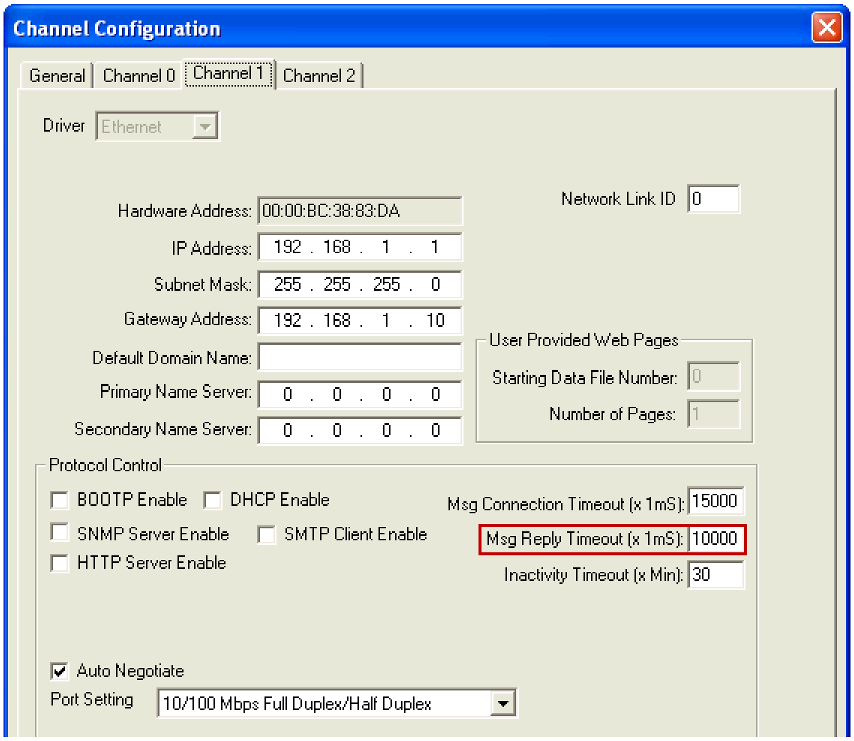
It is recommended to setup the ladder write message rungs not to start up simultaneously. Write messages should be setup to open the TCP connection sequentially. For more information it may be required to contact your PLC provider or Allen-Bradley or Rockwell Automation support.

PLC Sends Too Many “CIP Forward Open” and “CIP Forward Close” Messages

After the TCP connection is first established, then the CIP Forward Open command is sent to open the CIP connection. If there is always communication activity over that connection within eight times the Message Apply timeout of channel 1, there will be no more CIP Forward Close commands sent (this results in fewer messages sent over the air, which is good).

Often the Channel 1 Message Reply timeout is set to 3000 milliseconds. This would generate additional CIP Forward Open and CIP Forward Close messages on-air if the polling interval exceeds 3 sec × 8 = 24 seconds.

Figure 97 – Typical PLC Setup Channel Configuration Parameters



Channel Configuration

General | Channel 0 | Channel 1 | Channel 2

Driver: Ethernet

Hardware Address: 00:00:BC:38:83:DA

IP Address: 192 . 168 . 1 . 1

Subnet Mask: 255 . 255 . 255 . 0

Gateway Address: 192 . 168 . 1 . 10

Default Domain Name:

Primary Name Server: 0 . 0 . 0 . 0

Secondary Name Server: 0 . 0 . 0 . 0

Network Link ID: 0

User Provided Web Pages

Starting Data File Number: 0

Number of Pages: 1

Protocol Control

□ BOOTP Enable □ DHCP Enable

□ SNMP Server Enable □ SMTP Client Enable

□ HTTP Server Enable

Msg Connection Timeout (x 1mS): 15000

Msg Reply Timeout (x 1mS): 10000

Inactivity Timeout (x Min): 30

☑ Auto Negotiate

Port Setting: 10/100 Mbps Full Duplex/Half Duplex

When the polling interval is longer, CIP Forward Open and CIP Forward Close messages add 4 extra messages on-air between each unit polled. In each poll is 2 messages (message and reply), therefore the 4 extra messages increase the on-air message load by 200 %.

