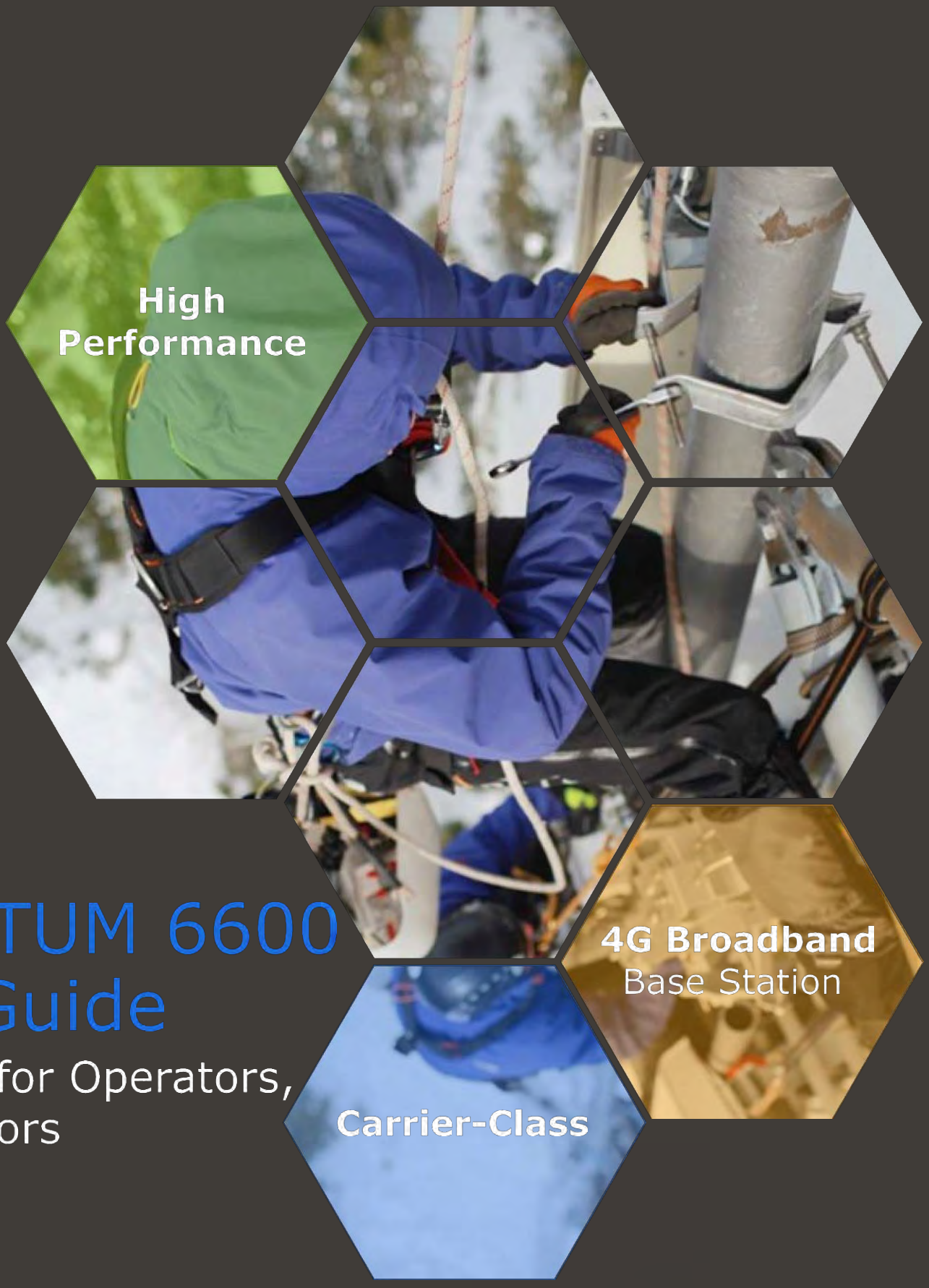


QUANTUM 6600 User Guide

Designed for Operators, by Operators

MERCURY networks

Table of Contents

Symbols used in this document

Notes, cautions, and timesavers use these conventions and symbols:

	Tip	A tip will help you to solve a problem. A tip might not be troubleshooting or even an action, but could be useful information.
	Note	Notes contain helpful suggestions or references to materials not contained in this manual.
	Caution	Be careful. In Caution situations, you might do something that could result equipment damage or loss of data.
	Warning	A warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.

Regulatory Notice

This device complies with the FCC limits a class B digital device, pursuant to Part 15 of the FCC Rules. A complete list of regulatory certifications can be provided by Mercury Networks upon request. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Re-orient or relocate the receiving antenna(s).
- Increase the separation between the equipment and other receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio frequency technician/engineer for help.

Shielded cables and I/O cords must be used for this equipment to comply with the relevant FCC regulations.

Changes or modifications not expressly approved by Mercury Networks, LLC. may void the user's authority to operate this equipment.

The 2.3, 3.3, and 3.5 GHz products have the CE (European Conformity) Mark.

	Note: This device must be professionally installed, and the operator and/or the licensed spectrum holder have the responsibility to comply with FCC regulations.
	Note: This device must be professionally installed, and the operator and/or the licensed spectrum holder have the responsibility to comply with FCC regulations.
	Note: The contention protocol MUST be turned on and used for the specified band (3.65GHz - 3.7 GHz) in the specified country or wherever FCC rules and regulations are enforced. Failure to comply makes the operation of this device illegal.

Safety Precautions

When operating or installing this equipment, please observe the following precautions to minimize the risk of danger or personnel injury:

	NEVER install equipment if there is a chance of lightning or other adverse weather conditions.
	NEVER install equipment in a wet location unless the equipment is specifically design for wet locations.
	NEVER touch un-insulated wires or terminals unless the wire has been disconnected from any equipment.
	ALWAYS use caution when installing or modifying cables.
	ALWAYS disconnect all lines and power connections before servicing or disassembling this equipment.
	ALWAYS assume that all components and assemblies are static sensitive and always follow local ESD-prevention guidelines to prevent equipment damage.
	For any external power supply that provides the power source for the Mercury Networks equipment, replace any power supply fuse with the same rating or equivalent; otherwise Mercury Networks cannot not be responsible for any subsequent damage to the equipment.

	For performance and safety reasons, only power supplies listed for use with telephone equipment by a Nationally Recognized Testing Laboratory (NRTL) should be used with equipment.
	ALL wiring external to the product(s) should follow the provisions of the current edition of the National Electrical Code.
	These units contain no user serviceable components. Only authorized service personnel should service or repair these units. Use only isolated Class 2 Power Source, Rated 48VDC, 5.0A Minimum.

1. Preface

1.1 About This Document

The purpose of this User Guide is to quickly familiarize the user with the Mercury Networks Quantum 6000 family of Base stations, their initial setup, and provisioning. It is not intended to be a comprehensive reference for the product and all its capabilities, nor does it cover in depth provisioning, operation, or administration using the PureView Network Management System or the Mercury Networks Quantum command line interface. Please refer to their respective user guides for more in-depth coverage of those tools.

Please also note that this guide does not cover the physical installation of the product, but rather assumes that the Base Station has been fully installed and is ready to be powered on. Please refer to the Mercury Networks Quantum 6600 Installation Guide for detailed professional installation guidelines.

Always refer to the current set of Release Notes for the most up to date information and a description of the current features as they relate to the Mercury Networks system. These may be different from and supersede the information contained within this “Installation Guide”.

1.2 Locating the Product Serial Number

The product identification information, serial number, and certification information are located on a label on the side panel of the Base station. Please take note of and keep this information for your records, as it is very important for warranty and support services.

1.3 Obtaining Documentation and Support

All requests for documentation and/or support should be addressed to:

Mercury Networks, LLC.
1100 Walnut St, Suite 2050
Kansas City, Missouri 64105
E-mail: support@mercurynets.com
Tel: (888) 909-6717
Fax: (408) 827-9124

2. Mercury Quantum Base Station Overview

2.1 Introduction – What is a Compact Base Station

At Mercury, we believe that true broadband data networks must roll out in a completely different manner than the traditional, low-throughput cellular networks of yesterday. The traditional cellular network paradigm of colossal "macro" Base stations and large cell radii developed from the need for high-coverage networks to carry low-bandwidth voice and messaging traffic. However, as the demand for data-based applications has grown, networks have quickly become congested, necessitating new wireless standards designed specifically for high-speed broadband data. Furthermore, as spectrum is always a scarce and expensive resource, the need for improved frequency re-use techniques has become more important than ever.

The clear solution to this is higher-efficiency wireless standards, such as IEEE 802.16e Mobile WiMAX, and more flexible cell sizes. Where medium and high population density exists, cell sizes should be small to enable increased spectral re-use, thereby ensuring that each subscriber enjoys a sufficient amount of throughput. In such cases it may be necessary to deploy Base stations on utility poles, flag poles, rooftops, small buildings and walls. This necessitates small, pleasant form-factor Base stations that can accept a variety of antenna types, both omni-directional and directional. Such Base stations are often referred to as "Pico". Because wired backhaul may not always be available in some such locations, it also suggests the need for wireless backhaul options.

On the other hand, in rural areas with lower population densities, it makes more economic sense to deploy fewer Base stations on higher towers or buildings and usually with higher transmit power. This is closer to the traditional cellular approach and typically involves large, expensive and power-hungry "macro" or "micro" Base stations, often with split designs requiring both indoor and tower-top electronics. Wherever indoor components are required an operator must obtain an air-conditioned shelter, which adds significantly to the continual operating expenditures of such a deployment and limits the deployment location.

Mercury has taken a revolutionary approach in the development of exclusively "Compact"
Base stations. A compact Base station shares the similar form-factor and cost of a Pico Base station, but with the performance of a Macro Base station. It is a zero-footprint device that can be fully co-located with its antennas. It is the best of all worlds and can be flexibly deployed in Pico, Macro, and Micro type deployments.

Welcome to the Revolution!

2.2 Mercury Quantum 6600 at a Glance

The Quantum 6600 is Mercury's 3rd generation Base station and is part of the Mercury X4G ecosystem. Built on a 6x6 design, the Quantum 6600 was made for non-line-of-sight and can handle the toughest of environments. The 6600 is quite simply the highest performing, most advanced carrier-grade Base station in the market.

This User's Guide covers the Mercury Quantum 6600 products, with models differentiated by only the frequency variant which is represented by the two right digits. For example, the Mercury Quantum 6625 is the 2.5GHz variant, supported 2.5-2.7GHz. Otherwise they are functionally identical. In this guide we will, without loss of generality, refer primarily to the Mercury Quantum 6600 product, which is

synonymous to writing Mercury Quantum 66xx. Please note that not all Quantum models are available in all markets. Please contact your sales representative for additional information and ordering options.

The Mercury Quantum Family of Base station products is fully 802.16e (Mobile WiMAX) compliant and designed to interoperate seamlessly with standard, off-the-shelf, WiMAX certified subscriber devices. All Mercury Quantum products feature a software-defined radio (SDR) architecture that allows them to continuously evolve and take on new features as they become available. Some of the key highlights of the Mercury Quantum 6600 include the following:

- **Superior Range** – An antenna array of 6 antennas operated in concert creates tightly focused radio beams that extend the range of each Base station by up to 40% or boost capacity where required.
- **Spectral Re-use** – Sophisticated interference mitigation techniques coupled with advanced beamforming technology, both made possible by Mercury's multiple antenna architecture, allow for simple network deployments and for improved spectral re-use.
- **Software Defined Radio** – Protects your investment through support for over-the-air, field upgrades of existing networks as standards evolve and new features and capabilities are released.
- **Completely Weatherproof** – Mercury Quantum Base stations do not require shelter and can be installed completely outdoors. This eliminates the capital cost of building a shelter and the recurring cost of leasing or running an airconditioned site.
- **Flexibly Mount Virtually Anywhere** – Mercury Quantum Base stations can be deployed on towers, utility poles, walls, rooftops, etc, without the need for remote RF heads.
- **ASN-GW Optional** – Mercury Quantum Base stations can operate with or without an ASN-GW, making even small deployments affordable.

Mercury Quantum Base stations can utilize virtually any off the shelf antennas, both omnidirectional and sectored. However, Mercury recommends our own line of affordable, compact, multi-antenna panels designed specifically to complement the performance of our Base stations.

Mercury Quantum Base Stations can be installed indoors or outdoors, however the antennas must always be installed outdoors. Figure 1 shows a Mercury Quantum 6600 Base station co-located on a tower with a Mercury 6-Port Antenna Panel.

Mercury's carrier-grade solution includes the full-featured and highly scalable PureView NMS (Network Management System), which can efficiently and powerfully provision and manage all Base station and Subscriber Stations in the access network. PureView features include automatic discovery, fault management, inventory tables, configuration, and performance management. PureView utilizes full open standard SNMP on the access network side, and employs a full-featured northbound interface for connection to virtually any existing NMS.

Figure 1 Mercury Quantum 6600 Base Station Mounted on Tower

In addition to the PureView NMS, all Mercury Quantum Base Stations support a fullfeatured Command Line Interface (CLI) and an integrated Web Interface. Please refer to the PureView NMS User Guide and the CLI User Guide for in depth coverage of those applications.

2.3 A Closer Look

The Mercury Quantum 6600 Base Station is a single, weather-resistant enclosure with overall dimensions 17.5” x 16.7” x 5.3” (44cm x 42cm x 13cm). The Base station is a single self-contained unit.

⚠	Note that the Mercury Quantum 6600 Base Station has no user serviceable components.

Mercury Quantum products employ a sophisticated and flexible hardware architecture that combines general-purpose processors, and application-specific hardware. Together these components deliver the processing power required to realize the high-performance required by today’s demanding applications, while yielding the flexibility to support future functionality as needs arise.

2.3.1 Ports and Indicators

The Mercury Quantum 6600 connector panel is shown in Figure 2. The product’s flexible architecture allows for a number of product variants to suite almost limitless deployment needs. The model shown includes six antenna ports, two CAT-5 Gigabit Ethernet backhaul ports, and a DC power connector. Single or Multi-Mode Fiber backhaul are also available. As the configuration of individual Base station models varies, so will the appearance of the connector panel. All Mercury Quantum Base stations include a serial (RS-232) console port, a GPS antenna connector, a ground terminal, and three high-intensity LEDs.

Figure 2 Mercury Quantum 6600 Base Station

⚠	Note that a professional installer must complete the installation and weatherproofing. Please refer to the Mercury Quantum 6600 Base Station Installation Guide for detailed instructions.

The function of each Base station connector/port is described in Table 1. Note that every connector present must be terminated to ensure proper Base station operation. Please refer to the Mercury Quantum 6600 Installation Guide for comprehensive installation procedures.

Connector	Function
Power	-48VDC power source inputs for the unit. DC power connector: LTW BB-04PMMS-LC7001 (chassis), LTW BB-04BFFA-LL7001 (mate)
GPS	N-type female connector for mandatory external GPS antenna. 3.3V power on center pin.
ETH-1	This Gigabit Ethernet port serves as the data traffic backhaul Interface and also provides for in-band management of the Base Station. Available port options are Cat-5 (RJ-45), Single-Mode Fiber (HartingPull/Han 3 A), and Multi-Mode (LC duplex) Fiber.
ETH-2	This Gigabit Ethernet port may be used for out-of-band management of the Base Station. It may also be used to connect to an external device, such as a web camera. Available port options are Cat-5 (RJ45), Single-Mode Fiber (HartingPull/Han 3 A), and Multi-Mode (LC duplex) Fiber.
Console	RJ-45 based RS-232 port for CLI control via a console. Defaults settings are 38400, 8 data bits, 1 stop bit, no parity bits, no flow control.
ANT 1-6	N-type Tx / Rx Antenna Ports.

Table 1 Base Station Connector Description

LED	Function
Status	Green - BS is up and running normally. No faults detected. Blinking Red – System booting up, or system is temporarily down. Solid Red - Fault detected. Off – LEDs disabled or Power is off. Fault detected if POWER LED is Green, but STATUS LED is Off.
Link	(Status LED for ETH-1 Gigabit Ethernet Port) Solid Green – Connected to an Ethernet switch. Blinking Green – Ethernet packet activity. Off – LEDs disabled or no Ethernet activity detected.
Power	Green – Power is being supplied to the BS. Off – LEDs disabled or no power is being supplied to the BS.

Table 2 Base Station LED Description

The Base Station's three high-intensity LEDs are intended to be viewable from the ground for quick confirmation of the unit's operational state. Table 2 describes the function of each indicator. Note

that the LEDs can be turned off by the operator using the PureView NMS, the Web Interface, or the Base Station's command-line interface.

2.3.2 Radio and Physical Layer Specifications

The Mercury Quantum Family of Base Stations is available in several models to support a variety of frequency bands and the regulatory requirements of a number of countries. Because several deployment-specific variables (e.g., antenna type, cable type and length, settings, etc) can affect the effective power output and other characteristics of the system, it is the customer's responsibility to assure that each deployment of this product meets applicable regulations. The PureView NMS, the Web UI, and the CLI all provide guidelines and feedback to ensure an appropriate installation.

Table 3 lists key radio-related specifications of Mercury Quantum Base Stations. Note that additional features, not listed, may be released in future software revisions.

Parameter	Specification
Frequency Bands	6623: 2.30-2.40 GHz 6625: 2.50-2.70 GHz 6633: 3.30-3.40 GHz 6635: 3.40-3.60 GHz 6635-IC: 3.45-3.65 GHz 6636: 3.65-3.70 GHz
Channel Sizes	3.5 MHz 5 MHz 7 MHz 10 MHz
Duplex Method	TDD
DL:UL Ratios	35:12, 29:18, 32:15, 26:21 (5 MHz and 10 MHz) 23:9, 21:12, 17:15 (3.5 MHz and 7 MHz)
Number of Tx/Rx Antennas	6 Tx, 6 Rx
Tx Power per Antenna	33dBm (RMS data power at maximum MCS level, measured at each external antenna connector of the Base Station)
Permutation	PUSC
Modulation Rates	QPSK-1/2, QPSK-3/4 16QAM-1/2, 16QAM-3/4 64QAM-1/2, 64QAM-2/3, 64QAM-3/4, 64QAM-5/6
Data Repetition Coding	QPSK-1/2 Repetition 2, 4, 6
MAP Repetition	1, 2

Smart Antenna Capabilities	Beamforming, MIMO Matrix A, MIMO Matrix B, Cyclic Delay Diversity, MRC
Air Link Optimization	HARQ, CTC

Table 3 Radio and PHY Specifications

2.3.2.1 Receiver Sensitivity

Table 4 presents typical receiver sensitivity specs of the Quantum 6600 Base Station. Note that sensitivity will be correspondingly less on models with fewer than 6 antennas. Note that the values presented are measured over the entire channel bandwidth, as opposed to WiMAX Radio Conformance Test (RCT) type measurements, which are measured over only a fraction of the channel bandwidth.

Typical 6-Ant RX Sensitivity (AWGN, 106 BER, Full Band, in dBm)				
UL MCS (CTS)	**3.5 MHz**	**5 MHz**	**7 MHz**	**10 MHz**
QPSK-1/2	-107	-105	-104	-102
QPSK-3/4	-104	-102	-101	-99
QAM16-1/2	-102	-100	-99	-97
QAM16-3/4	-98	-96	-95	-93
QAM64-1/2	-97	-95	-94	-92
QAM64-2/3	-93	-91	-90	-88
QAM64-3/4	-92	-90	-89	-87
QAM64-5/6	-89	-87	-86	-84

Table 4 Typical Uplink RX Sensitivity

2.3.2.2 Computing EIRP Power

Effective Isotropic Radiated Power (EIRP) refers to the transmit power radiating out of the antenna. The accurate computation of EIRP is essential to proper network planning and to ensuring that the system meets local and regional maximum power regulations.

As indicated in Table 3, the average Tx power output at each Base Station antenna connector is 33dBm. The average EIRP per antenna is computed as follows:

Ave EIRP per Ant (in dBm) = Ave Tx Pwr per Ant + Ant Gain – Cable and Connector Loss

For example, if deployed with a 15dBi antenna connected to the Base Station with only a few feet of cable, the average EIRP per Antenna might be 33dBm + 15dBi – 1dB = 47dBm.

The total average EIRP of the Base Station with all antennas combined can then be computed as follows:

Total Ave EIRP (in dBm) = Ave EIRP per Ant + 10log (Number of Antennas)

For a 6 antenna Base Station, the example above yields Total Ave EIRP = 47dBm + 7.78dB = 54.78dBm.

Note that some regulations refer to *peak* power, which in a WiMAX system is normally as much as 10dB higher than average power. In the case of the Mercury Quantum products the peak power can be assumed to be 9dB higher than average. Therefore, Peak EIRP should be computed as follows:

Peak EIRP per Ant (in dBm) = Ave EIRP per Ant + 9dB

Total Peak EIRP (in dBm) = Total Ave EIRP + 9dB

For the above example, Peak EIRP per Ant = 46dBm + 9dB = 54dBm and Total Peak EIRP = 53.78dBm + 9dB = 62.78dBm. These equations are summarized in Table 5.

EIRP Metric	Formula
Ave EIRP per Ant (in dBm)	= Ave Tx Pwr per Ant + Ant Gain – Cable and Connector Loss
Total Ave EIRP (in dBm	= Ave EIRP per Ant + 10log(Number of Antennas)
Peak EIRP (in dBm)	= Ave EIRP per Ant + 9dB
Total Peak EIRP (in dBm)	= Total Ave EIRP + 9dB

Table 5 EIRP Calculations

Note that some regulations are specified for particular channel bandwidths and/or antenna beamwidth and in such cases the allowable power should be scaled accordingly. As with the previous calculations, each case is often unique. Although the PureView NMS provides guidance and limits where known regional regulations apply, it is ultimately the responsibility of the spectrum holder to assure that appropriate limits are set.

2.3.2.3 Smart Antenna Capabilities

Beamforming is a technique that combines and focuses signals to and from multiple antennas to improve both downlink and uplink performance. On the uplink, the Base Station combines signals received on its multiple antennas, resulting in substantial link budget gains that improve range and throughput. Maximum Ratio Combining (MRC) and **Minimum Mean-Square Error (MMSE)** are basic techniques from which more sophisticated uplink processing techniques (such as interference mitigation) are built.

On the downlink (Base Station to Subscriber Station), sophisticated digital signal processing algorithms exploit information gathered during the uplink beamforming process to concentrate the transmitted RF energy from the antenna array to the exact subscriber stations locations, improving gain, efficiency and signal to noise ratio (SNR), resulting in greater range and throughput.

MIMO Matrix A utilizes a technique called space-time coding (STC), which exploits the spatial diversity of the channel to improve downlink performance. By improving data reception, it can increase range and maximize the utilization of available sector capacity.

MIMO Matrix B utilizes a technique called spatial multiplexing (SM), in which multiple streams of data are simultaneously transmitted through multiple antennas and effectively separated by the receiving device. This technique can actually increase the spectral efficiency and, hence, the capacity of a system.

The effectiveness of MIMO relies upon the spatial diversity inherent within the channel as well as other factors, and therefore a given technique may be more appropriate for certain users or deployments.

Fortunately, Mercury Quantum Base Stations make these decisions automatically, maximizing the efficiency of your valuable spectrum.

Cyclic Delay Diversity (CDD) is a technique employed by Mercury Quantum Base stations to allow the power of multiple antennas to be combined in transmitting a single stream of data even when MIMO or beamforming cannot be supported (e.g., when transmitting the MAP).

2.3.3 Capacity and Performance Characteristics

Table 6 summarizes key upper layer and overall performance characteristics of Mercury Quantum Base Stations. Note that some features may not be currently available but are planned for future software releases. In addition, detailed throughput tables for each DL:UL ratios are presented in Appendix B.

Parameter	Specification
Maximum Number of Connected Users	200
Maximum Number of Service Flows per User	16

Peak Throughput	Aggregate: Up to 58Mbps (35:12 Ratio) DL: Up to 43Mbps (35:12 Ratio) UL: Up to 8Mbps (26:21 Ratio)
QoS	BE, UGS, eRTPs, nRTPs, RTPs
Convergence Sub-Layer	IP-CS, Eth-CS, IPv4, IPv6 Pass-Through
Security	Security AES-128, EAP-TLS, EAP-TTLS, PKMv2
Management	PureView NMS / EMS, Remote CLI, Web Interface, SNMP v2c, SNMPv3
Core Network Interface	R6 (NWG 1.2.2, NWG 1.3.1), Radius

Table 6 Performance Characteristics

2.3.4 Electro-Mechanical and Environmental Specifications

All Mercury Quantum Family Base Stations consist of a single, all-in-one, fully weatherproof unit that may be installed entirely outdoors or indoors, as dictated by each deployment. Please refer to the Mercury Quantum Base Station Installation Guide for detailed installation instructions and guidelines.

Table 7 lists the mechanical, electrical, and environmental properties of the Mercury Quantum 6600 Base Station.

Physical & Environmental	Specification
Dimensions	17.5” x 16.7” x 5.3” (44cm x 42cm x 13cm)
Weight	32lbs (14.5kg) (does not include mounting hardware)
Power	-48 VDC (150 Watts Max)
Temperature	-40C to +55C (ETSI EN 300 019-1.4 Class 4.1E)
Humidity	5-100% non-condensing
Altitude	To 10,000 ft above sea level

Surge Protection	UL497B
Lightning Protection	Min 10kA IEC 6100-4-5 (optional via external kit)
Weatherproofing	IEC IP67
Wind Loading	160Km/hr operation, 200Km/hr survival
Safety and IEC IP	EN 300 019-2-2, GR487, IEC 60529
Vibration and Dust	ETSI EN 300 019-1-4 Class 4.1E

Table 7 Environmental and Mechanical Specifications

For temperatures above +45 degrees C in direct sunlight it is necessary to deploy the Base Station with the available solar shield, shown in Figure 3. Again, details can be found in the Mercury Quantum 6600 Base Station Installation Guide.

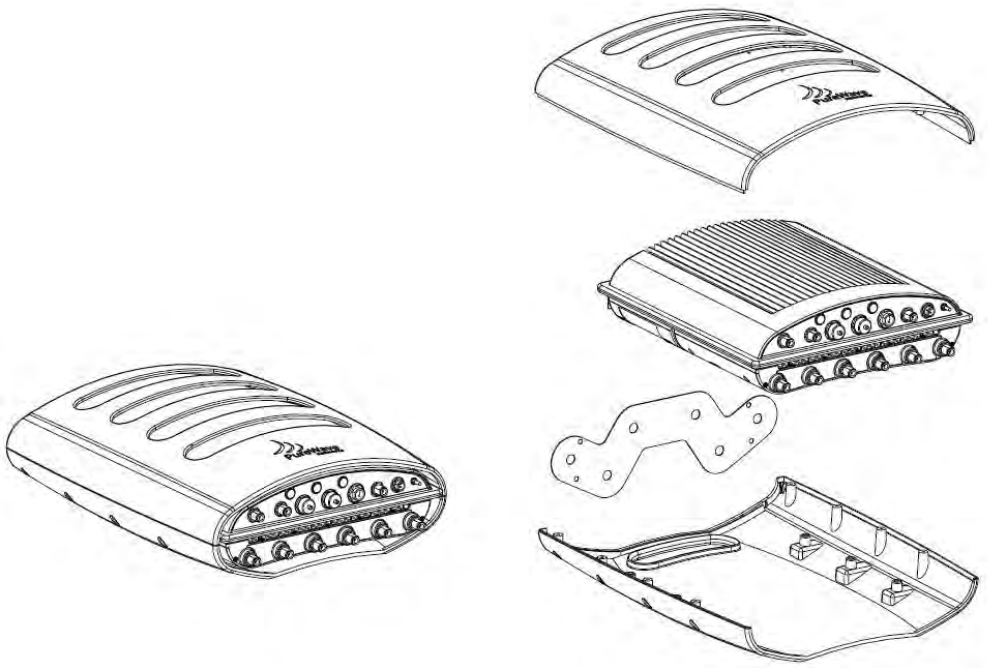


Figure 3 Quantum 6600 with Available Solar Shield

3. Quick Start Guide

This section describes how an Operator may power-up the Mercury Base Station and verify proper system initialization and configuration. There are two methods by which a Mercury Quantum Base Station may be configured and/or managed. This can be achieved via either a graphical user interface (GUI) Web Interface or a command line interface (CLI).

Each interface has the capability of configuring all parameters available in the Base Station. It is generally recommended to configure using the CLI for the first initial configuration of the Base Station or if the Base Station management interface parameters are not known. Mercury thereafter recommends using the Web Interface for all configuration parameters.

Note that the Web Interface and the CLI utilize the same terminology, parameter names, etc.

3.1 Preparing and Powering Up the Base Station

	Before powering on the Base Station, it is critical that all its connector panel ports be properly connected or terminated per the detailed instructions in the Mercury Quantum 6600 Installation Guide. Failure to do so may result in damage to the Base station.

The procedures in this section assume the following connections have been to the Base Station:

- Antennas have been connected to each Base Station ANT (ANT 1 through ANT 6) ports.
- A GPS antenna is properly installed and attached to the Base Station GPS port.
- The ETH-1 port is connected to an accessible network via a router or other mechanism.
- An appropriate cable has been connected to the Console port. To connect to the Console port, the User will need the following hardware that is provided with the Base Station installation kit. These are as follows:
    - RJ45 cable
    - DB9 male connector (Network Adapter)
    - DB9 female to DB9 female adapter

  The adaptor should be connected to a “straight-through” serial cable. Do not use a Cisco “rollover” cable or a null modem serial cable as these are not supported. Please see the Mercury Quantum 6600 Installation Guide for more details.

  Optional: Serial to USB connector. Most laptop nowadays comes with USB connection instead of serial connection. If the PC/laptop has a DB9 serial connection, then there is no requirement for a USB adapter. If not, then you will need to get serial to USB adapter to access the Base Station CLI. Plug one end of a “straight” Cat 5 Ethernet cable into the Base Station Console port and the other end into the RJ45 to Modem adapter. Connect the other end of this Modem adapter to a DB9 serial cable and connect this DB9 serial cable to a USB adapter that connect to your laptop.

With the Base Station and all cables properly installed, power may now be applied to the Base Station.

	The Base Station has no power switch so it will begin to power up immediately when a power source is attached. The POWER LED should be solid green

3.2 Default Parameters

Table 8 lists the factory default values that are set prior to shipment. These default parameters provide the means for a User to gain access to the system.

Parameter	Factory Default
Mgmt IP Address	192.168.1.10
Mgmt IP Network	255.255.255.0
Mgmt Default Gateway	192.168.1.254
Hostname	quantum-bs
Admin Username	admin
Admin User Password	admin123

Table 8 Base Station Management Interface and Access Default Parameters

3.3 Logging in to the CLI

The Mercury Quantum Base Station's Command Line Interface (CLI) has a standard Cisco IOS (Internetwork Operating System) look and feel to its operation. It is accessible via the Base Station Console interface using an appropriate terminal emulator, or via a Base Station ETH-1 port using either SSH or Telnet. Both methods of access will be described.

	Telnet is disabled by default so may not be used for initial configuration. It is assumed that the default parameters (IP address, baud rate, etc) are still in use. If defaults have been changed then please use the current values.

3.3.1 Accessing the CLI via the Base Station Console Port

1. Connect a computer to the Base Station Console port as detailed in section 3.1.

2. Open a terminal emulation program on the computer. Suitable programs are PuTTY or HyperTerminal (Figure 4).

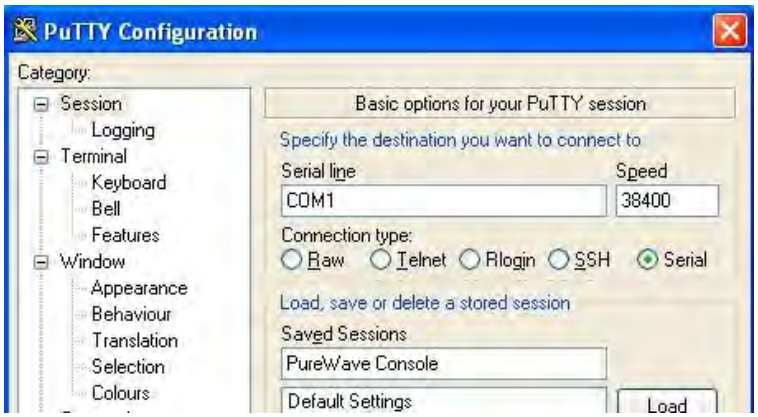


Figure 4 PuTTY Serial Port Configuration Window

Create a new connection with the serial port settings as outlined in Table 9.

Serial Console Port Settings	
Serial Line	COM1
Speed (Baud Rates)	38400
Data bits	8
Stop Bits	1
Parity	None
Flow Control	None

Table 9 Console Port Settings

A login prompt will be displayed as in Figure 5: Console Login. The default Login and Password are:

Default Login: **admin**
Default Password: **admin123**

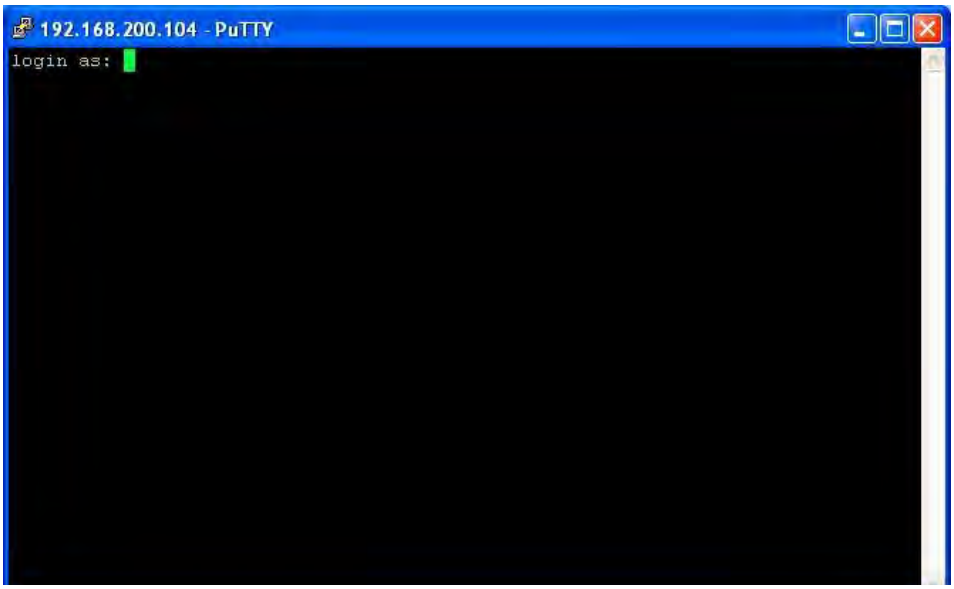


Figure 5 Console Login

3. After this login, the User will be presented at the *hostname prompt* (Figure 6). If the Base Station is still in its default status, then the hostname prompt will be *quantum-bs*.

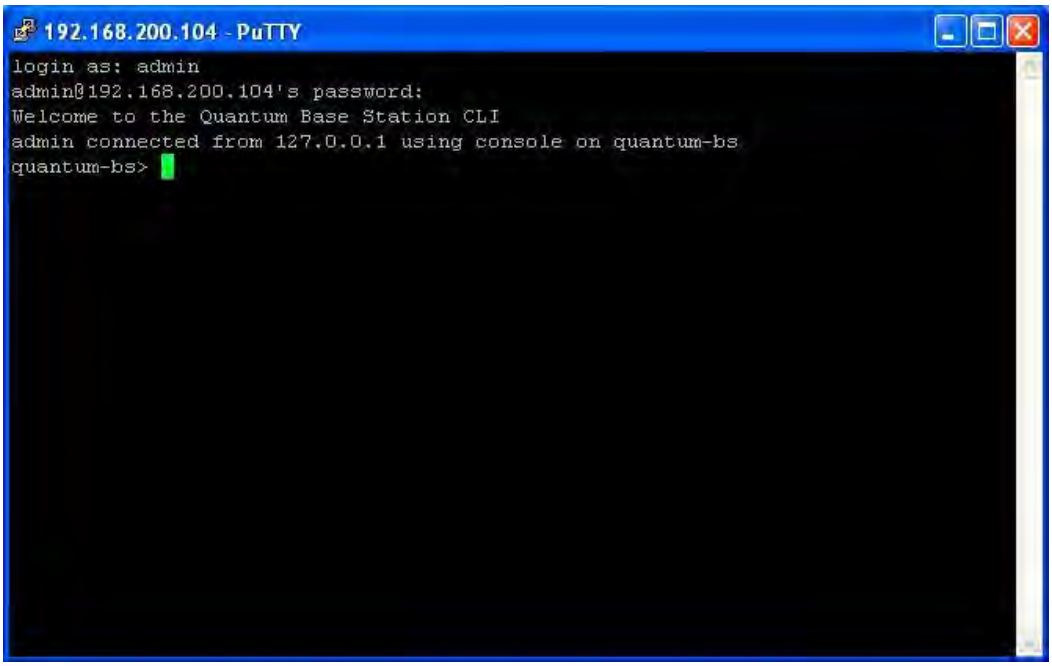


Figure 6 Console Login Default Status

3.3.2 Accessing the CLI via an Ethernet Port

1. Connect a computer using an Ethernet connection to the Base Station ETH-1 port (either directly or via a router or network). Open an SSH client program such as PuTTY (Figure 7). The default port number is 22.

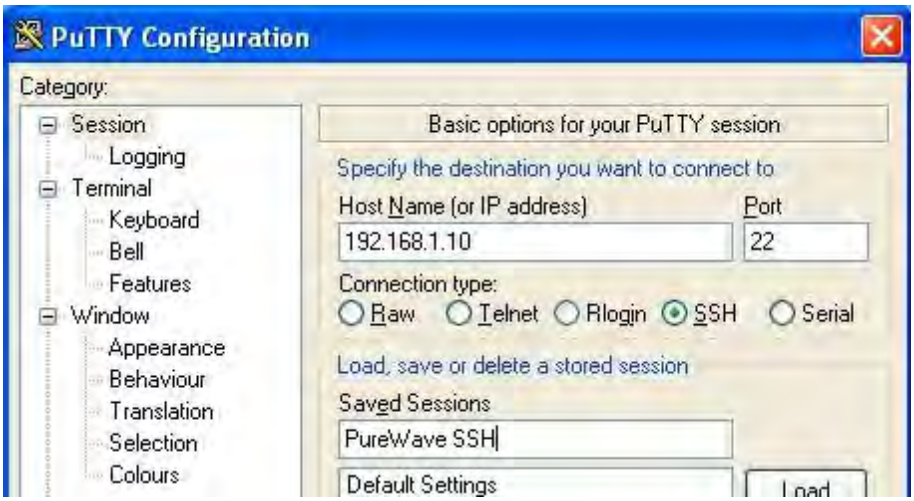


Figure 7 PuTTY SSH Client Configuration

2. Create a new SSH profile using the default management IP values. If the defaults have been changed, please use their current values.

	If the management IP settings are "unknown" then the Base Station can only be accessed via its Console port (refer to section 3.3.1). Once the Base Station has been accessed, its management IP settings can be reset using the procedure detailed in Section 3.5.2.

3. The default Login and Password are:
   Default Login: **admin**
   Default Password: **admin123**

3.4 Logging into the Web GUI Interface

The Mercury Quantum Base Station's Web Interface is accessible through most major web browsers that support SSL connections. The Web Interface has been specifically tested on Internet Explorer (Version 7 and up) and Mozilla FireFox. Access via HTTP and HTTPS are both supported; however, HTTPS is the default and HTTP is disabled by default.

If the current ETH-1 port IP settings have been lost, then they must be reset using access via the Base Station Console CLI (see section 3.3.1). The ETH-1 management IP settings must be known if the Base Station is to be accessed via the Web GUI Interface.

1. Connect a computer using an Ethernet connection to the Base Station ETH-1 port (either directly or via a router/network). Open an SSH client program on the computer.
2. Open a web browser and type https://192.168.1.10 or http://192.168.1.10 (if HTTP has been enabled, which is disabled by default) in the address field. If the default ETH-1 management IP settings have been changed, please use the current management IP.

	If the User is presented with a “certificate error” in the browser, then just click “ignore” or “continue to web site” and proceed.

3. The login page is displayed in Figure 8. The default Username and Password are:
   Default Login: **admin**
   Default Password: **admin123**

Figure 8 Web GUI Interface Login Page

4. After login, the User will be presented at the Main Web GUI Interface Screen (Figure 9). This will be the starting position for all subsequent configurations.