For example, a system is set up for the PLC to poll the remote PLCs every 120 seconds and is set to wait for the next poll loop if polling is not completed after the 120 seconds, therefore the loop becomes 240 seconds.

Take the 240 seconds and divide it by 8, which gives 30 seconds. Set the Message Reply timeout on Channel 1 to 30000 milliseconds — or 32000 ms is some margin is required.

More about Message Reply Timeout

The Message Reply timeout is also used for retransmission of messages in case there is no reply. Since TCP connection is used, the retransmissions are normally not required. Therefore, with TCP longer timeouts within reason are okay.

The Message Reply timeout on Channel 1 settings of the PLC should be set to the value determined by the previous example and since traffic is on-air and is retried, and the TCP driver performs its own retries, then:

Msg Reply Timeout minimum = 10000 msec.

Msg Reply Timeout maximum = based on value determined by the above example.

With future releases of PLC software and firmware, the described operation could change. It is always recommended to be informed on PLC release changes from your PLC provider or manufacturer or Allen-Bradley or Rockwell Automation support.

PLC Sends Many TCP/IP Keep-Alive Messages

This has been seen on the MicroLogix 1100 and 1400 and on the SLC 5.

The PLC sends many IP keep-alive messages that are sent on-air. When several PLCs do the same, it is possible that a good part of the on-air bandwidth is used up by the keep-alive traffic.

We recommend that the Viper be configured in router mode and that the TCP Proxy is enabled. The Viper TCP Proxy feature will filter-out the TCP/IP keep-alive messages.

It has been recommended to Allen-Bradley and Rockwell Automation to have an option in the PLC settings to disable keep-alive and have user-selectable keep-alive intervals. This could potentially become available in future releases of PLC firmware.

PLC Reopens TCP/IP Connection with the Same Source Port

This has been seen on the MicroLogix 1100 and 1400 and on the SLC 5.

When the PLC is restarted, it uses the same TCP/IP connection source port previously used.

Note: The SLC 5 also uses the same source port for each new connection without PLC restart.

Earlier Viper firmware, when in Router mode and having TCP Proxy enabled, did not allow the new TCP connection to go through immediately if the same TCP source port was used and if the PLC did not terminate the old connection. After the old TCP Proxy connection timeout, the new connections are okay.

Starting with Viper firmware v1.10 and Viper SC firmware v3.2 (and continuing forward with Viper SC+) a new enhancement was added to allow new connection created when using the same source port.

It has been recommended to Allen-Bradley and Rockwell Automation to have the TCP source port randomized when the unit is restarted. This could potentially become available in future releases of PLC firmware.

PLC Detecting Communication Failure While Viper TCP/IP Filters Keep-Alives

The PLC should not reopen a new connection while the connection for the same remote PLC is still in progress.

This has been seen on MicroLogix 1100 and 1400.

When the MicroLogix PLC sends messages but does not receive response messages, it will keep the TCP connection open forever if the Viper ACKs the keep-alives. Even if the PLC application reports communication loss at the PLC application level, the PLC will not open a new connection. This is often a result after having communication issues with remotes.

New firmware is available from Allen-Bradley for the MicroLogix 1100 and 1400.

Allen-Bradley MicroLogix firmware overview at the time of writing this document

For website downloads:
http://www.ab.com/linked/programmablecontrol/plc/micrologix/downloads.html

MicroLogix 1100 series B (FRN 4 and above are Series B)**:**
MicroLogix 1100 series B before FRN 10 require to be upgraded to FRN 10 (released).

MicroLogix 1400 series A:
MicroLogix 1400 series A before FRN 6 require to be upgraded to FRN 6 or 7 (released).

MicroLogix 1400 series B:

MicroLogix 1400 series B before FRN 11 require to be upgraded to FRN 11 (released).

For other MicroLogix models, please contact Rockwell Automation Technical Support.

ALLEN-BRADLEY CONTROLLOGIX AND COMPACTLOGICS PLC FOR VIPER SYSTEM

This guide is intended to assist with Allen-Bradley CompactLogix and ControlLogix communication setup between master PLC and remote PLC using AB Ethernet/IP TCP protocol between PLCs.

PLC communication via serial lines or serial terminal server is not covered here, nevertheless some information may be applicable.