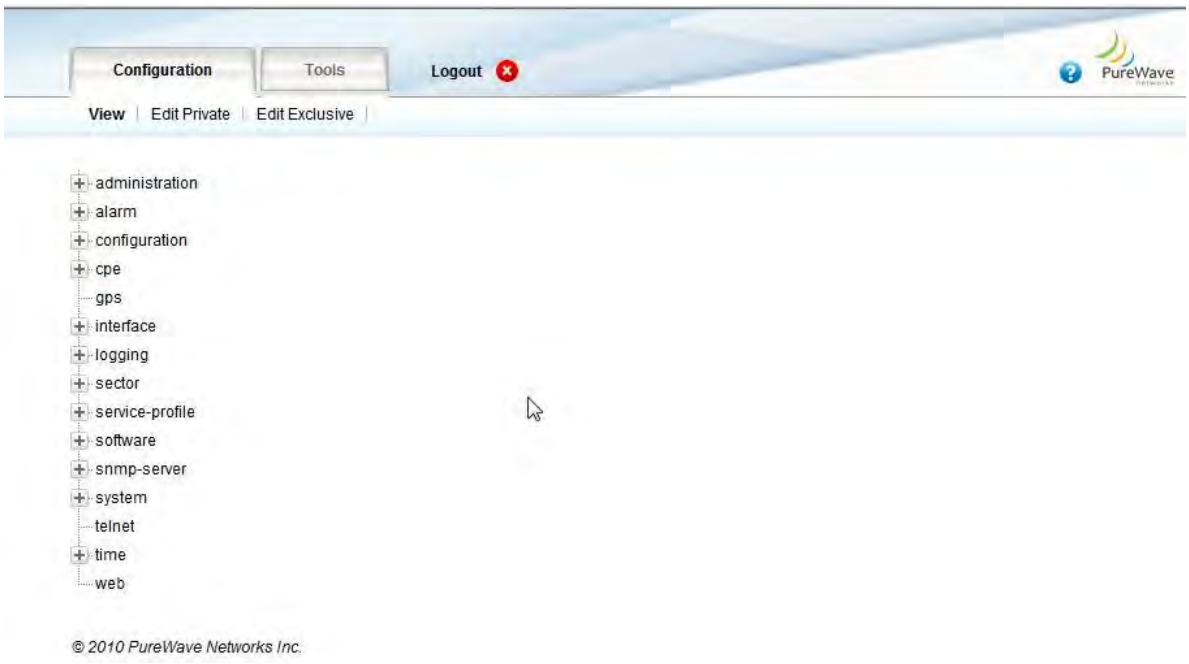


Figure 9 Main Web GUI Interface Screen

5. The structure of the Main Web GUI Interface Screen is as follows:
   - Configuration and a Tools tab across the top of the screen
     i. Underneath these Tabs there are the View or Edit modes of operation (Edit Private and Edit Exclusive).

- Configuration tree on the left-hand side of the screen which consists of the Main Menu Options. The plus sign "+" indicates that there are Main Menu Sub-Elements to each Main Menu Option. The right-hand side of the screen to the right of the Main Menu Options will be blank.

6. Once a Main Menu Option has been selected and navigated to, even if the User reverts to the Main Web GUI Interface Screen, the previous menu option will be displayed on the right-hand side of the screen. Once the screen is "refreshed", this will be cleared away.

To enable Base Station access via HTTP:

1. From the Main Web GUI Interface Screen select the *Configuration* Tab and then the *web* Main Menu Option form the left-hand side menu (Figure 10)

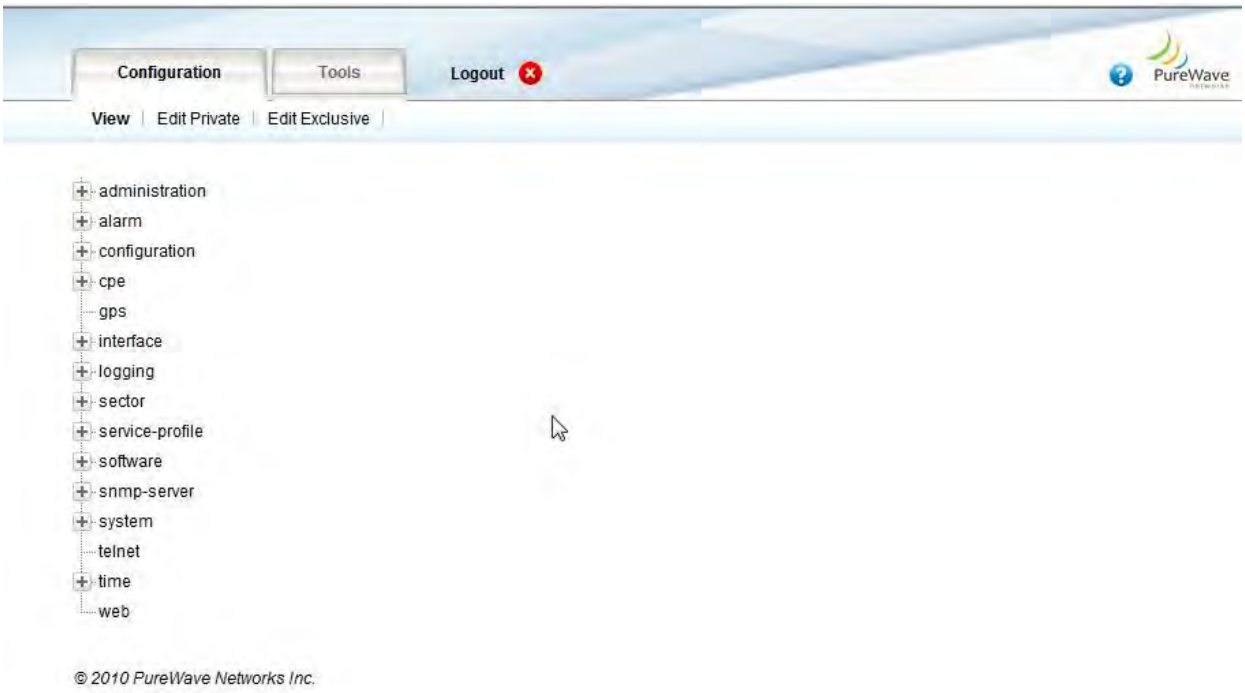


Figure 10 Web GUI Interface Configuration Menu

2. A window will be displayed that provides an indication or not as to the Web Server HTTP Support (Figure 11).

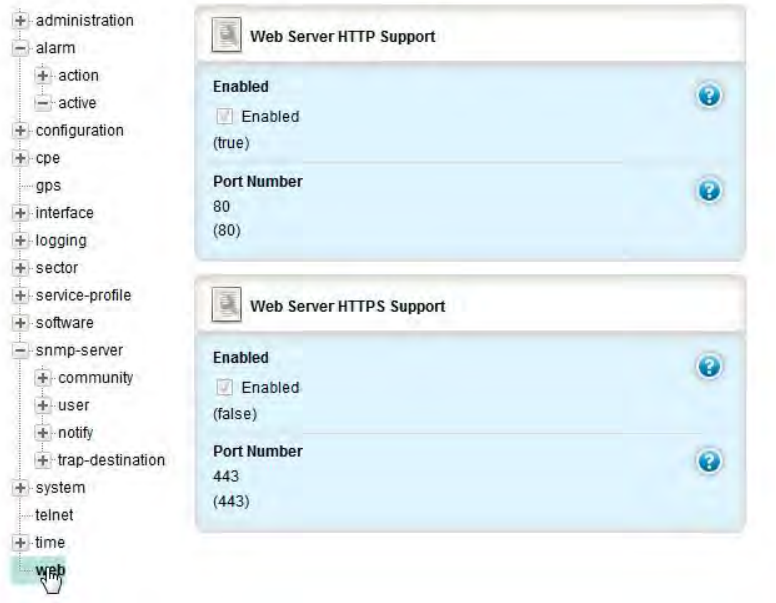


Figure 11 Web GUI Interface HTTP Support

3. To enable first select *Edit Private* or *Edit Exclusive.* This will drop the User into the Edit mode (Figure 12). The User can enable the Web Server HTTP Support by selecting the *Enabled* option.

4. The User must ***Commit*** the changes (apply the configuration in run-time). To commit, select the ***Commit*** option. A prompt screen will appear directing the User to confirm the pending configuration changes. To proceed the User must select ***Cancel*** or ***OK***.

3.4.1 Web Interface Configuration Key Concepts

The Web GUI Interface, when the Configuration Tab has been selected, has two major modes of operation:

- ***View Mode:*** Read-only access of all parameters. This is the default mode upon initial log in (refer to Figure 9).
- ***Edit Mode:*** Write access configuration of all available parameters. Within this mode there are two sub-options:
    - *Edit Private*. Edit Private will allow the user to configure all parameters but will not lock the configuration database, allowing for other users to make configuration changes at the same time (s).
    - *Edit Exclusive*. Edit Exclusive will lock the configuration database and prevent any other user from making configuration changes.

⚠	Note: System configuration changes are first made to the running configuration database in memory. This allows the opportunity for the user to test the changes first before saving. In order to make the change persistent and survive a restart, the "Configuration-Write" command must be used.

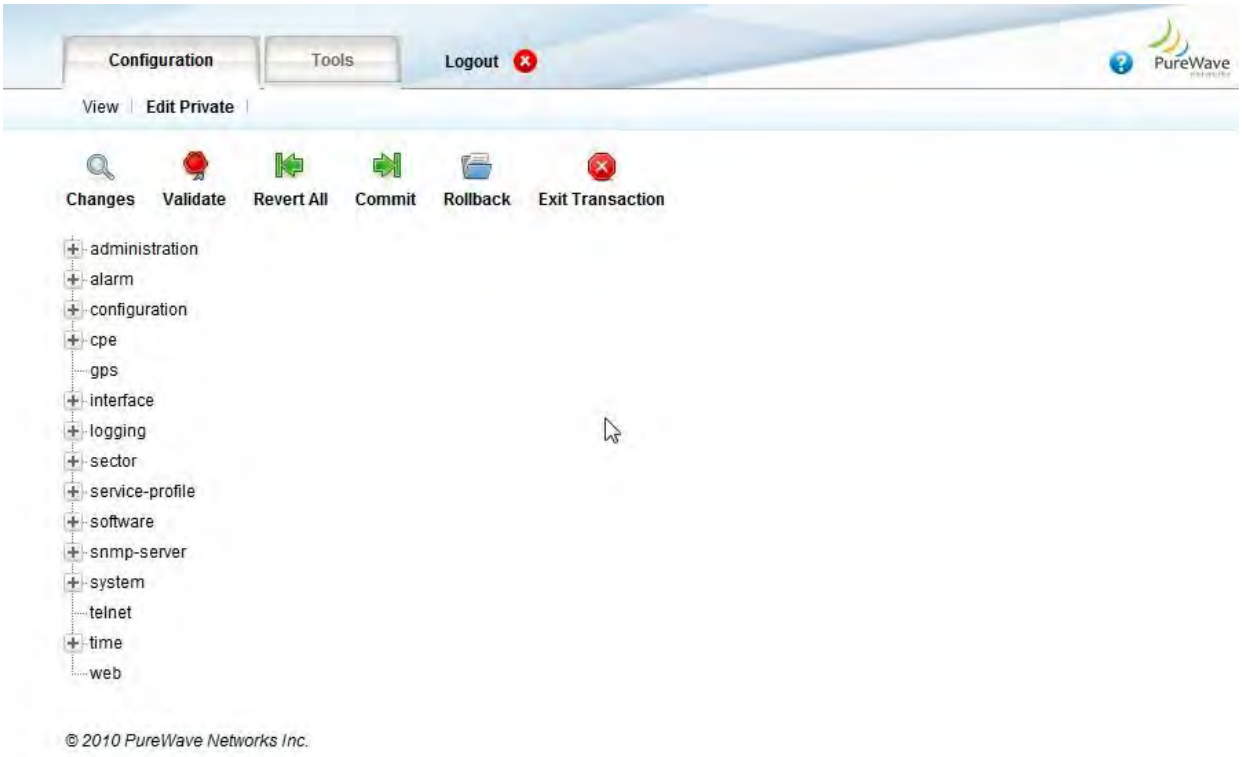


Figure 12 The Web GUI Interface Screen in Edit Private Mode

At the Main Web GUI Interface Screen, select the *Configuration* Tab, select the *configuration* Main Menu option and then *Edit Private* or *Edit Exclusive.* The User will now be in the Edit mode.

There are a number of key concepts that will be repeatedly used when the User is in the Edit mode and thus making configuration changes. These key concepts form the six Command Menu Options when the User is in the Edit mode. These are:

- ***Changes.*** This prompts the User to see the configuration changes that have been made.
- ***Validate.*** This validates that the changes are valid and have been configured correctly.
- ***Revert All.*** This will cancel (or revert) any changes that may have been made.
- ***Commit.*** This will commit the changes to the running database.
- ***Rollback.*** This will rollback any changes to a previously saved state.
- ***Exit Transaction.*** This will exit the Edit mode.

When the User selects the *Changes* Command Menu Option then they are presented with the following options:

- If no configuration changes have been made, then a popup window appears stating "No configuration changes have been made". The User simply selects the *OK* prompt to navigate back to the Edit Mode.

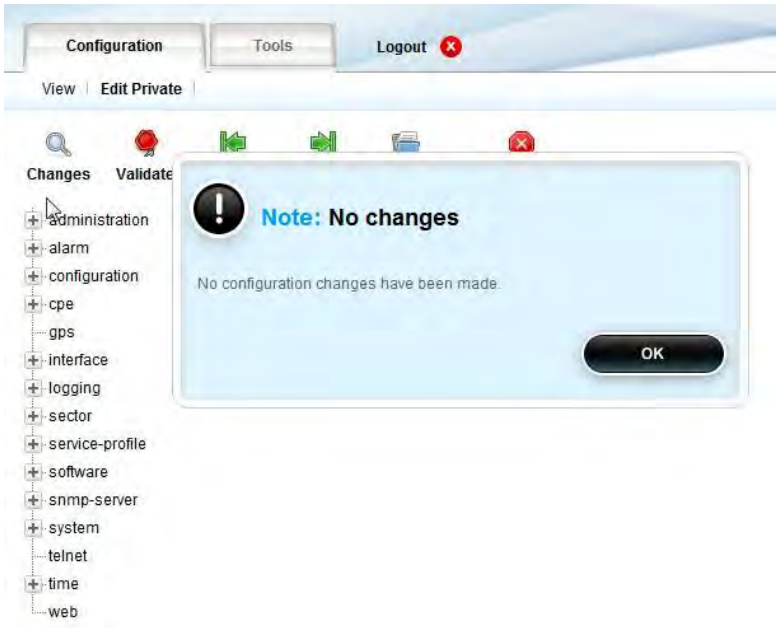


Figure 13 Configuration Changes Popup Window

- If relevant changes have been made, then a window appears. This indicates the relevant parameter that is in the process of being changed and the old and the new value.
- There is also an option within this window to ***Revert*** the change (Figure 14). If the User selects this revert option, then the intended changes will be reversed and the "No configuration changes" will appear (Figure 13).

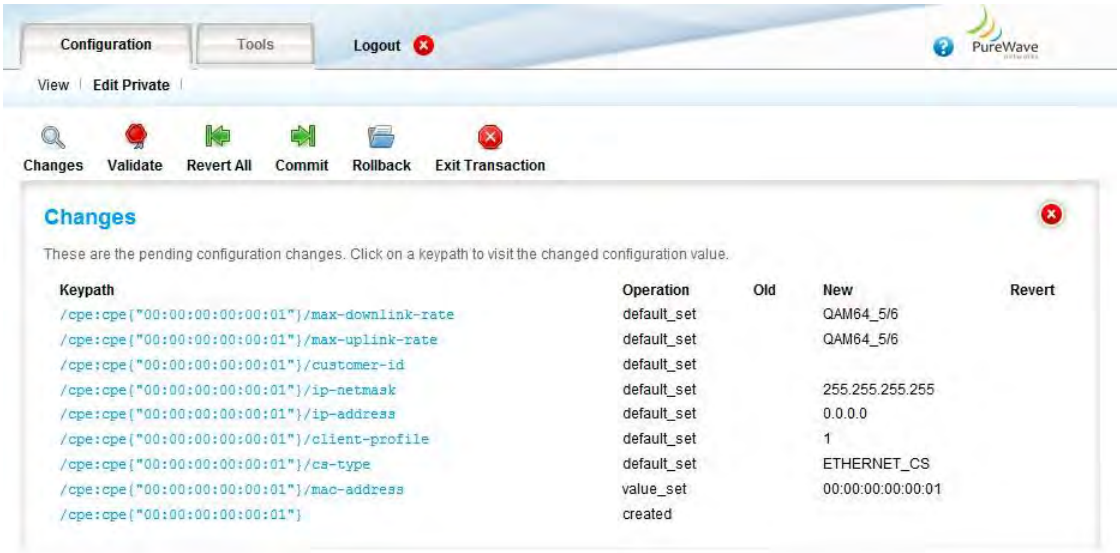


Figure 14 Revert Option

If the User has made some configuration changes and then they decide to reverse the changes then the User can select the *Revert All* window option. Selecting this option presents:

- If no configuration changes have been made, then a window appears stating "There is nothing to revert". The User simply selects the ***OK*** prompt to navigate back to the Edit Mode.
- If changes have been made, then a window appears stating "All your noncommitted configuration changes will be reverted" (Figure 15). The User simply selects the ***OK*** prompt to proceed and navigate back to the Edit Mode.

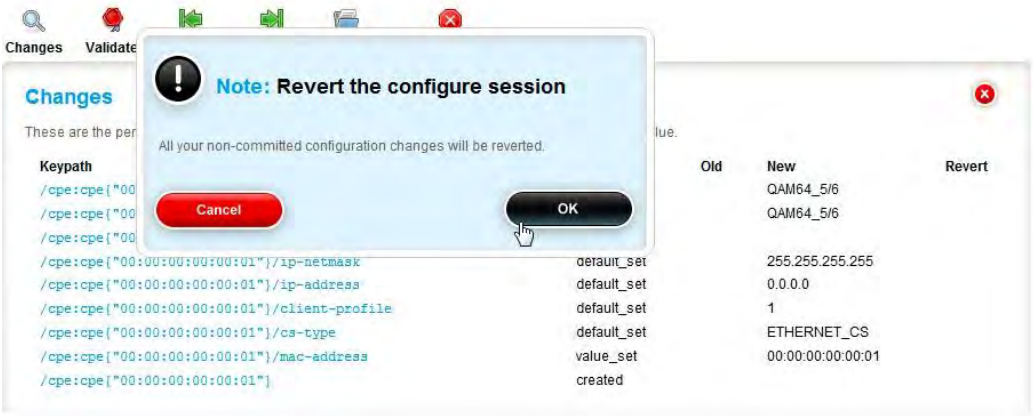


Figure 15 Revert All Configuration Changes

If the User has made some configuration changes and these have been committed and saved the User can make use of the *Rollback All* window option. A rolling audit log of all configuration changes in stored within the Base Station. This log is a record of:

- *Rollback File*. This is the name of the rollback file.
- *Creator*. This is the creator of the change. This will be the login name that was used at the time of the configuration change.
- *Date*. This was the date of the change.
- *Via*. This was the method of access to the Base Station that was used to effect the change.
- On the right side of the window, is a text pad that provide details of the parameters and how they were changed.

To perform the *Rollback* procedure then the User simply must highlight the relevant rollback file and then select the *Load* Command Menu Option below.

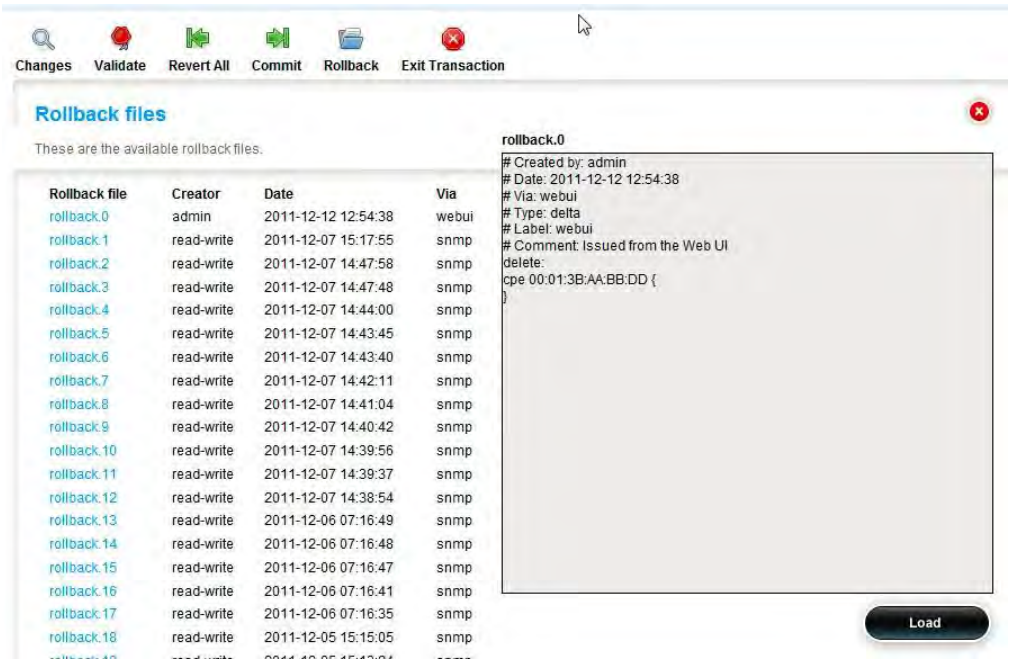


Figure 16 Rollback Option

If the User has made some configuration changes and they wish to Validate the changes then the User can select the ***Validate*** Command Menu Option. If the User, after making the relevant changes, selects the Validate option then if the intended changes are valid, then a window appears stating "The configuration is ready to be committed" appears below. The User simply selects the *OK* prompt to proceed and navigate back to the Edit Mode.

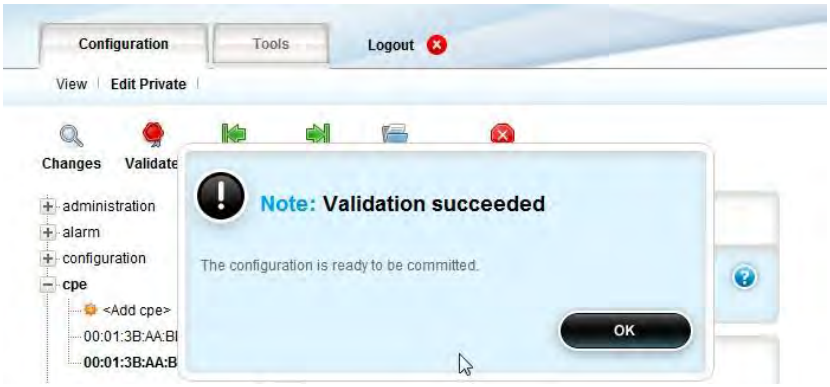


Figure 17 Validate Option

The ***Commit*** Command Menu Option performs a crucial procedure in that it commits all configuration changes to the running database.

	When in Edit mode, the method of configuring and saving changes remains the same. A user may change any number of parameters but none of those changes will take effect until they are committed.

Clicking the Commit Menu will result in one of the following actions

- If no configuration changes have been made, then a window appears stating "There is nothing to commit". The User simply selects the *OK* prompt to navigate back to the Edit Mode.
- If changes have been made, then a window appears stating "Do you want to commit your pending configuration changes?". The User simply selects the *OK* prompt to proceed.

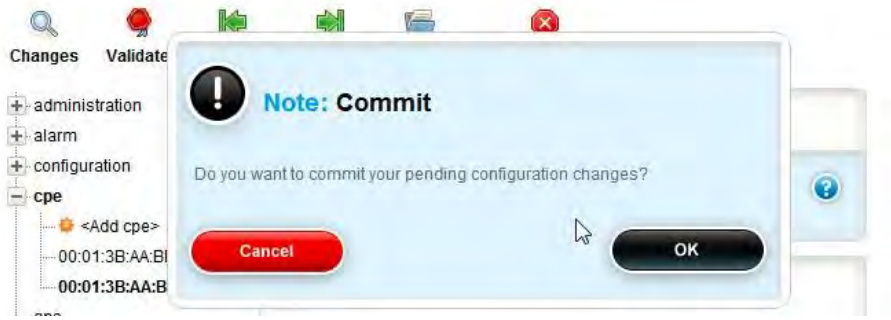


Figure 18 Commit Option

⚠	Note: System configuration changes are first made to the running configuration database in memory. In order to make the change persistent and survive a restart, the "**Configuration-Write**" command must be used.

- When *OK* has been selected then a window appears stating "The configuration has been committed". The User simply selects the *OK* prompt to proceed and navigate back to the Edit mode.

✎	Unsaved configuration changes persist for only the current boot. If the Base station is rebooted then those changes will be lost if the configuration has not been saved.

Several menus have two sets of parameters, these are defined as:

- ***Configured Parameters*.** These are the most recently saved settings and are stored in the system's configuration database
- ***State Parameters*.** These are the readings of the actual state from the Base Station. State Parameters may be identical to Configured Parameters, or they may be committed but not propagated to the Base Station.

✎	After a reboot, both sets of parameters will be identical.

The "**Save Procedure**" is to ensure that the running configuration is saved is:

1. At the Main Web GUI Interface Screen, select the *Configuration* Tab, select the *configuration* Main Menu Option then the *write* Main Menu Sub-Element. The User will have to click on the ***Perform*** Command Menu Option to copy the running configuration to the startup as below.

Figure 19 Writing Running Configuration to Startup

2. A pop-up window indicating that the write was successful will be displayed.

	Note: Several configuration changes require that the Sector be rebooted. The only parameter requiring a complete Base Station reboot is enabling or disabling the ASN Gateway settings.

The procedure to reboot a Base Station is as follows:

1. At the Main Web GUI Interface Screen, select the *Configuration* Tab, select the *administration* Main Menu option and then ***reboot*** Main Menu Sub-Element. The User will have to click on the ***Perform*** Command Menu Option to reboot the entire Base Station (Figure 20).

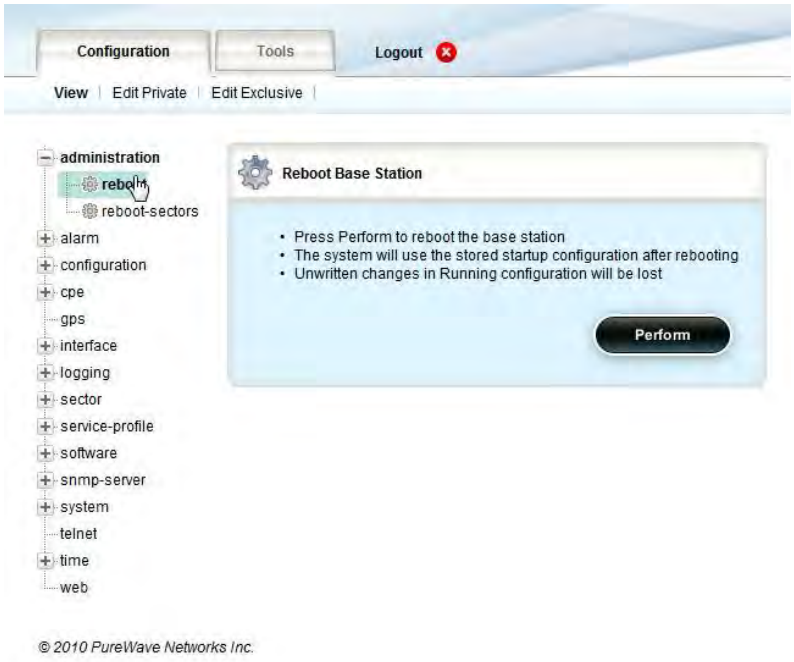


Figure 20 Reboot Base Station

2. Upon clicking perform, the user must confirm the reboot operation by clicking ***Ok***. After the reboot option has been performed then an appropriate window indicating a successful reboot execution will be displayed. The subsequent time for the Base Station to become operational is approximately 5 minutes.
3. The system will use the stored startup configuration after rebooting. Unwritten changes in the running configuration will be lost.
4. There are two reboot options under the administration Main Menu options including:
   - ***reboot*.** This option will reboot the Base Station
   - ***reboot-sectors*.** This option will reboot the internal elements of the Base Station that are pertinent to the sector RF elements only. After the reboot sectors option has been performed then an appropriate window indicating a successful reboot execution will be displayed. The subsequent time for the Base Station to become operational is approximately 2 minutes.

3.4.2 Web GUI CLI Access Level

The Mercury Quantum Base Station has a Command Line Interface (CLI) that can be accessed from within the Web GUI. To access the Web GUI CLI then at the Main Web GUI Interface Screen, select the ***Tools*** Tab. The User will be presented with a number of User tools as below.

Figure 21 The Tools Tab Menu Options

- The User is presented with four *Tools* Command Menu Options. These are:
  - ***Logs.*** This allows the User to display and hence view:
    - ***System log***
    - ***Alert log***
    - ***Audit log***
- ***Accessories.*** The following protocols are made available to the User:
    - ***Ping***
    - ***Traceroute***
    - ***CPU Load***
  - ***CLI.*** The User has access to the CLI and can execute all the CLI commands directly if required.
  - ***Users.*** This indicates all the Users that are currently connected to the Base Station. It also provides a means to physically "kick" them off their connection. In addition, a message board is provided thus enabling instant messages to be sent to the Users that are currently connected to the Base Station.

3.4.2.1 Tools Logs

At the Main Web GUI Interface Screen, select the *Tools* Tab and then *Logs*.

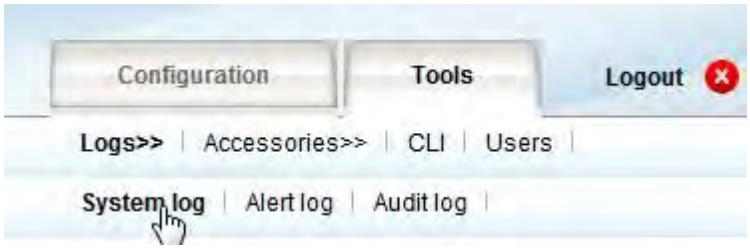


Figure 22 The Tools Tab Logs Menu

To view the relevant Log, the User simply must select one of the 3 logs that are available to view. These logs are system, alert and audit logs. The three Tools logs are displayed below.

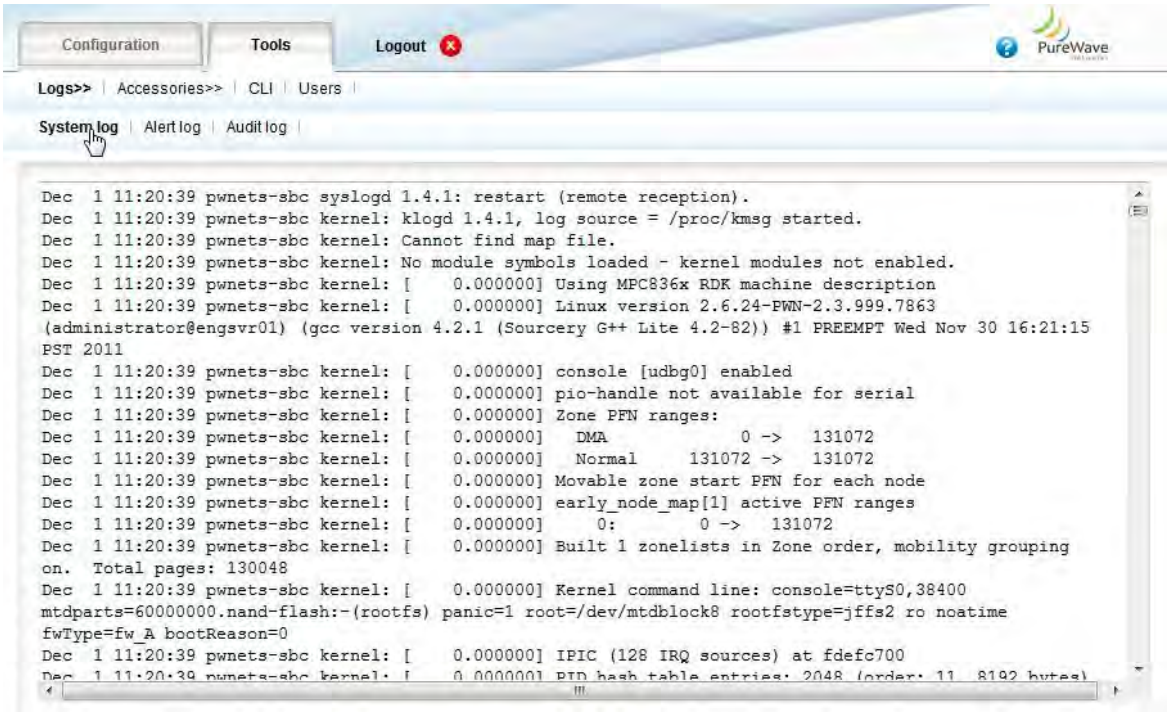


Figure 23 The Tools Tab System Log

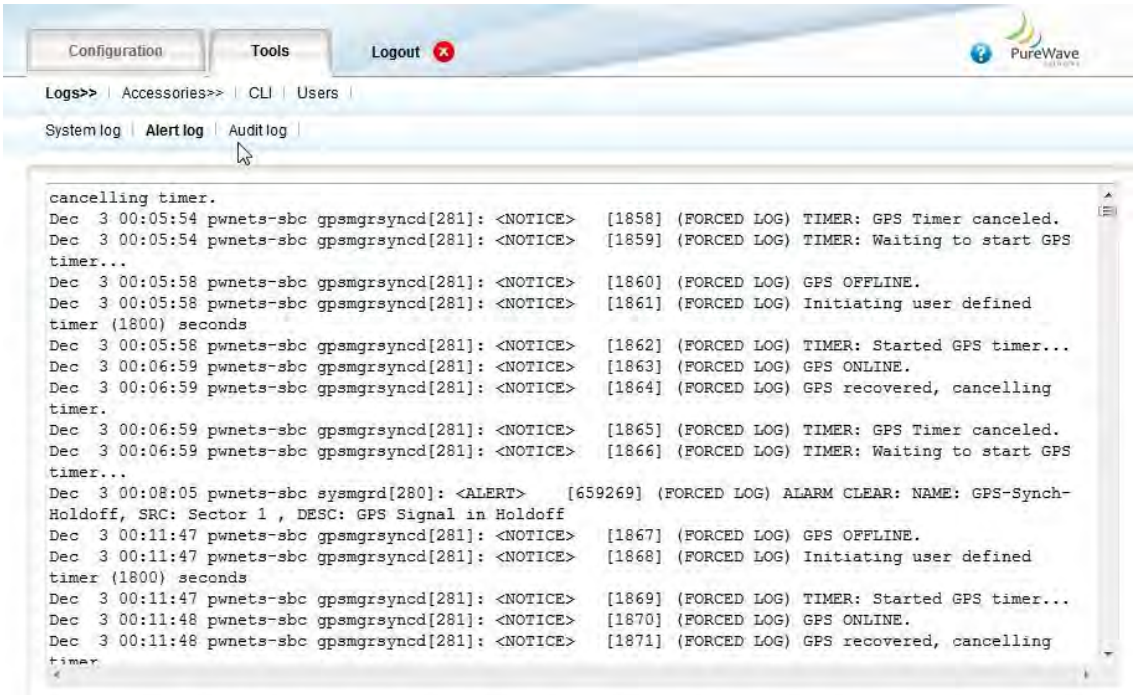


Figure 24 The Tools Tab Alert Log

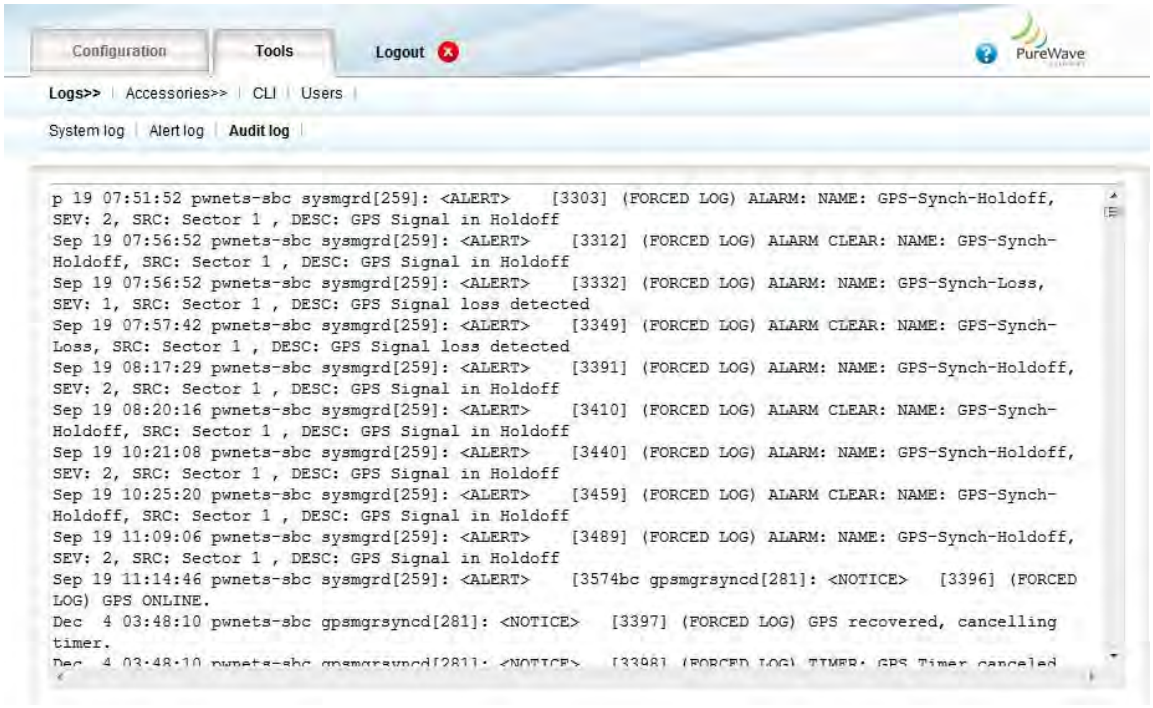


Figure 25 The Tools Tab Audit Log

3.4.2.2 Tools Accessories

At the Main Web GUI Interface Screen, select the *Tools* Tab and then *Accessories* as below.

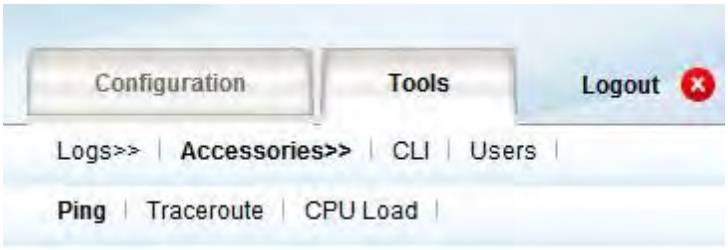


Figure 26 The Tools Tab Accessories Menu

To perform the relevant protocol, the User must select the relevant option. To enable *Ping* or ***Traceroute***, the User must:

1. Select the ***New*** button
2. A pop-up window will appear, this will enable the User to specify the host (Figure 27)
3. The User must now select the ***OK*** command button
4. The results will be displayed as below

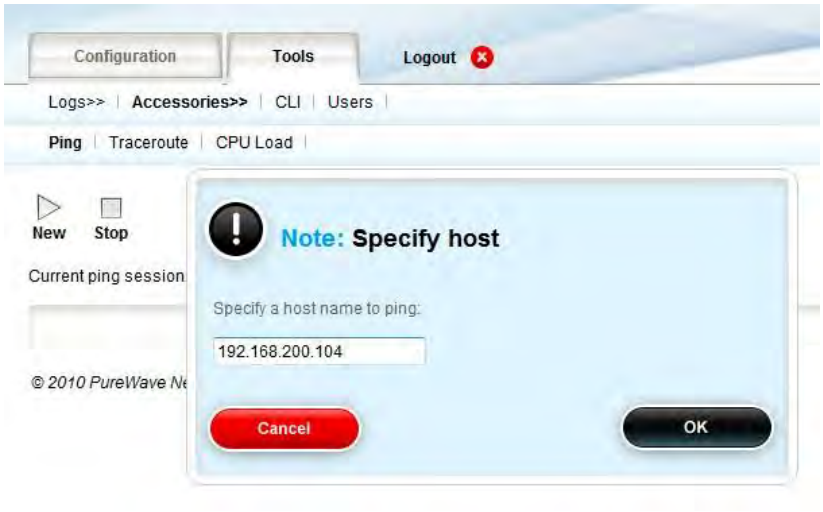


Figure 27 The Accessories Ping Command

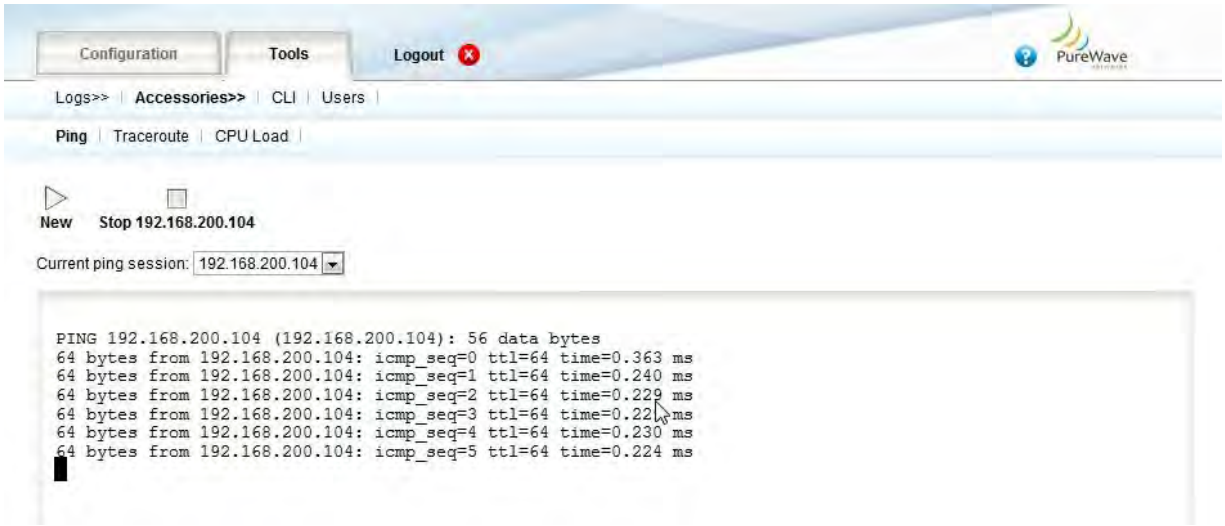


Figure 28 The Accessories Ping Results

To examine the *CPU Load*, the User must select the ***CPU Load*** option. The User is presented with a display of the current CPU load. This will automatically be updated every 5 seconds and it will calculate the load averages over 1, 5 and 15 respectively (Figure 29).