Note: Please consult the Viper General PLC setup, earlier in this appendix for important information about setting up systems with PLCs.

ALLEN BRADLEY COMPACTLOGIX AND CONTROLLOGIX PLCS

Following are important settings recommended to improve communications when used with a limited bandwidth Viper network. This provides more specific information that supplements the general PLC communication information presented earlier in this appendix.

Note: When required, contact your PLC provider or Allen-Bradley or Rockwell Automation support.

PLC Ladder Logic on Restart Opens All Connections at Once Instead of Sequentially

When the PLC ladder program is set up to have at startup all write message rungs set to true, all TCP connections are triggered “simultaneously.” This creates an overload of TCP SYNs and somewhat could congest the on-air traffic depending on the system.

It is recommended to setup the ladder write message rungs not to start up simultaneously. Write messages should be setup to open the TCP connection sequentially. For more information it may be required to contact your PLC provider or Allen-Bradley or Rockwell Automation support.

Allen-Bradley CompactLogix and ControlLogix Series PLCs Ethernet IP Connection Timeout
(Setting Timeout Too Short Can Cause Problems!)

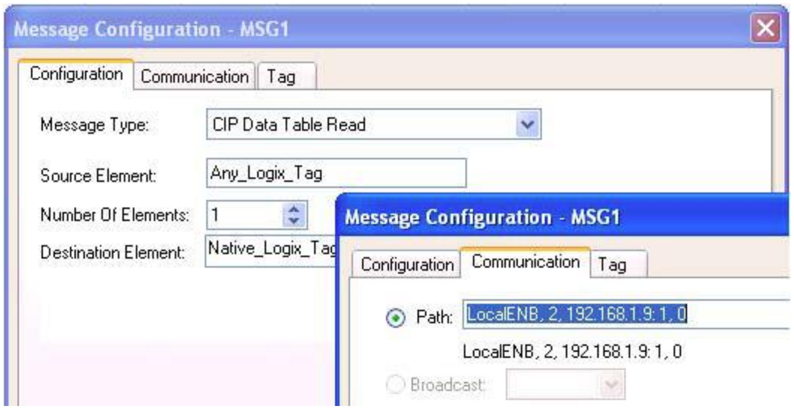
When using the Ethernet IP with Allen-Bradley CompactLogix or ControlLogix (Logix series), the TCP Connection timeout is set on a per-message instruction basis using Message Configuration rather than Channel Configuration – Channel 1 of the MicroLogix series that was shown in the previous section.

When messages are defined using Message Configuration and using path, for example, LocalENB,2,192.168.1.9:1,0, in this example:

- TCP connection is opened when the first message is sent.
- The TCP connection timeout is set by default to 120 seconds since the inactivity default setting is 120 seconds.
- While connection is established with the same remote IP and same port (in this example, 192.168.1.9) other messages will use the same TCP connection and therefore resetting the timeout count for each message sent.
- When all messages are using the same default inactivity time (120 seconds) the TCP connection stays open if the next message is sent within the inactivity timeout period.
- The TCP connection is closed after the last message plus the inactivity period (default 120 seconds).
- The TCP connection can also be terminated based on network connection problems.

The message configuration for this example will look like the following figure.

Figure 98 – Message Configuration » Configuration and » Communication tabs in PLC setup utility



Message Type: CIP Data Table Read

Source Element: Any_Logix_Tag

Number Of Elements: 1

Destination Element: Native_Logix_Tag

● Path: LocalENB, 2, 192.168.1.9: 1, 0

LocalENB, 2, 192.168.1.9: 1, 0

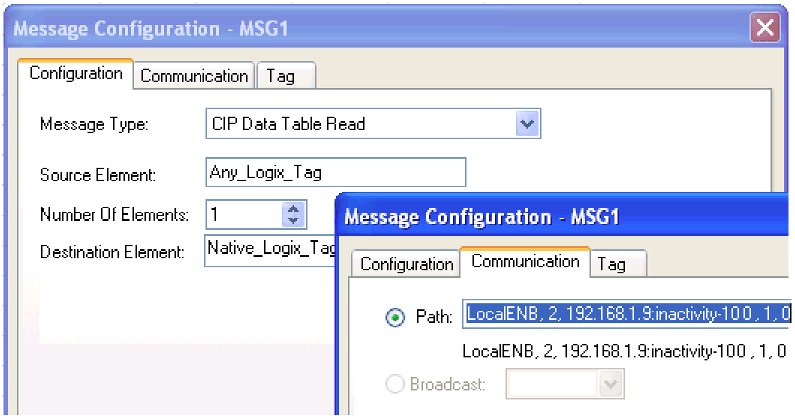
○ Broadcast:

Overriding the Default Inactivity Timeout —Not Recommended Unless Required

Overriding the default inactivity timeout for the TCP connection in the Message Configuration is not recommended unless it is required. But here are instructions how it would be done if required.

It is possible to override the Message Configuration default inactivity timeout by adding to the path, for example, LocalENB,2,192.1.9: inactivity-100,1,0. Using inactivity-100 would set the inactivity timeout to 100 seconds instead of the default 120 seconds. (Note: Setting of inactivity-x, where x can be between 1 and 120 seconds. Using x > 120 seconds will disable the message completely.)

Figure 99 – Setting Example Using Custom Inactivity Timeout (100 seconds)



Message Type: CIP Data Table Read

Source Element: Any_Logix_Tag

Number Of Elements: 1

Destination Element: Native_Logix_Tag

● Path: LocalENB, 2, 192.168.1.9:inactivity-100 , 1, 0

LocalENB, 2, 192.168.1.9:inactivity-100 , 1, 0

○ Broadcast:

Overriding the default inactivity timeout is normally not required and can cause additional undesired side-effects. One of these side-effects would be when the inactivity timeout is less than the longest delay between two messages; additional IP messages are sent for each close and reopen of the TCP connection. This adds a lot of on-air traffic and negatively impacts the system performance.

Note: When using different inactivity timeout values for messages with the same TCP connection:
When different messages for the same remote share the same TCP connection, each different message's inactivity timeout would restart the timeout timer. Message example: msg1 inactivity-60, msg2 inactivity-100, msg3 inactivity-30. These messages are then sent as follows: msg1 is sent, msg2 is sent, msg3 and then a wait is done. Since the last message was msg3 with inactivity timeout of 30 seconds, the TCP connection would close after 30 seconds of msg3.

Summary on TCP Connection Timeout (Inactivity Setting)

Since the longest inactivity timeout per TCP connection with a remote unit (PLC/RTU) is 120 seconds (based on message inactivity for maximum of 120 seconds), it is important that each remote (PLC/RTU) is polled with the 120 second period to avoid extra traffic resulting from additional TCP/IP open and close connection messages. For systems where polling is done infrequently (> 120 seconds), the additional TCP traffic needs to be considered for the system traffic plan.

For normal operation, the inactivity timeout does not need to be specified in the Path setting. Master and remotes should be set this way, especially if remote PLCs send unsolicited messages or initiate communication with other remotes. If a system has a mix of PLCs (CompactLogix or ControlLogix with MicroLogix or SLC), then also refer to information earlier in this appendix regarding the Allen-Bradley Micrologix 1100 or 1400 (may also apply to SLC 5) and information, which precedes it.

ALLEN-BRADLEY COMPACTLOGIX OR CONTROLLOGIX SERIES PLCS SENDS TOO MANY CIP FORWARD OPEN AND CIP FORWARD CLOSE

When using the Ethernet/IP with CIP communications protocol with Allen-Bradley CompactLogix or ControlLogix PLCs (and with other Logix series PLCs), the option to use Connected or Unconnected is available in the Message Configuration. By default, the Connected checkbox is selected and therefore it will add additional messages (CIP Forward Open and CIP Forward Close) for each read-write operation when the next message is sent outside the message timeout period. The default setting is 30 seconds.

To lower the on-air traffic, the Connected checkbox should be unchecked (Unconnected).

Connected or Unconnected operation description for CIP

When the Connected checkbox is checked (Connected), if there is not a CIP connection already established, then the controller sends an Open Forward CIP Connection command and waits for the good response before transmitting the read or write command. The CIP connection remains open if there is activity before the timeout (default = 30 seconds). Any message instruction sending commands to the same device can use the same CIP and TCP connection. If this timeout is reached, a close CIP connection is sent.