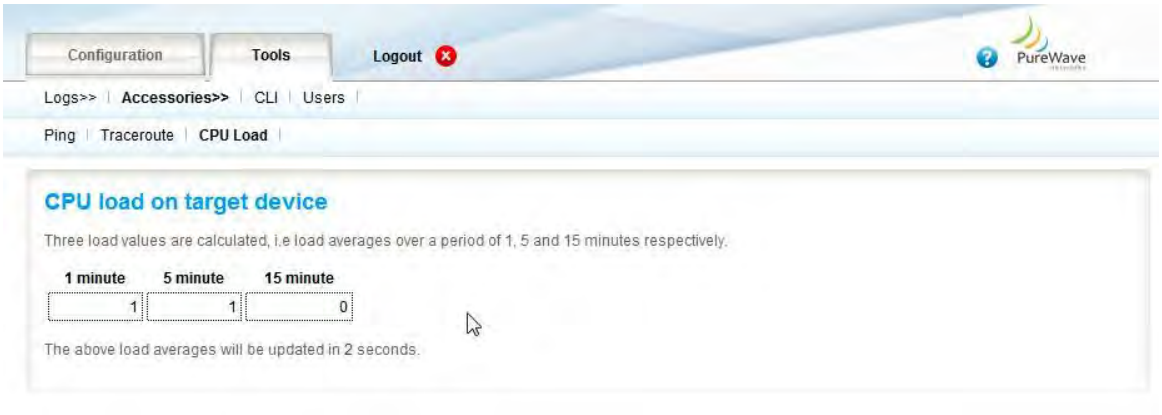


Figure 29 The Accessories CPU Load Results

3.4.2.3 Tools CLI

At the Main Web GUI Interface Screen, select the *Tools* Tab and then *CLI.* The User is presented with a CLI screen (Figure 30). The User is free to enter all the available CLI options.

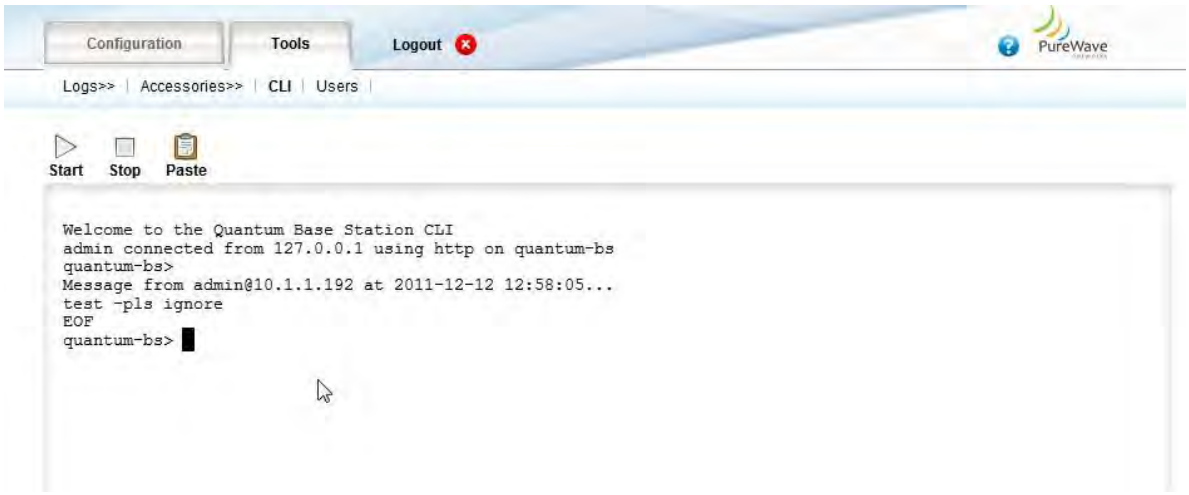


Figure 30 The Tools Tab CLI

3.4.2.4 Tools Users

At the Main Web GUI Interface Screen, select the ***Tools*** Tab and then ***Users****.* The User is presented with a screen that indicates the Users that are currently logged in to the Base Station and an instant messaging section to communicate with these Users (figure 37).

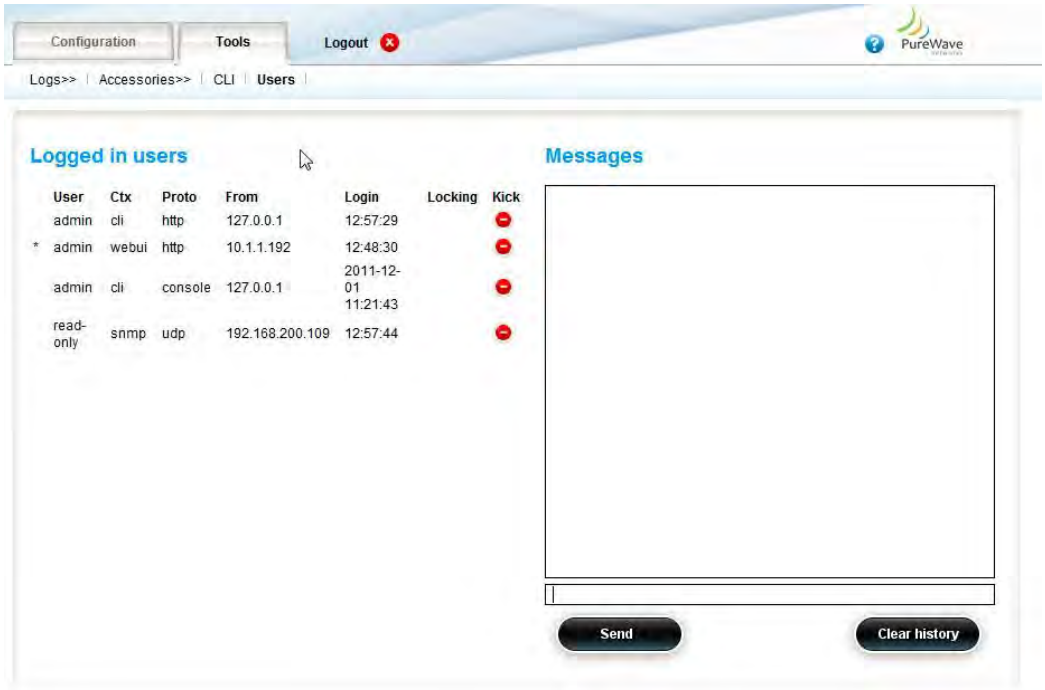


Figure 31 The Tools Tab Users Connected to Base Station

The User can also physically disconnect or "kick" off the User. The User must select the ***Kick*** command option. A message board is provided to enable instant messages to be sent to the Users that are currently connected to the Base Station. The User must enter the relevant message in the text box and then press ***Send***. There is also the option to ***Clear history*** if required (refer to figure 38).

Figure 32 The Tools Tab User Instant Messaging

3.5 Base Station Initial Configuration

3.5.1 System Architecture and Terminology

In this section we will configure the minimal set of parameters that must be appropriately set prior to deployment. It is important to first clarify some terminology related to the system architectural model.

In typical terminology, a Base Station is comprised of one or more co-located sectors. Each Mercury Quantum 6000 Base Station can be deployed either by itself, as a single sector Base station, or as one sector in a multi-sectored Base station. In either case, each Mercury Quantum 6000 must be fully configured and provisioned in its entirety, as if it was a standalone Base Station.

The various Web Interface configuration parameters are organized into a hierarchical tree, and that some parameters are labeled as “Base Station” level and some “sector” level. Since the Quantum 6000 Base Station is really both a sector and a Base station, the differentiation is for organizational purposes, as well as compatibility with future multisector functionality or products.

Additionally, a Base Station must be connected to subscriber devices on the air-interface side and to a Core Network on the backhaul side. As discussed previously, Mercury Quantum 6000 Base Stations can flexibly support a variety of core network configurations, ranging from a simple router (“Standalone Mode”) to a full ASN-GW. It also has a built-in Radius client for connection to an external AAA server when in Standalone Mode.

3.5.2 Base Station Management Interface Access Parameters

Table 10 lists the minimum set of management interface parameters that must be set prior to deployment. These parameters govern how an operator, administrator, or management system interfaces with and gains access to the Base Station. Before proceeding, please gather the information listed in the table. Factory default values are provided here as they are required for initial access.

Parameter	Description	Factory Default
Mgmt IP Address	IP address used for all external Mgmt interfaces (CLI / Web / SNMP).	192.168.1.10
Mgmt IP Netmask	Mgmt interface IP netmask	255.255.255.0
Mgmt Default Gateway	Mgmt interface default gateway	192.168.1.254
Hostname	String name assigned to the Base Station.	quantum-bs
Admin User Password	Unique password for default admin	admin123

Table 10 Base Station Management Interface and Access Parameters

To perform the initial configuration of the Base Station, it is recommended to configure the Management Interface Parameters via accessing through the Base Station Console Port. To complete this section, you will need the data in Table 10.

	If the management IP settings are "unknown" then the Base Station can only be accessed via its Console port (refer to section 3.3.1). Once the Base Station has been accessed, its management IP settings can be reset using the procedure detailed in section 3.4.

	Even though the CLI may be accessed through the Ethernet ports, it is not the recommended method of changing the management interface parameters, as connectivity with the port will be lost immediately upon changing them.

Log into the CLI (Section 3.3) and execute the commands as indicated to configure the Base Station access parameters. Text in brackets <…> should be replaced with your configuration data to replace the default values from the table above.

1. At the quantum-bs> prompt, type ***enable***. This will drop the User into the enable mode and the prompt will change from > to # (Figure 33).

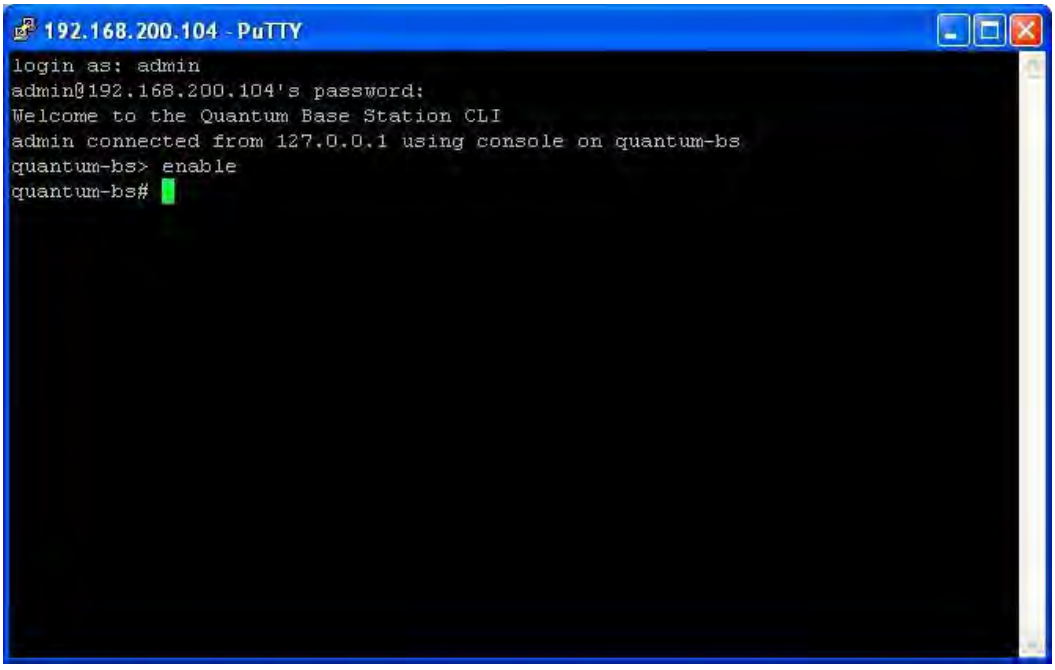


Figure 33 Initial Connection to CLI

2. At the quantum-bs# prompt type ***configure terminal***. The prompt will now indicate that the User is now in config mode and it will display the current Base Station time (Figure 34).

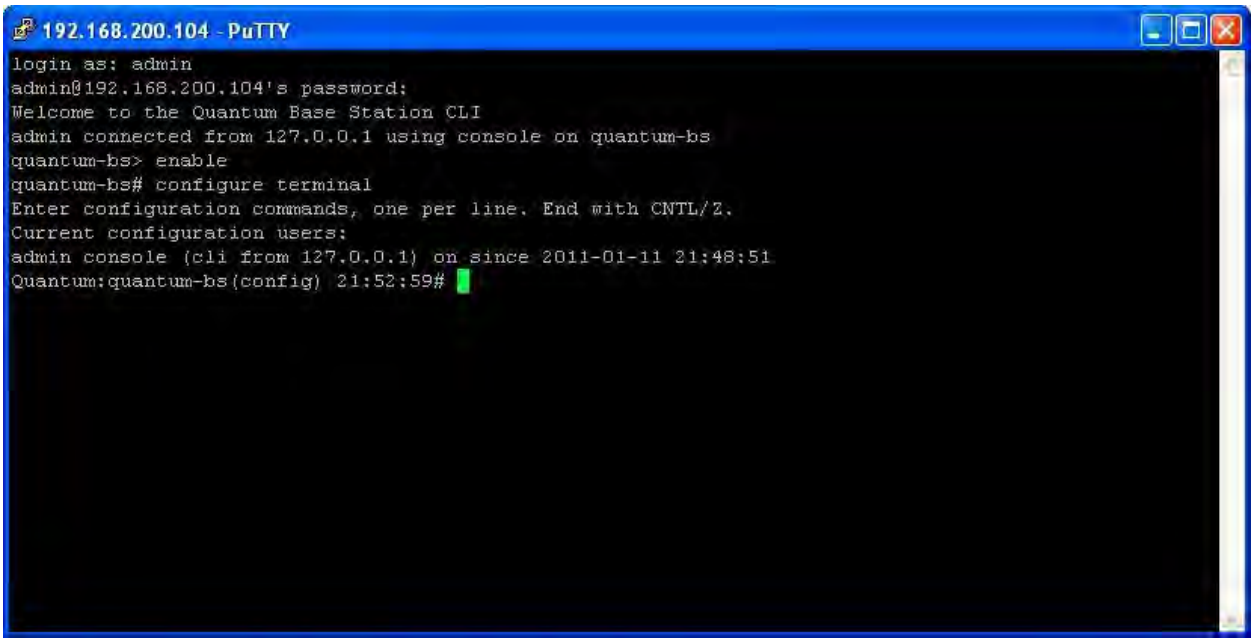


Figure 34 Base Station CLI Time

3. To set the Management IP address, at the Quantum:quantum-bs(config) prompt type ***system interface ip address <Mgmt IP Address> netmask <Mgmt IP Netmask>*** **e.g.** ***system interface ip address 192.168.200.104 netmask 255.255.255.0***
4. To set the default Gateway at the Quantum:quantum-bs(config) prompt type ***system interface ip default-gateway <Mgmt Default Gateway>*** **e.g.** ***system interface ip default-gateway 192.168.200.1***
5. To exit, at the Quantum:quantum-bs(config) prompt type ***exit***
6. The changes must be written to memory. At the quantum-bs# prompt type ***write memory*** (Figure 35)

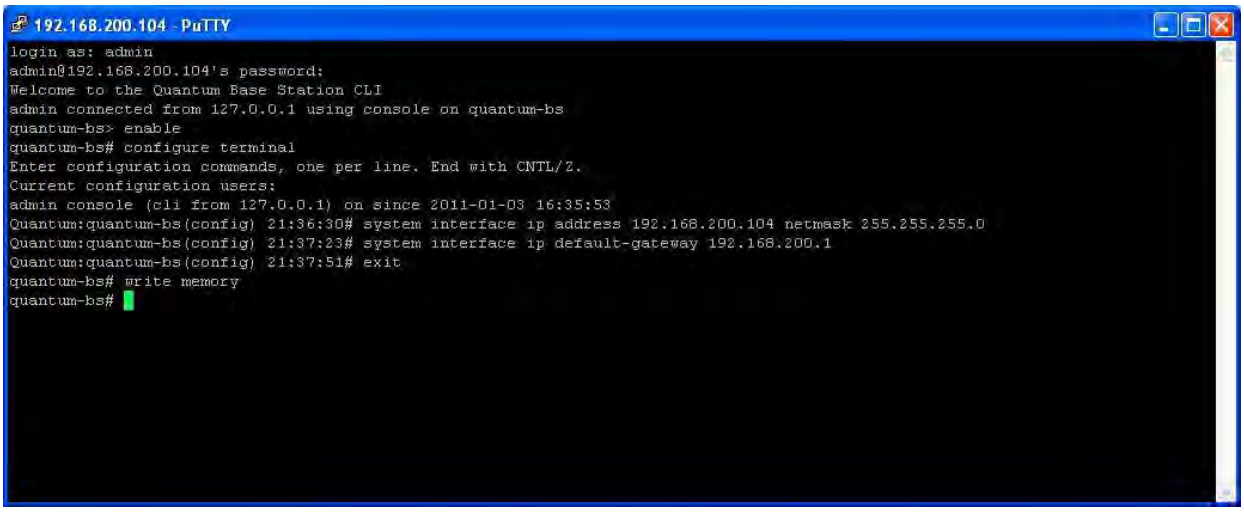


Figure 35 Base Station CLI Initial Configuration

7. The IP address change to the Base station is immediate and does not require a reboot
8. Another useful command is the ability to change the default Quantum prompt. When the User is in the ***config*** mode, type ***system hostname <Hostname>*** (refer to Figure 36). The change must be written to memory and the Base Station must be rebooted

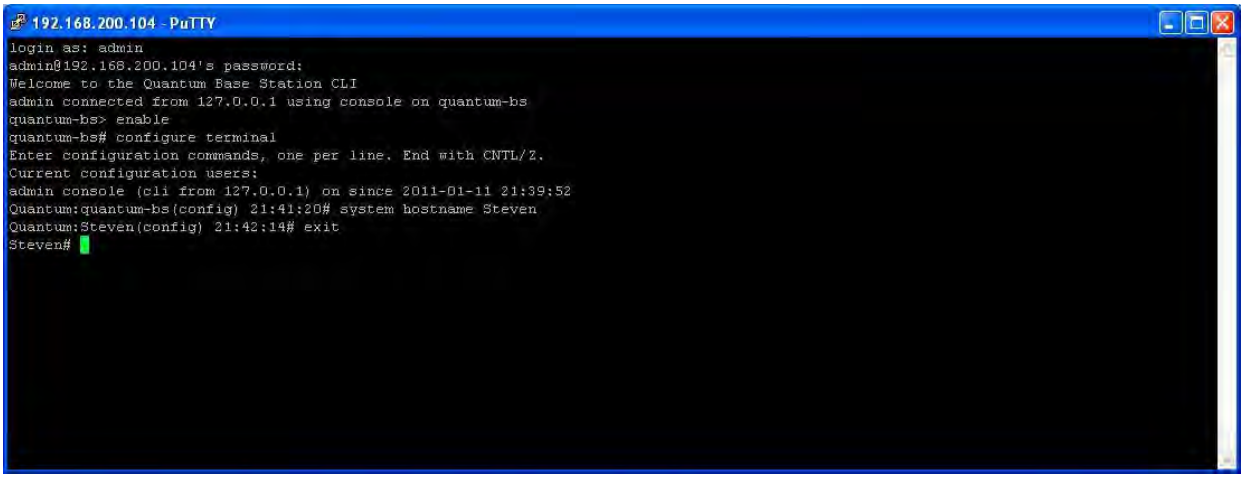


Figure 36 Base Station CLI Hostname Change

9. To change the username admin password, when the User is in the ***config*** mode, type

   username admin password

   - ***Password <new admin User Password>***

The change must be written to memory (Figure 37).

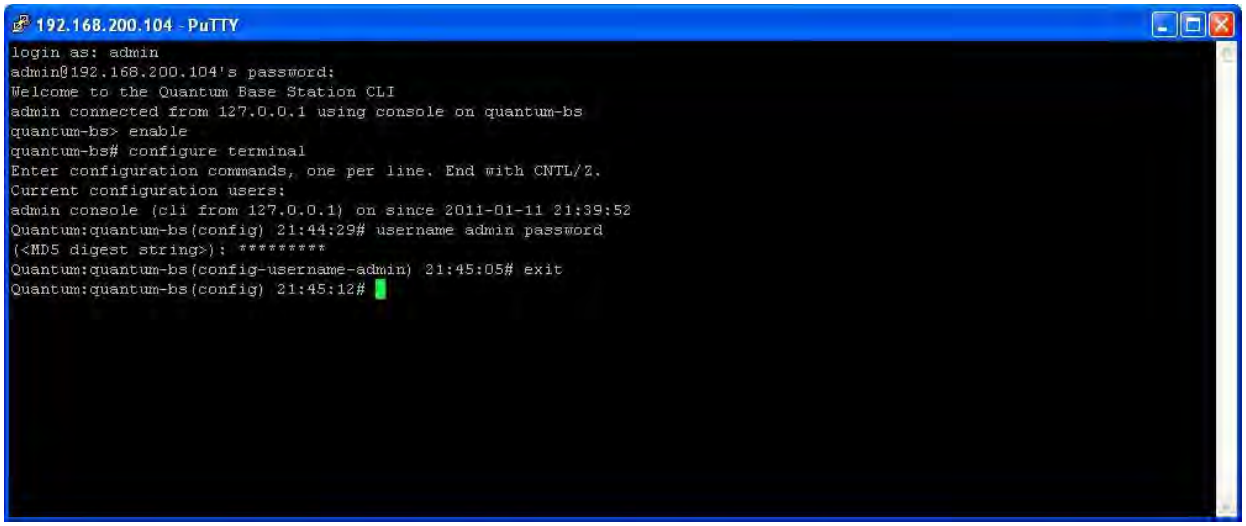


Figure 37 Base Station CLI Username Password Change

3.5.3 Base Station Configuration Parameters

There are several key parameters that must be configured, as a minimum, prior to deployment and operation of the Base Station. Table 11 is a list of these parameters. In addition to these key parameters, there are several other parameters that can be configured on the Base Station. Such parameters can be left in their default configuration for "nominal" Base Station operation but there is the option to change based upon specific operating conditions. All parameters will be described in the following sections.

One point to make, is that in the context of the Mercury Quantum 6600, as this is a single sector Base Station, the terms “Sector” and “Base Station” are effectively synonymous. This fact is represented within the Web GUI Interface using the number 1 at the appropriate menu option. The number 1 stands for Sector 1.

The key Base Station parameters that must be configured are:

Configuration Item	Description
Base Station Mode	Standalone Local Mode(default) or ASN Gateway Mode
ASN Gateway IP Address	IP Address of the ASN-GW (ASN-GW Mode only)
Configuration Item	**Description**
Base Station Radius IP Address	IP Address of the Radius Server (Standalone Mode only)
Base Station Radius Port	Radius Server Port (Standalone Mode only)
Base Station Radius Secret	Radius string secret (Standalone Mode only)
Sector IP Address	IP Address of the sector’s datapath interface
Sector IP Netmask	Netmask of the sector’s datapath interface
Sector Default Gateway	Default gateway of the sector’s datapath interface
Sector BS-ID	Base Station ID of the sector. In 6 Byte format like MAC Address format
Sector CS Type	Convergence sub-layer type of the sector: Ethernet CS (default) or IPv4 CS

Sector Radio Center Frequency	Center frequency in kHz
Sector Channel Bandwidth	3.5MHz, 5MHz, 7MHz, or 10 MHz (default)
Sector Radio Power Output	Preamble power output value per antenna (includes 3 dB preamble). Default: 23 dBm. ***Operations under FCC Part 96:*** ***Power setting shall not exceed:*** ***3.5 MHz: 31 dBm*** ***5 MHz: 32 dBm*** ***7 MHz: 32 dBm*** ***10 MHz: 33 dBm***
Sector Radio Antenna Gain	Antenna gain (dBi)
Sector Radio Cable Loss	Estimated external cable loss (dB)
Sector Antenna TX Mode	MIMO-A (default) or MIMO-AB
Sector DL:UL Frame Ratio	26:21, 29:18, 32:15, 35:12 (default) in 5MHz and 10MHz 23:9, 21:12, 17:15 in 3.5 and 7MHz

Table 11 Base Station Sector Configuration Data

The Web GUI Interface will be used to configure the parameters that are required in Table 11. The starting point for all configurations is the Main Web GUI Interface Screen. The relevant parameters are distributed across several different menu options and hence screens and windows. Each of these options will be discussed in detail.

After making the various configuration changes, the User will need to "commit" and "save" the changes.

3.5.3.1 Sector, General Settings

At the Main Web GUI Interface Screen select the *Configuration* Tab, select *sector* Main Menu Option and then *general* Main Menu Sub-Element. This will display the Sector Settings window.

There are two basic groups to this Sector option. These are:

- ***Sector Advanced Settings (configured)***
- ***Sector Provisioning (configured)***

The User now has to navigate to the next level, therefore at the Main Web GUI Interface Screen select the ***Configuration*** Tab, select ***sector*** Main Menu Option, ***general*** Main Menu Sub-Element and then ***1***, this will display the key settings window. There are three distinct groups to this window (Figure 38).

- ***Key Settings*.** This indicates the relevant sector, which as has been described in number 1. This is not a configurable parameter. A new key may be added in Edit Mode (Figure 39)
- ***Sector General Administration (configured)*.** This is an indication whether the sector has been enabled for general administration. This parameter is not used. Use the Auto Transmit after Reset Mode parameter to disable the Sector from transmitting after the next reset. See Section
- ***Sector General Status*.** This indicates the current status of the following parameters. These parameters are non-configurable:

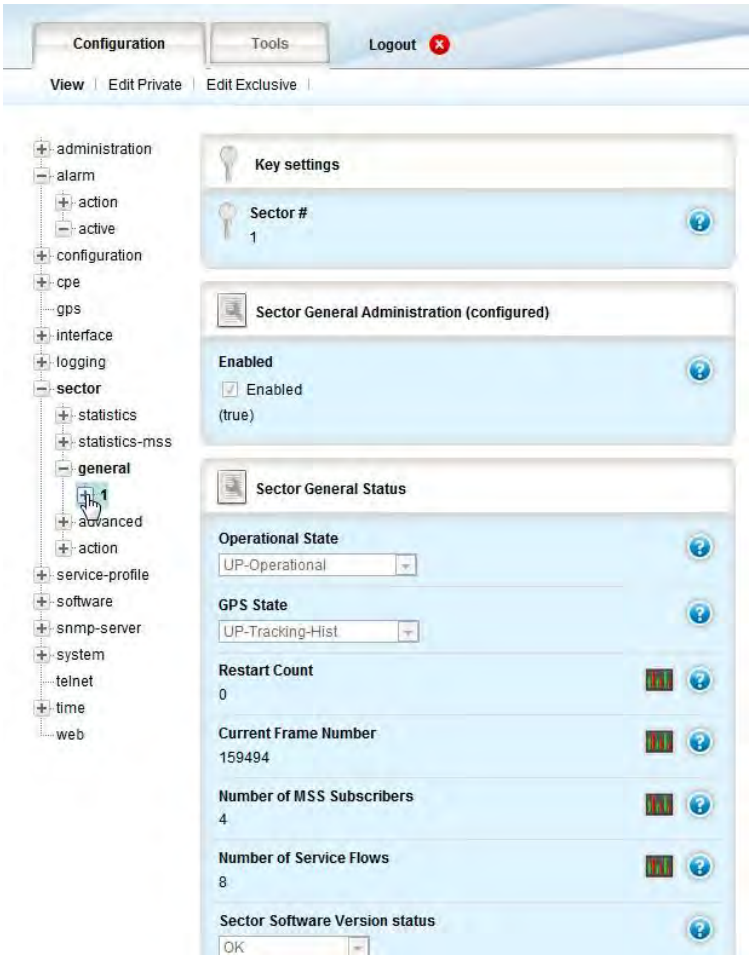


Figure 38 Sector General Options

The Key Settings are defined by the following parameters (Figure 39):

- ***Operational State*.** This indicates if the Sector is operational
- ***GPS State*.** This indicates the GPS status of the Sector.
- ***Restart Count*.** This is a cumulative count of the number of sector restarts since the Base Station was power cycled.
- ***Current Frame Number*.** Represents the count of WIMAX frames being allocated for transmission.

- ***Number of MSS Subscribers*.** This is a count of the current Subscribers that are connected to the sector.
- ***Number of Service Flows*.** This is a count of the total number of Subscriber service flows that are currently in use.
- ***Sector Software Version Status*.** Indicates the sector software version if there is a mismatch or if the sector is running from a recovery image.
- ***Running Software Version*.** This is the current running sector software version.
- ***Last Reset Reason*.** This provides a reason for the last sector reset.

Figure 39 Sector Key Settings

At the Main Web GUI Interface Screen select the *Configuration* Tab, select ***sector*** Main Menu Option, ***general*** Main Menu Sub-Element, ***1*** and then ***system***. This will display the currently configured Sector

General Provisioning window. There are a further two sub-elements to this window but only one is displayed.

These sub-elements are:

- ***system*.** This option enables the User to configure the parameters.
- ***state*.** This is a duplication of the windows and parameters that are contained within the system options. These are "read-only" screens and provide an indication as the current state or status of the system parameters.

The status of the following parameters is displayed, and the User is free to configure as required (refer to (Figure 40). To edit and configure then the User must enter the Edit Mode (select Edit Private/Exclusive):

- ***Base Station ID*.** This is the unique identifier that specifically identifies the Base Station to the Subscribers. It is recommended that this is changed to have a unique value in deployment. For inter-provider handover, please see the IEEE 802.16e guidelines.
- ***Cell ID*.** This is a numeric identifier that will define the cell (acceptable range is 0 to 31).

- ***Convergence Sublayer Type*.** This is the convergence sublayer type that is globally set for the sector. The available options are ETHERNET_CS and IPv4_CS. The default is ETHERNET_CS.
- ***Downlink Broadcast Rate*.** This is a User defined parameter that specifies the maximum \ Downlink (DL) rate in bits/second for the purposes of Ethernet Multicast, Ethernet Broadcast and IP broadcast traffic. This rate can be set up to 1Mbps and it uses QPSK ½ modulation rate over the air. This parameter is only valid when operating in stand-alone mode. The default is 64000.
- ***Block DHCP Downlink Broadcasts***. Selecting this option prevents rouge DHCP servers behind Subscriber Units from assigning IP addresses back to the network. This is primarily applicable for the Ethernet CS (Convergence Sublayer) mode of operation. By default this option is disabled.
- ***CPE to CPE Relaying (ETH CS)*.** If this option is enabled, it would allow all traffic to flow between the two CPEs without the need for the frames to be sent back to the backhaul side. This is applicable only in Ethernet CS stand-alone mode of operation. Only unicast and ARP broadcast frames will be relayed. This is useful for allowing two remote offices or locations to communicate. Please note that latency will be double on communications and the maximum capacity will be determined by the lowest of the uplink modulation rates between Subscriber Units.
- ***CPE to CPE All Broadcasts (ETH CS)***. If this option is enabled, it would allow *all* broadcast traffic to be relayed between the two CPEs. This is useful if the application requires Ethernet Broadcast frames other than ARP to be relayed. Examples include video broadcasting using IPTV. This is applicable only in Ethernet CS stand-alone mode of operation when *CPE to CPE relaying* is enabled.
- ***Downlink ARP Override*.** Downlink ARP Unicast packets are retransmitted as ARP broadcast packets.
- ***Mode*.** This is the Base Station Mode of network operation and the available options are:
    - standalone-local. Base Station operates in standalone mode where the users are local to the Base Station; CPE provisioning database is location and it is not connected to an ASN Gateway)
    - standalone-local-AAA. Base Station operates in standalone mode, uses AAA for provisioning of the CPEs and is not connected to an ASN Gateway. The AAA specifies the AC address of the CPE and the Client Profile ID that should be used by the CPE. The Client Profiles are configured in the Base Station and is must be maintained the same across all base station in a deployment served by the same AAA server
    - asn-gateway. ASN Gateway is used for all provisioning of the CPEs, there will be a GRE tunnel created between the Sector and the ASN Gateway and all data traffic will be sent out from the ASN Gateway (aggregator) and AAA provisioning

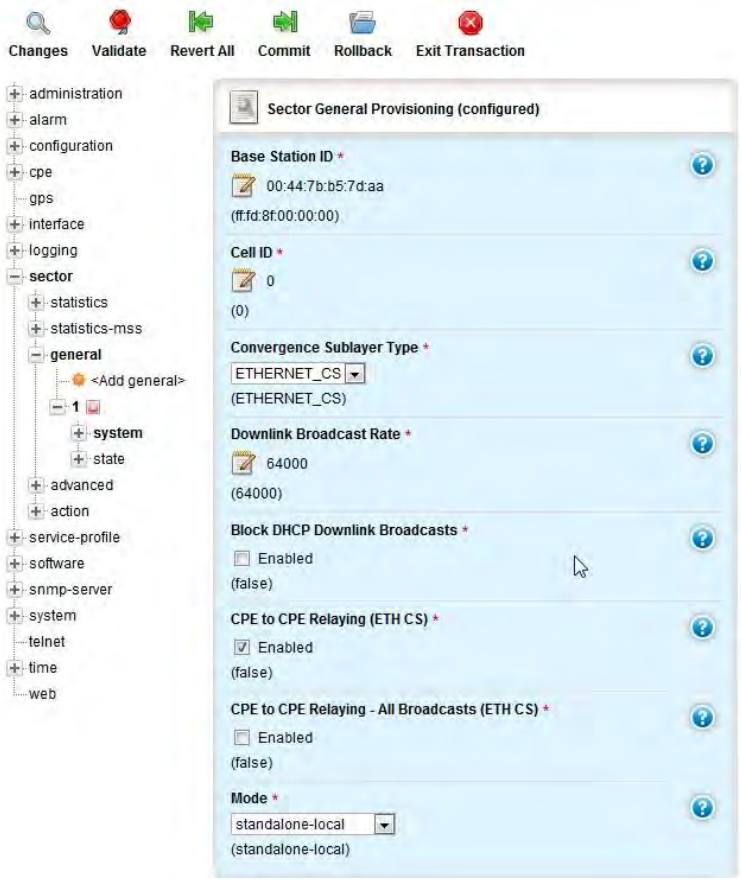


Figure 40 Sector General Provisioning Parameters

At the Main Web GUI Interface Screen select the *Configuration* Tab, select *sector* Main Menu Option, *general* Main Menu Sub-Element*, 1, system* and then *ip* and this will display the current configuration of the Sector External IP Address (Figure 41). This is a different IP address from the one configured on the Base Station and is recommended to be configured within the same IP subnet as the Base station IP pointing to the same default gateway. This IP address is used for:

- Generation of AAA Authentication requests (if sector security is enabled) when operating in Stand Alone mode.
- As the Source for all data traffic (towards the network) when operating in IP CS Stand Alone mode.
- As the GRE tunnel source for all data traffic when operating in ASN Gateway mode.

- ***Address*.** This is the IP address
- ***Netmask*.** This is the netmask associated with the IP address
- ***Gateway*.** This is the default gateway.

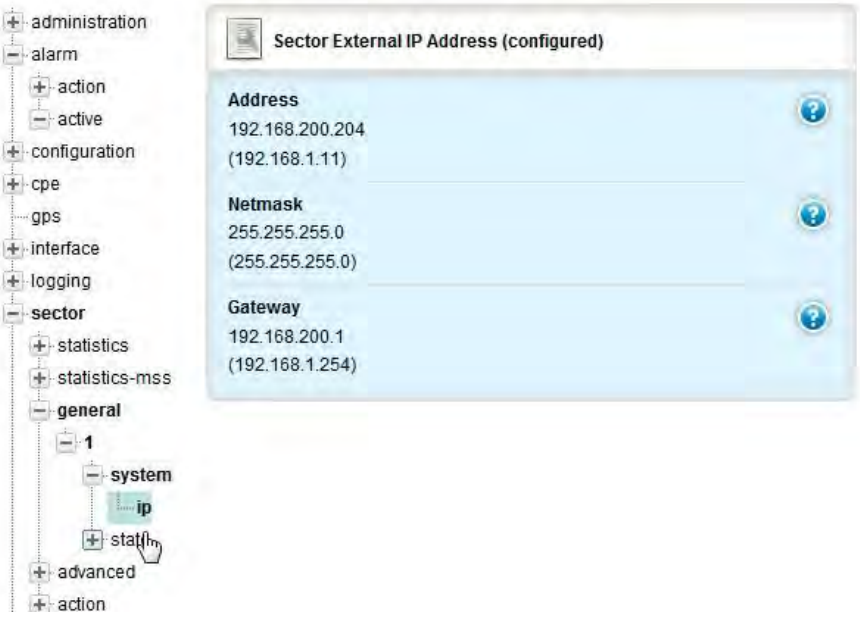


Figure 41 Sector External IP Address

To edit the parameter, the User must enter the Edit Mode (select Edit Private or Edit Exclusive). Once in the Edit Mode the User must select the notepad icon and this will provide an option to edit the IP address (Figure 42).

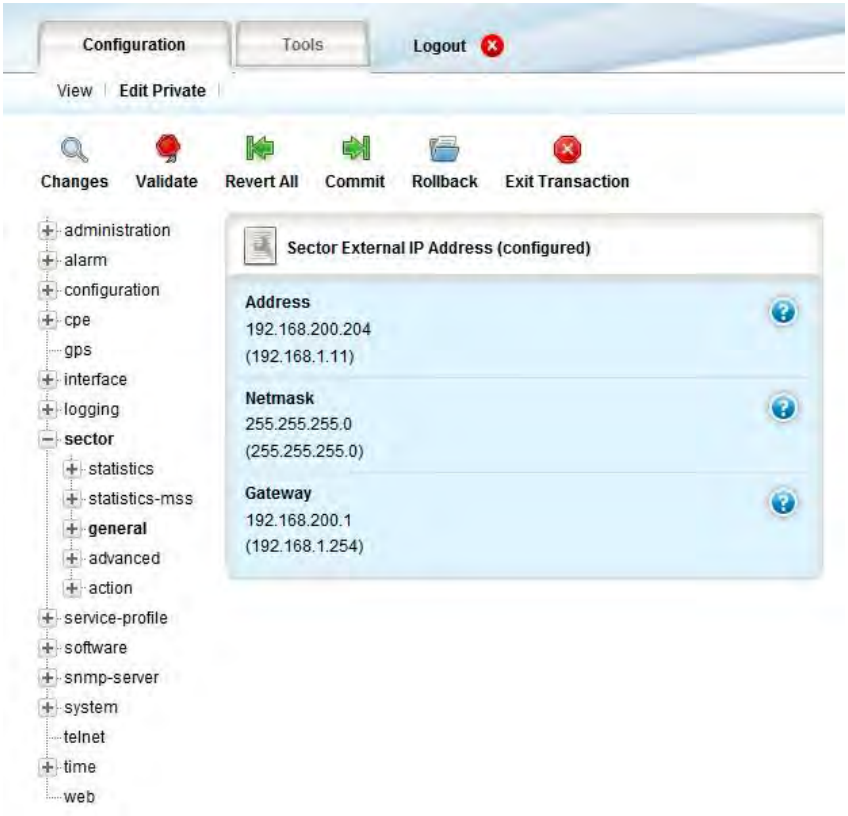


Figure 42 Sector External IP Address Configuration

At the Main Web GUI Interface Screen select the ***Configuration*** Tab, select ***sector*** Main Menu Option, ***general*** Main Menu Sub-Element***, 1, state*** and then ***system***. This provides another view that will display the current configuration of the Sector. Even if the User enters the Edit Mode (select Edit Private or Edit Exclusive), no parameters are made available for editing. The options to configure these parameters are contained under the ***system*** and then ***base station*** options. This shows the currently used parameters by the Sector. Configuration is performed at the system level (Figure 43 and Figure 44).