When the Connected checkbox is unchecked (Unconnected), the controller uses the Unconnected CIP service to transmit the read or write command so there is less overhead.

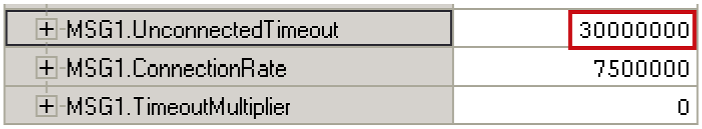
The **Connection timeout** is on a per-message instruction basis as shown below – this is with regards to the CIP connection, which is only controlled by the Inactivity timeout.

Table 19 Mnemonics and Data Types with Description for Allen-Bradley -Logix PLCs

Mnemonic	Data Type	Description	
Unconnected Timeout	□INT	Timeout for an unconnected message or for making a connection. The default value is 30 seconds.	
		If the message is	**Then**
		Unconnected	The ER bit turns on if the controller does not receive a response within the Unconnected Timeout time.
		Connected	The ER bit turns on if the controller does not get a response for making the connection within the Unconnected Timeout time.
Connection Rate	□INT	Timeout for a connected message once it has a connection. This timeout is for the response from the other device about the sending of the data.	
Timeout Multiplier	□ INT		
		• This timeout applies only after the connection is made. • The timeout = Connection Rate × Timeout Multiplier. • The default Connection Rate is 7.5 seconds. • The default Timeout Multiplier is 0 (which is a multiplication factor of 4). • The default timeout for connected messages is 30 seconds (7.5 seconds× 4 = 30 seconds). • To change the timeout, change the Connection Rate and leave the Timeout Multiplier at the default value.	

For the Logix controllers, the Unconnected Timeout must be individually adjusted in each message instruction tag. The default is 30,000,000 microseconds (µsec or µs), or 30 seconds.

Figure 100 – MSG1 Unconnected Timeout, Connection Rate, and Timeout Multiplier



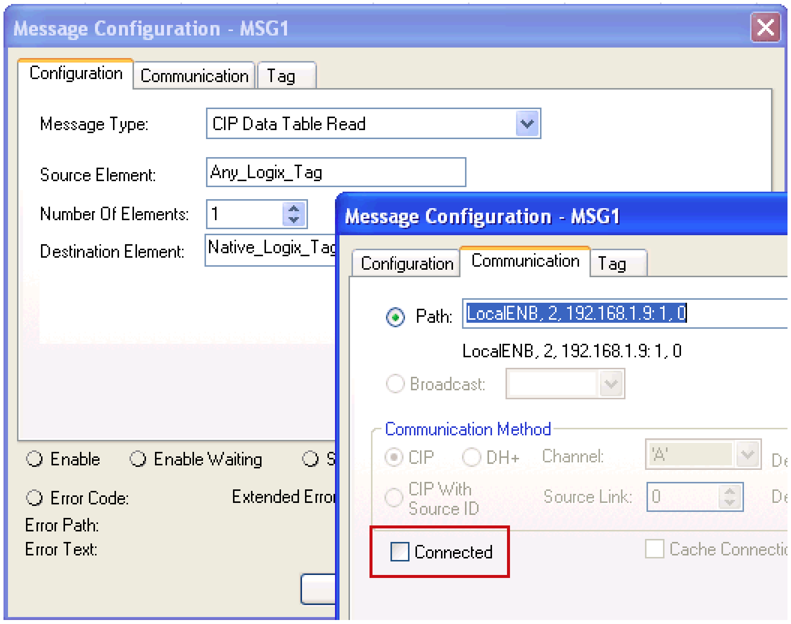
⊞ MSG1.UnconnectedTimeout	30000000
⊞ MSG1.ConnectionRate	7500000
⊞ MSG1.TimeoutMultiplier	0

When Communication Is Between ControlLogix or CompactLogix And Other –Logix Series PLCs

To lower the on-air traffic, uncheck Connected in the Message Configuration » Communication tab in the PLC setup.

The following figure shows an example when the Message Type is CIP Data Table Read or CIP Data Table Write. Note that the Connected checkbox should be unchecked. This is because if you leave it checked, then every time the MSG instruction is executed, a CIP connection (with CIP Open message) will be established and broken (with CIP close message) which adds unnecessarily to the network traffic.

Figure 101 – Message Configuration » Communication, showing Connected checkbox unchecked



Message Configuration - MSG1

Message Type: CIP Data Table Read

Source Element: Any_Logix_Tag

Number Of Elements: 1

Destination Element: Native_Logix_Tag

Message Configuration - MSG1

● Path: LocalENB, 2, 192.168.1.9: 1, 0

LocalENB, 2, 192.168.1.9: 1, 0

○ Broadcast:

Communication Method

● CIP ○ DH+ Channel: 'A'

○ CIP With Source ID Source Link: 0

□ Connected

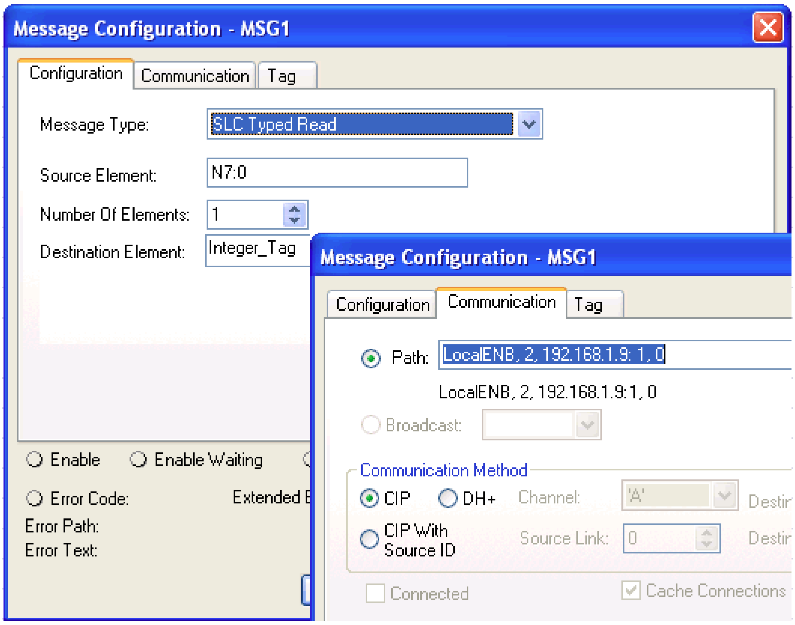
□ Cache Connecti

When Communication Is Between ControlLogix or CompactLogix and other –Logix Series PLCs.

These PLCs/Controllers usually use Ethernet/IP CIP unconnected protocol to communicate with each other.

Note (see the following figure) that when the Message Type is SLC Typed Read or SLC Typed Write, the Logix MSG instruction always uses an Unconnected CIP (notice that the Connected checkbox is grayed out). For example, this is used when using PCCC encapsulated in Ethernet/IP command. Others than read or write for SLC

Figure 102 – Message Configuration » Communication, showing CIP selected and Connected Checkbox Unavailable



Message Configuration - MSG1

Message Type: SLC Typed Read

Source Element: N7:0

Number Of Elements: 1

Destination Element: Integer_Tag

Message Configuration - MSG1

● Path: LocalENB, 2, 192.168.1.9: 1, 0

LocalENB, 2, 192.168.1.9:1, 0

○ Broadcast:

Communication Method

● CIP ○ DH+ Channel: 'A' Destir

○ CIP With Source ID Source Link: 0 Destir

□ Connected

☑ Cache Connections

Summary of Connected or Unconnected Operation

With the Connected option selected and polling interval between messages for the same remote CIP connection is longer than the Unconnected Timeout (default 30 seconds), CIP Forward Open and CIP Forward Close messages add 4 extra on-air messages (includes message reply) for each unit polled. **If each poll is 2 messages (message and reply), the 4 extra messages increase the message load (on air) by 200 %**.

Therefore, the **Connected checkbox should be unchecked (Unconnected)** to avoid sending CIP Forward Open and CIP Forward Close messages. If connected is required, then increase the Unconnected Timeout and Connection Rate timeout to a value greater than the polling interval per remote (use precaution with this).