- *Sector External ASN-Gateway (state)*.
- *Management Vlan*
- *Sector General Provisioning*
- *Sector External Radius Server Settings*

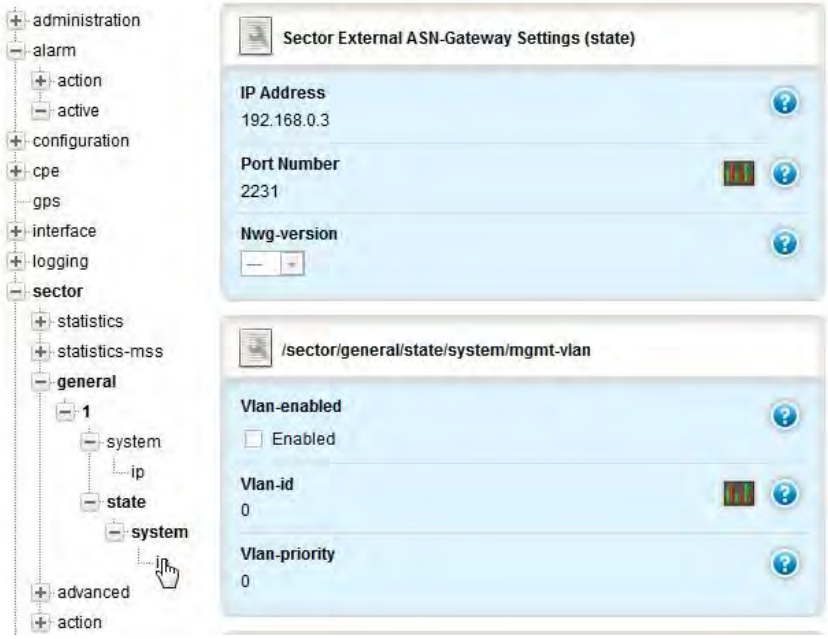


Figure 43 Management Vlan Settings (state)

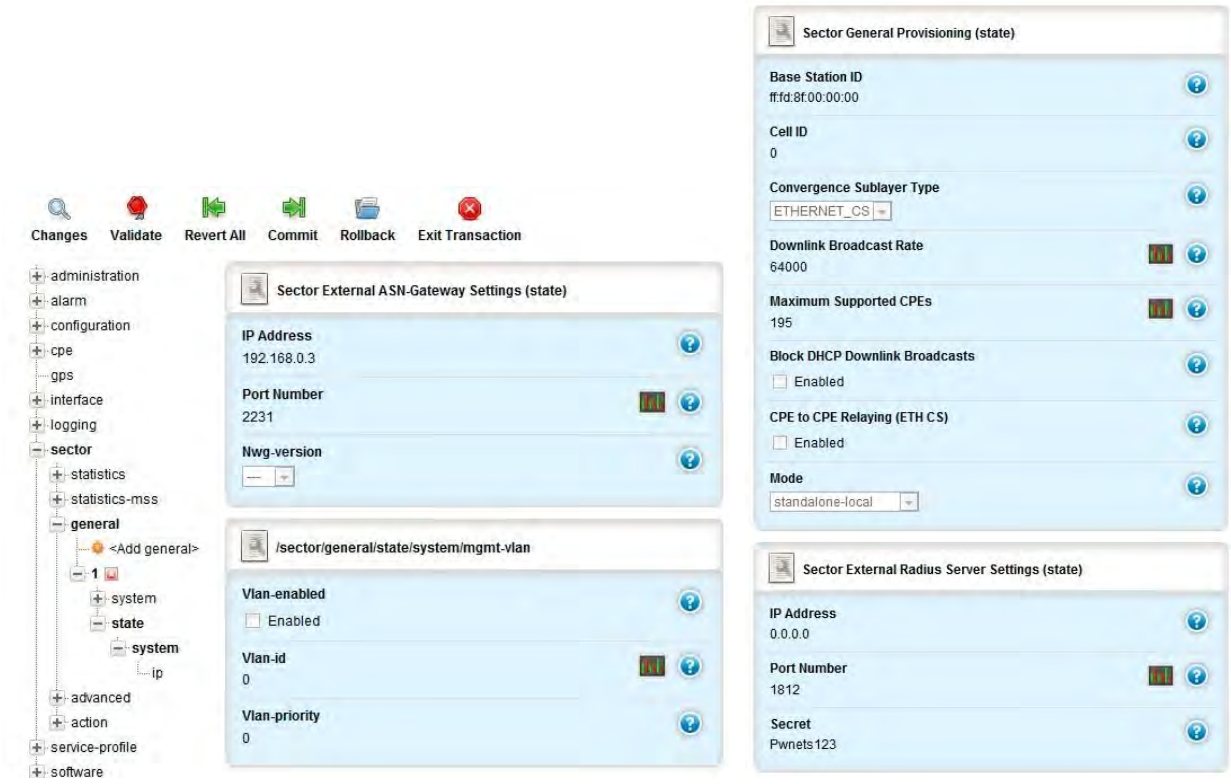


Figure 44 Sector General Provisioning and External Radius Server State

At the Main Web GUI Interface Screen select the ***Configuration*** Tab, select ***sector*** Main Menu Option, ***general*** Main Menu Sub-Element, ***1, state, system*** and then ***ip***. This provides another view that will display the current External IP Address of the Sector. Even if the User enters the Edit Mode (select Edit Private or Edit Exclusive), no parameters are made available for editing.

There following information is displayed in Figure 45.

- *Sector External IP Address*
- *Netmask*
- *Gateway*

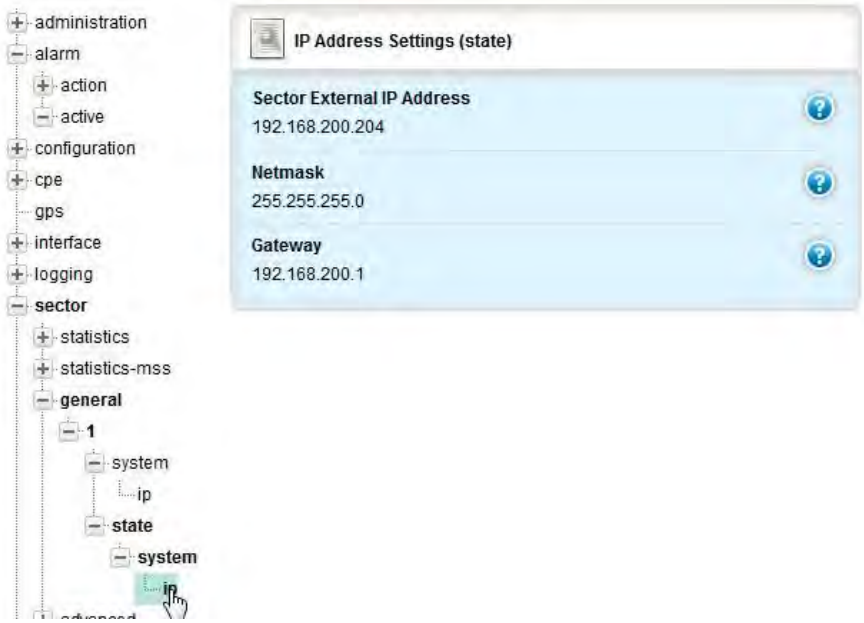


Figure 45 Sector External IP Address Settings (state)

3.5.3.2 Sector, Advanced Settings

At Main Web GUI Interface Screen select the *Configuration* Tab, select *sector* Main Menu Option, *advanced* Main Menu Sub-Element and then *1*, this will display the key settings window. There are two further sub-elements to this window but the information is only displayed when the actual element is selected. These further sub-elements are (refer to Figure 46):

- ***wimax*.** These are the parameters that can be configured as defined by the WiMAX 802.16e specification
- ***radio*.** These are the parameters that can be configured as part of the specific Base Station radio transmission configuration
- ***security.*** Parameters for the authorization key settings

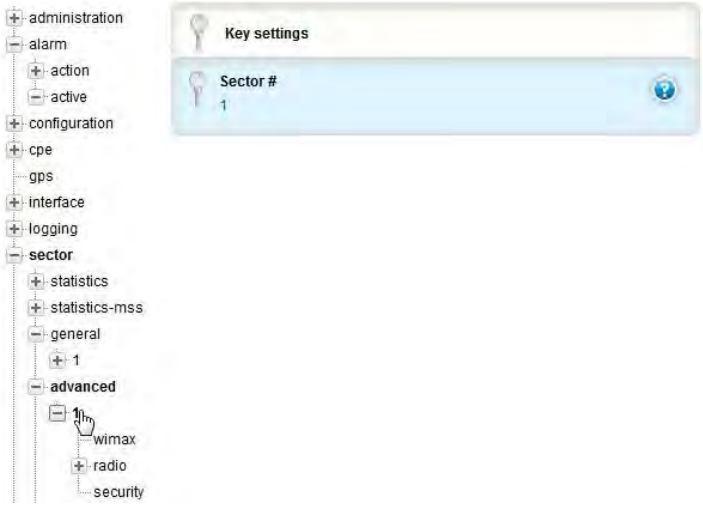


Figure 46 Sector Advanced Settings

To view the Sector WIMAX Settings, at the Main Web GUI Interface Screen select the *Configuration* Tab, select *sector* Main Menu Option, *advanced* Main Menu Sub-Element*, 1*, and then *wimax*. The display is split into two main sections. These sections do not fit onto one screen and therefore the User has to scroll down to view etc (refer to Figure 47 and Figure 48).

- ***Sector WIMAX Settings (configured).*** These are the parameters that the User can Edit
- ***Sector WIMAX Settings (state).*** These are the currently used configuration values of the parameters

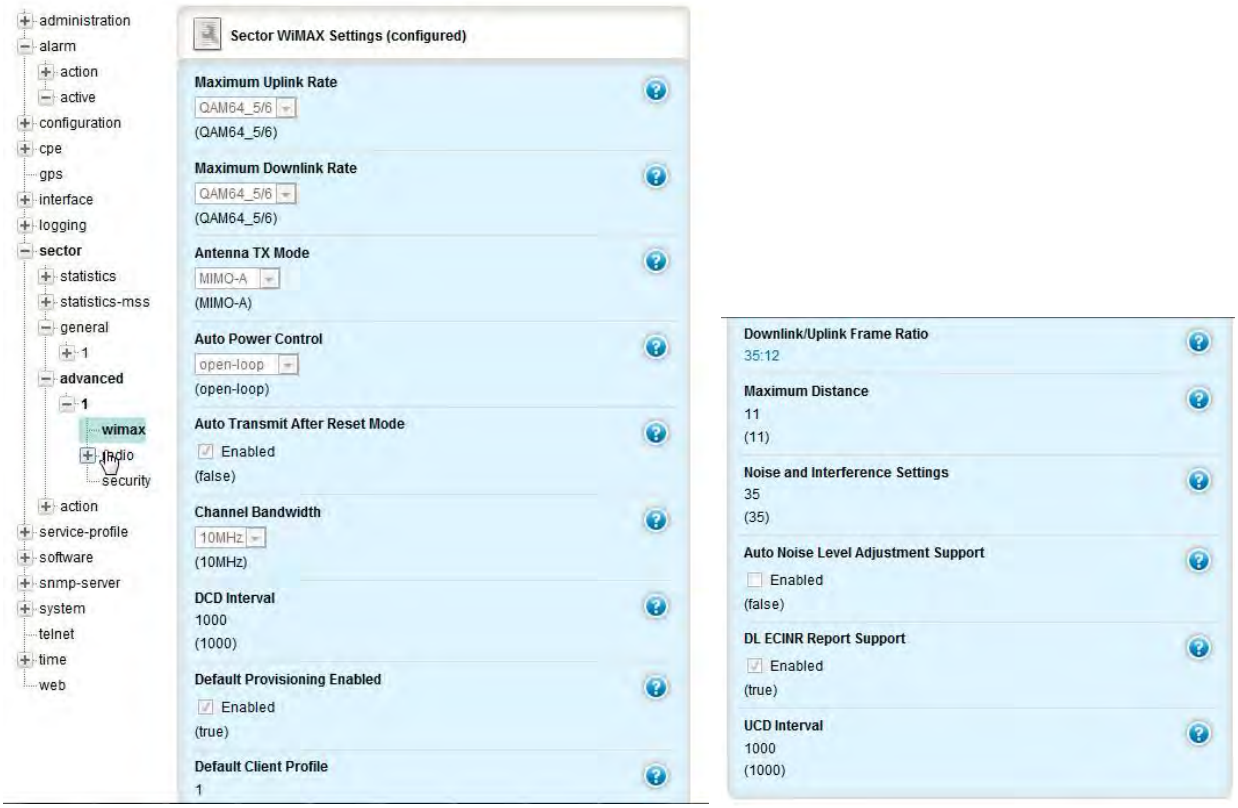


Figure 47 Sector WiMAX Settings (state)

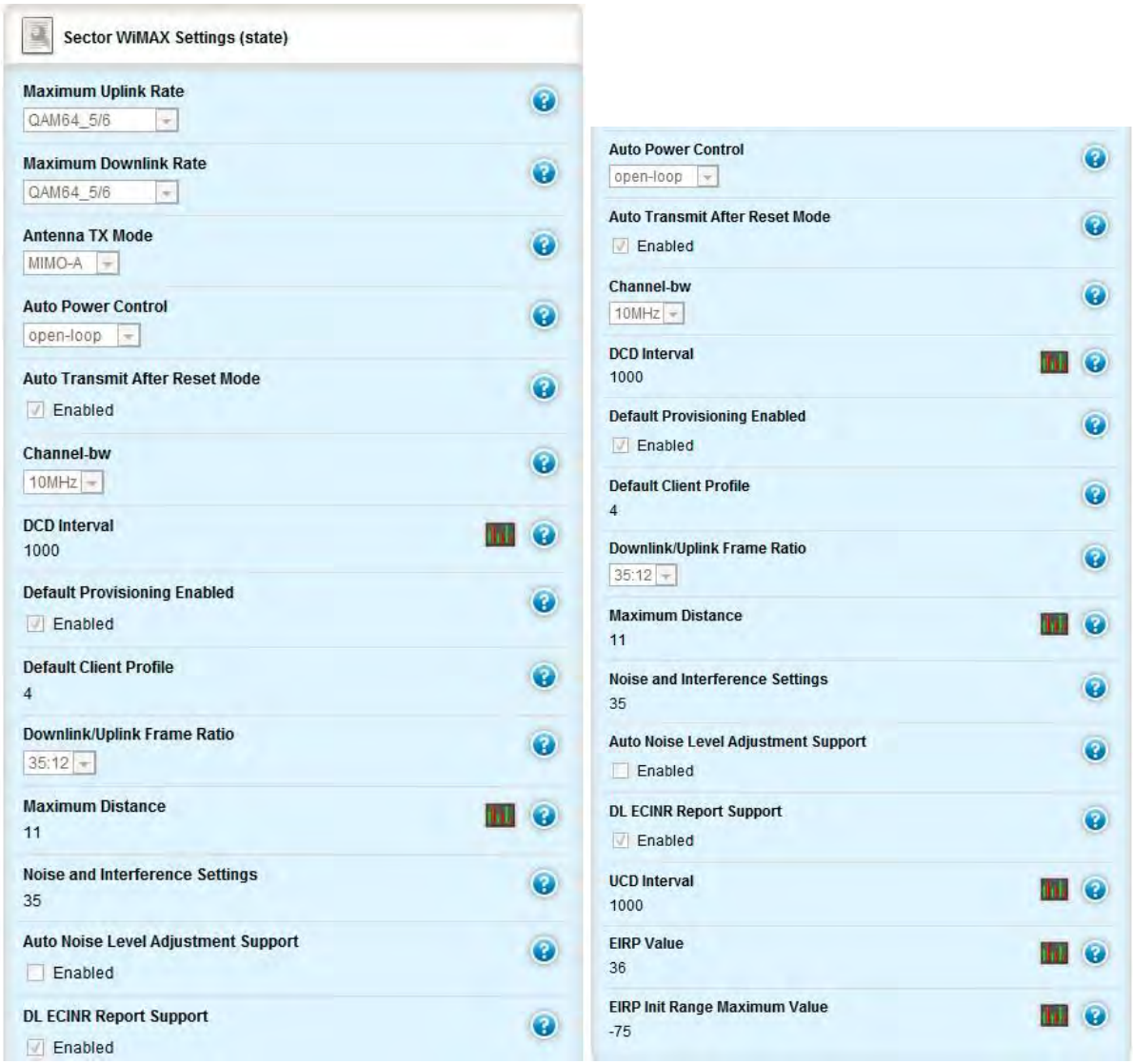


Figure 48 Sector State WiMAX Settings

If the User wants to configure any of the WiMAX parameters, then they must enter the Edit Mode (select Edit Private or Edit Exclusive) and edit as necessary. The methods to Edit the parameters will be offered via a drop-down menu of choices, enabling of a check box or editing of a notepad icon.

After making the various configuration changes, the User will need to "**Commit**" and "**Save**" the changes.

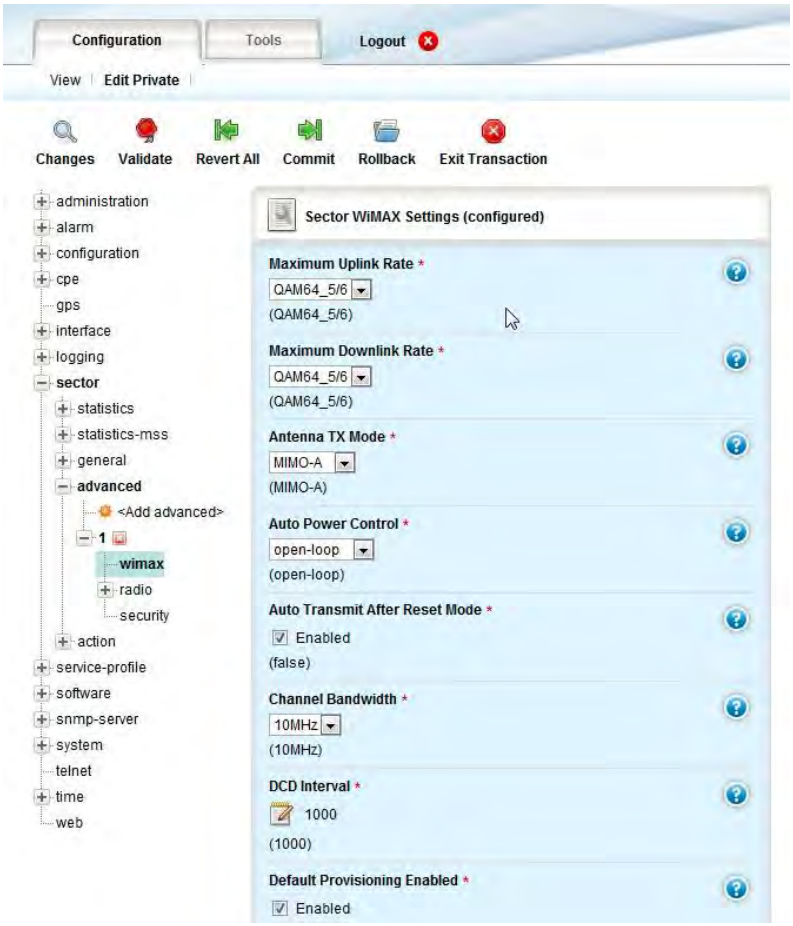


Figure 49 Sector WiMAX Settings Configuration

The Sector WIMAX Settings parameters that the User can configure are defined below:

- ***Maximum Uplink Rate*.** This parameter provides the means to globally fix the maximum modulation rate in the Uplink direction (defined as Subscriber to Base Station). If the User wants to dynamically adapt the rate to the maximum, then the default value of QAM64_5/6 can be left unchanged. Refer to Appendix A for an explanation of how the maximum modulation rate, defined as MCS Rate, effectively caps the system data throughput. If the User wants to physically cap the rate and hence cap the throughput, they are free to select from the following MCS rates:
    - QAM64_5/6
    - QAM64_3/4
    - QAM64_2/3
    - QAM64_1/2
    - QAM16_3/4
    - QAM16_1/2
    - QPSK_3/4
    - QPSK_1/2

- ***Maximum Downlink Rate*.** This parameter provides the means to globally fix the maximum modulation rate in the Downlink direction (defined as Base Station to Subscriber). The default is QAM64_5/6 and the same options as maximum uplink rate parameter are available.
- ***Antenna TX Mode*.** This the option to define the Smart Antenna Capabilities that were described in section 2.3.2.3. The default setting is MIMO-A and the available options are:
    - MIMO-AB
    - MIMO-A. In MIMO-AB mode, if the Subscriber Unit indicates that the channel conditions allow the operation of MIMO-B (usually in high multipath conditions with very strong downlink signal and CINR) the Base station will dynamically assign the CPE to operate in MIMO-B mode doubling the capacity on the downlink direction.
- ***Auto Power Control*.** The transmit power of a Subscriber is controlled via automatic algorithms in the Base Station. This control of the transmit power ensures optimum performance. The default is open-loop and the available options are:
    - open-loop. In the case of an open loop algorithm, the Base Station sends a signal to the Subscriber of the required settings and the Subscriber adjusts its transmit power dynamically.
    - closed-loop. In the case of closed loop, the Base Station controls the Subscriber transmit power settings with a full measurements loop.
- ***Auto Transmit After Reset Mode*.** When this is enabled the Base Station will automatically start transmitting upon a power cycle. If this is disabled, then the User will have to manually start the transmission. By default, this is disabled. The user needs to enable this after connecting the antenna, setting the frequency and TX power level.
- ***Channel Bandwidth*.** This is the current channel bandwidth of the radio transmission. The default is 10MHz and the options are:
    - 10MHz
    - 7MHz
    - 5MHz
    - 3.5MHz
- ***DCD Interval*.** This is the internal with which WiMAX 802.16e DCD messages are transmitted and is defined in milliseconds. The default is 1000 (1 second) and the available range is 15 up to 10000.
- ***Default Provisioning Enabled*.** The user has the choice to enable or disable this feature. If this is enabled, then any non-explicitly provisioned CPE will be assigned the *Default Client Profile*. If this is disabled and the CPE is not explicitly provisioned, the CPE will remain wirelessly connected but will not be assigned any data service flows which will cause no data traffic to pass through.
- ***Downlink/Uplink Frame Ratio*.** This is the ratio of downlink to uplink frame symbols, refer to Appendix A and how this affects data throughput. The default option is 35:12.
- ***Maximum Distance*.** This is the maximum distance, defined in km, that a CPE can communicate with a Base Station. The default is set to 11Km and the user can select in the range 1 to 58Km. Increasing the value above 11km will lower the maximum achievable downlink performance. Configuring a distance greater than 28Km will cause a donut effect, where the area of coverage will be between the outer and inner radius. The outer radius will be the maximum distance configured and the inner radius will be the maximum distance

configured minus 28. Example 1: If the Maximum distance is set to 13Km, the area of coverage will be between the Base Station up to 13Km. Example 2: If the Maximum distance is set to 44Km, the area of coverage will be between 16Km and 44Km. We recommend configuring this value appropriately such that the desired area is covered. When applying the change, a popup will appear and you will be required to commit (Figure 50).