Timeouts used for message responses over Ethernet /IP Connected or Unconnected should not be too short, and therefore should not be set shorter than 15 seconds (normally) in the event it is required to be lower than 30 seconds for application-level retransmission. The TCP/IP communication driver does its own retransmissions and will not require application retransmissions of messages since a TCP connection will not lose a message unless the connection terminates normally or due to a problem. Therefore, with TCP longer timeouts within reason are okay. Longer timeouts (for example, 30 seconds) are okay since they minimize duplicated messages being buffered by TCP in the event of network congestion or communication problems with the remote unit.

With future releases of PLC software and firmware, the described operation could change. It is always recommended to be informed on PLC release changes from your PLC provider or manufacturer or Allen-Bradley or Rockwell Automation support.

ALLEN-BRADLEY COMPACTLOGIX OR CONTROLLOGIX SERIES PLCS SEND MANY TCP/IP KEEP-ALIVE MESSAGES

The CompactLogix and ControlLogix series PLCs send TCP/IP keep-alive messages every 8 seconds in both directions for each TCP connection. When several PLCs do the same, it is possible that a good part of the on-air bandwidth is used up by the keep-alive traffic.

We recommend that the Viper be configured in router mode and that the TCP Proxy is enabled. The Viper TCP Proxy feature will filter-out the TCP/IP keep-alive messages.

The PLCs TCP keep-alive cannot be disabled nor adjusted. It has been recommended to Allen-Bradley and Rockwell Automation to have an option in the PLC settings to disable keep-alive and have user-selectable keep-alive intervals. This could potentially become available in future releases of PLC firmware.

Also please refer to , earlier in this appendix.

APPENDIX K – SERVICE AND SUPPORT AND WARRANTY STATEMENT

Product Warranty, RMA, and Contact Information

NextGen RF guarantees that every Viper SC+™ IP router will be free from physical defects in material and workmanship for one (1) year from the date of purchase when used within the limits set forth in the specifications section of this manual.

The manufacturer's Warranty Statement is available on the following page. If the product proves defective during the warranty period, contact NextGen RF Customer Service to obtain a Return Material Authorization (RMA).

RMA Request/Contact Customer Service

NextGen RF
2130 Howard Drive W
North Mankato, MN 56003
507.514.6246

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

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

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

Product Documentation

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

Tech Support

NextGen RF
2130 Howard Drive W
North Mankato, MN 56003
E-mail: support@NextGenRF.com

Phone: 1-507-514-6245

WARRANTY STATEMENT

NextGen RF warrants to the original purchaser for use ("Buyer") that data telemetry products manufactured by NextGen RF ("Products") are free from defects in material and workmanship and will conform to published technical specifications for a period of, except as noted below, one (1) year from the date of shipment to Buyer. NextGen RF makes no warranty with respect to any equipment not manufactured by NextGen RF, and any such equipment shall carry the original equipment manufacturer's warranty only. NextGen RF 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 NextGen RF. NextGen RF, 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 NextGen RF. 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 NextGen RF or authorized service agent. NextGen RF 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 all warranty obligations on the part of NextGen RF.

This warranty is void and NextGen RF 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 NextGen RF 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 NextGen RF or authorized service agent of the defect during the applicable warranty period. NextGen RF 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. NEXTGEN RF AND BUYER AGREE THAT BUYER'S EXCLUSIVE REMEDY FOR ANY BREACH OF ANY OF SAID WARRANTIES IT AS SET FORTH ABOVE. BUYER AGREES THAT IN NO EVENT SHALL NEXTGEN RF 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 NextGen RF 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

NextGen
— RF DESIGN —

ABOUT NEXTGEN RF

NextGen RF is a USA owned and operated engineering services company providing valuable wireless design expertise on a variety of products, ranging from design consultation to fully turnkey product development. Because we know design, NextGen RF has become the chosen partner for companies worldwide who require a high level of design expertise and responsiveness for their product development. We understand the difficulties of implementing RF solutions in designs and have a proven track record of helping clients efficiently meet their design objectives and requirements. We focus on process-oriented engineering from discovery and idea generation, definition of product requirements and specifications to design, verification and ultimately factory introduction. For more information visit www.nextgenrf.com