- ***Noise and Interference Settings*.** The default is 35. NI is defined as per the IEEE 802.16-e as the noise per tone in 0.5 db steps above the -150 dBm, where 0 is -150dbm and 35 is -132.5dbm per tone. This value represents the noise level per tone at the receiver of the Base station which gets advertised and is used by the CPEs to determine their uplink TX power when operating in open loop power control.
- ***Auto Noise Level Adjustment Support.*** Enables the automatic dynamic adjustment of NI and internal settings with respect to the measured noise level on the channel. The Noise measurement values can be seen in the radio tab.
- **DL ECINR Report Support.** Specifies the mode of CINR reporting to be provided from the CPEs. Default is enabled (ECINR). Disabling CINR reporting should be done only in case of older CPE revisions that do not support ECINR reporting.
- ***UCD Interval*.** This is WiMAX 802.16e UCD Interval value and it is to be defined in milliseconds. Interval defined in milliseconds. The default is 1000 (1 second) and the available range is 15 up to 10000.
- ***5MHz Large Map Support*** – Available and applicable only in case of 5MHz channel bandwidth setting. Extends the MAP size and supports larger number of bursts per frame. Recommended to be enabled in case of large number of CPEs and when using combined data + voice.

To view the Radio Settings, at the Main Web GUI Interface Screen select the *Configuration* Tab, select *sector* Main Menu Option, *advanced* Main Menu Sub-Element*, 1*, and then *radio*. The display is split into three main grouping sections. These sections do not fit onto one screen and therefore the User must scroll down to view etc (refer to Figure 51 and Figure 52).

- ***Radio Settings (configured)*.** These are the parameters that the User can Edit
- ***Radio Settings (state)*.** These are the current configurations values of the parameters
- ***Noise and Interference Measurements (status).*** These are the current configurations values of the parameters. The Noise level is represented in 3 different measurement units

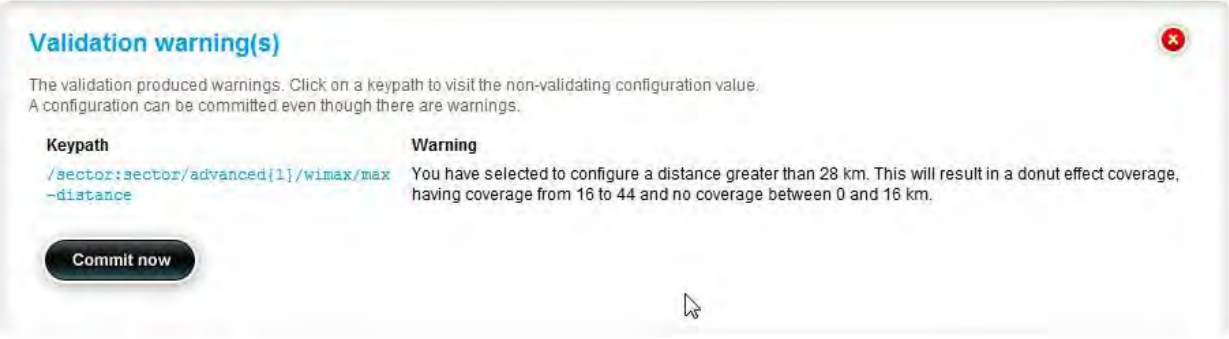


Figure 50 Distance Setting Warning Pop-up

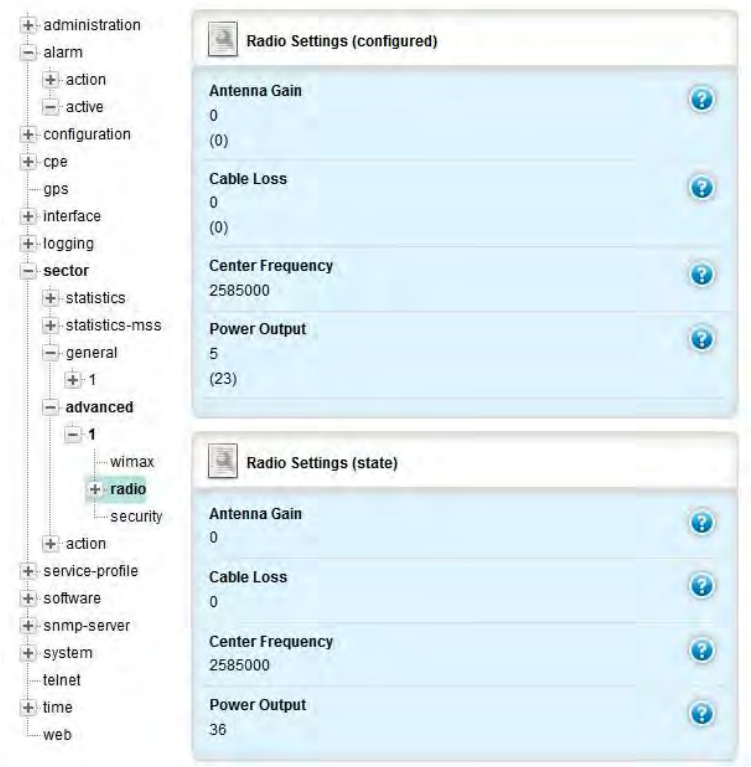


Figure 51 Sector Radio Configured Settings

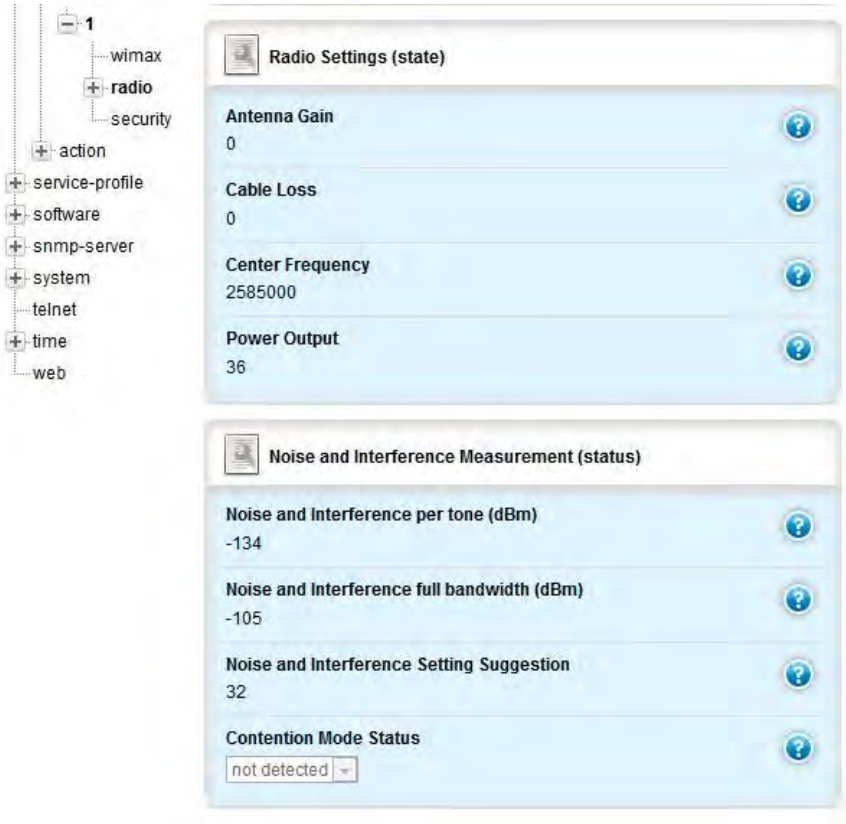


Figure 52 Sector Radio State Settings

If the User wants to configure any of the Radio parameters, then they must enter the Edit Mode (select Edit Private or Edit Exclusive) and edit as necessary. The methods to edit the parameters will be offered via editing of a notepad icon (Figure 53).

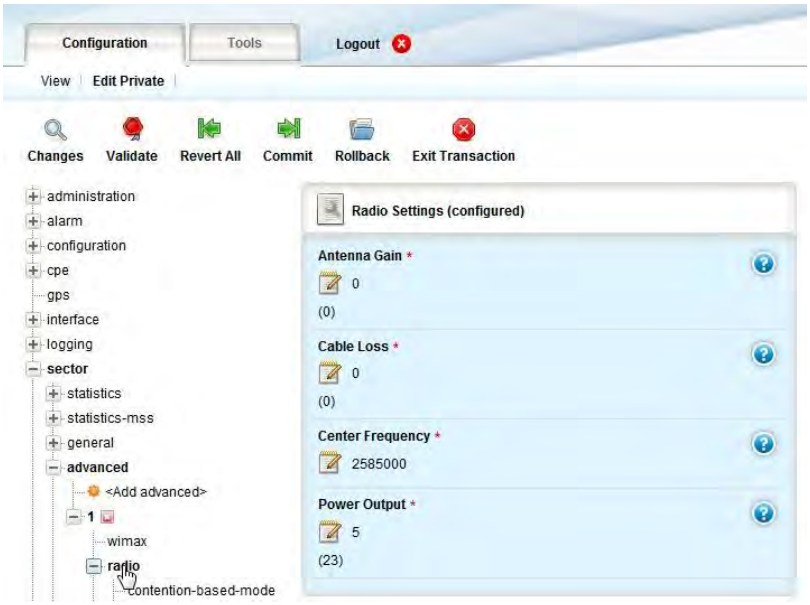


Figure 53 Sector Radio Settings Configuration

After making the various configuration changes, the User will need to "Commit" and "Save" the changes.

The Radio Settings parameters that the User can configure are defined below:

- *Antenna Gain*. This is the gain (in dB) for the Antenna that the Base Station is connected to. The default setting is 0, however this should be set exactly as the antenna that is used. Setting an incorrect value may cause the degraded performance.
- *Cable Loss*. This is a loss of the cable (in dB's) from the Base Station to the Antenna. The default setting is 0 but needs to be set according to the loss of the cable used. Setting an incorrect value may cause the degraded performance.
- *Center Frequency*. This is the center frequency of the Base Station and it must match with what is configured on the Subscribers. The default setting is relative to the frequency range of operation of the Base Station. To re-configure, the center frequency has to be input in KHz.
- *Power Output*. This is the radio output power in dBm. The default setting is relative to the frequency range of operation of the Base Station. The User must ensure that the maximum output power is defined as described in section 2.3.2.2.

Contention Based Mode must be enabled on the Radios to support the upper 25 MHz of the 3.65 GHz US band. The diagram below provides an example of utilizing part of the upper 25 MHz for a 7 MHz channel width. In this case Contention-Based Mode must be enabled. To utilize WiMAX Contention Based Mode, at the Main Web GUI Interface Screen select the ***Configuration*** Tab, select *sector* Main Menu Option, ***advanced*** Main Menu Sub-Element, ***1***, and then ***radio*** and contention-based mode. The display is split into two grouping sections. These sections do not fit onto one screen and therefore the User must scroll down to view etc. (Figure 54).

- ***Mode (enable/disable).*** Allows the feature to be enabled or disabled
- ***Carrier Sense Threshold.*** Set to -85.0 dBm by default. Any signals detected beyond this threshold will be ignored
- ***Carrier BackOff Frame.*** Number of frames to wait for transmission when an interfering carrier is detected
- ***Carrier Sense Resume Frame.*** Number of frames to resume listening when an interfering carrier is detected. Default is 752.

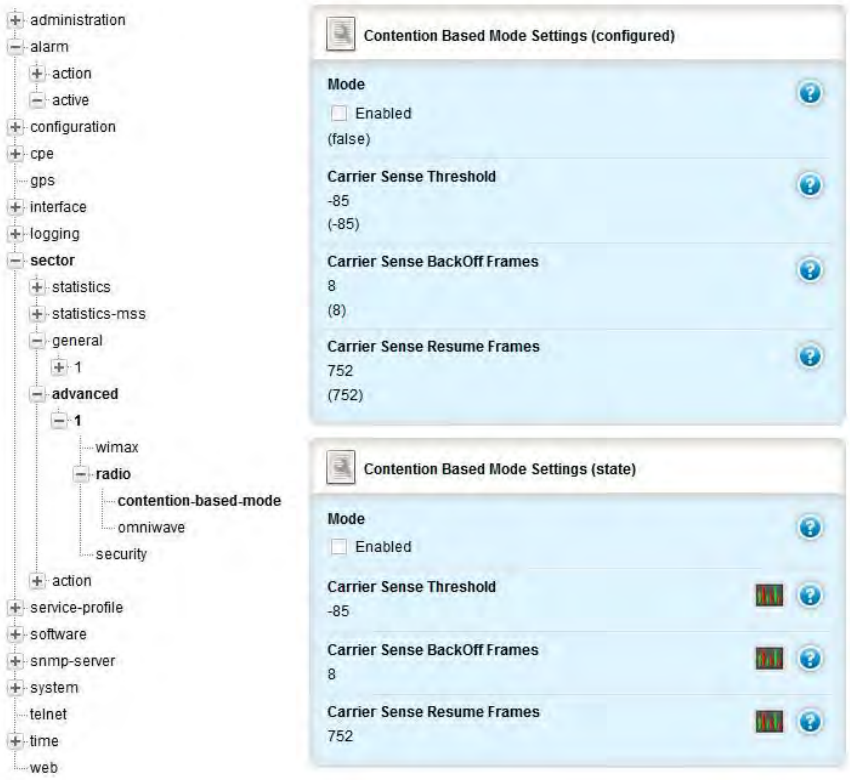


Figure 54 Contention Based Mode

Omniwave may be enabled on the radio level to support a 3x2x2 configuration. To utilize Omniwave, at the Main Web GUI Interface Screen select the ***Configuration*** Tab, select ***sector*** Main Menu Option, ***advanced*** Main Menu Sub-Element*, 1*, and then ***radio*** and omniwave.

- ***Mode (enable/disable).*** Allows the feature to be enabled or disabled
- ***Status.*** Current configuration (enabled or disabled)

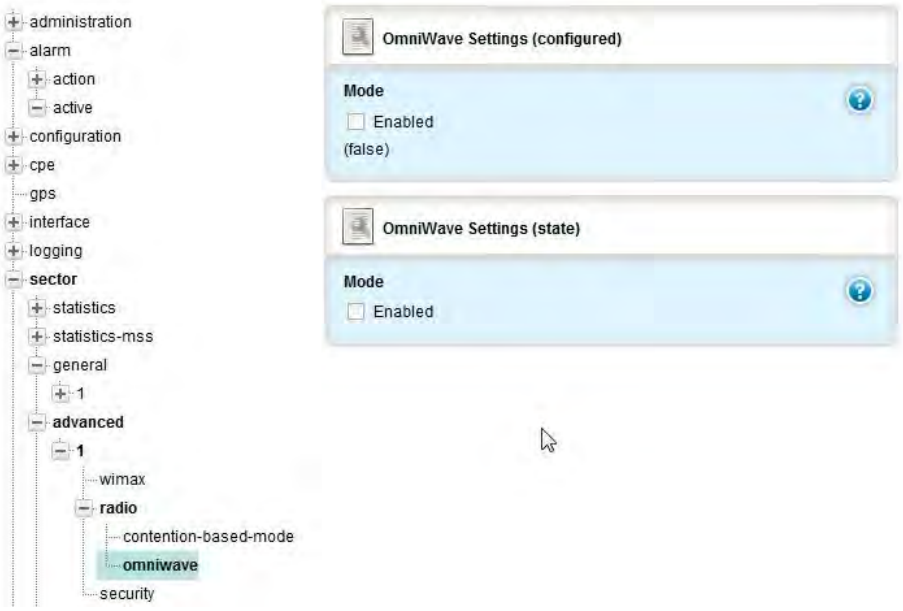


Figure 55 OmniWave Settings

To view the Security Settings, at the Main Web GUI Interface Screen select the ***Configuration*** Tab, select ***sector*** Main Menu Option, ***advanced*** Main Menu Sub-Element***, 1***, and then ***security***. The display is split into two main grouping sections (Figure 56).

- ***Security Settings (configured).*** These are the parameters that the User can Edit.
- ***Security Settings (state).*** These are the current configurations values of the parameters.

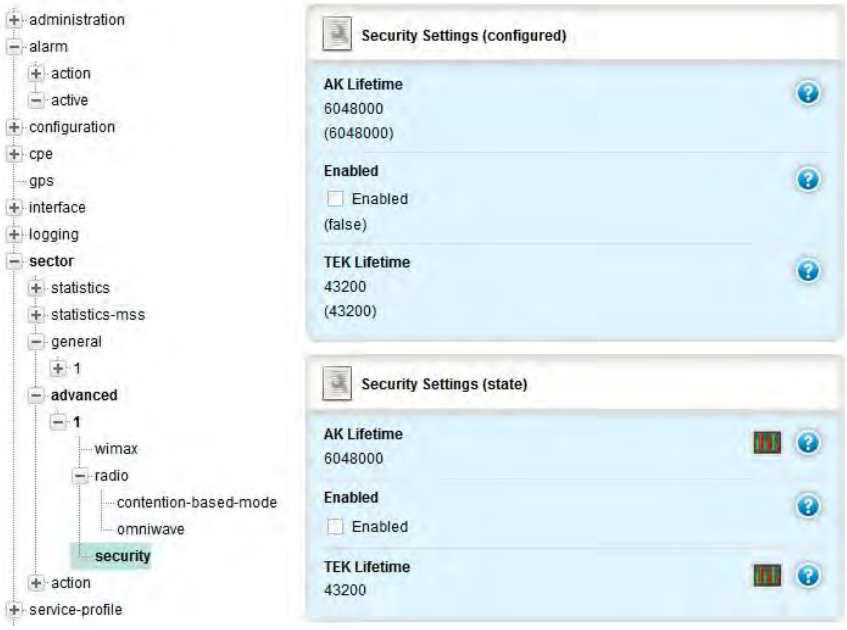


Figure 56 Sector Security Settings

If the User wants to configure any of the Security parameters, then they must enter the Edit Mode (select Edit Private or Edit Exclusive) and edit as necessary. The methods to Edit the parameters will be offered via an enabling of a check box or editing of a notepad icon (Figure 57).

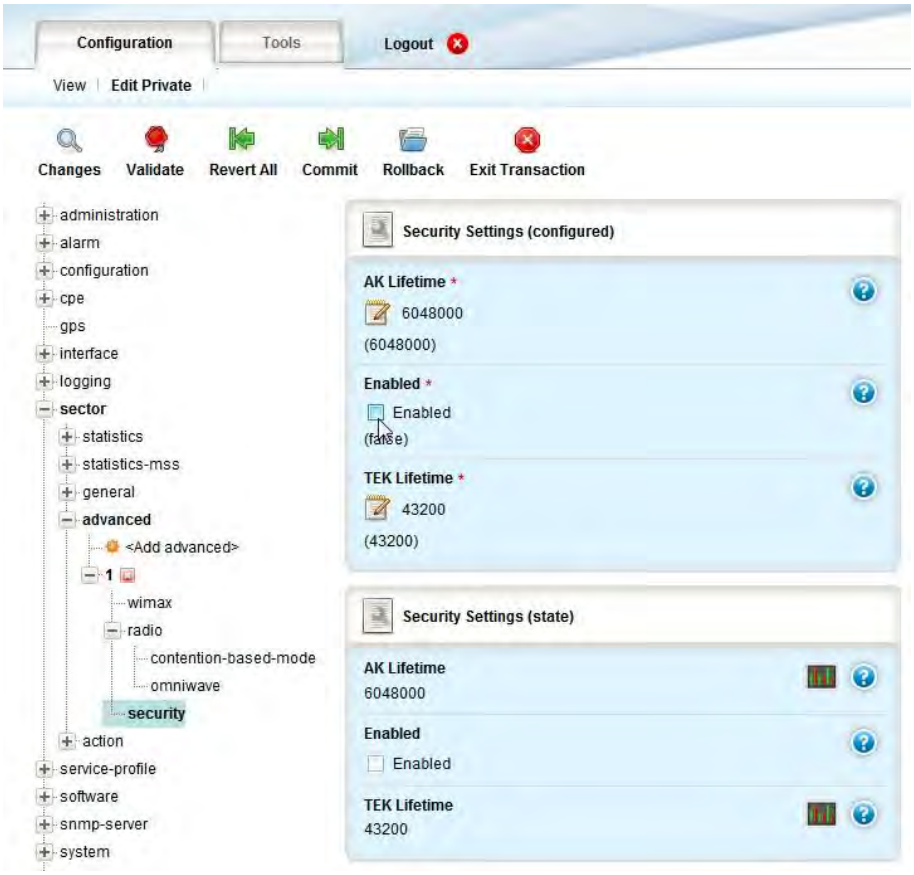


Figure 57 Sector Security Settings Configuration

After making the various configuration changes, the User will need to "Commit" and "Save" the changes.

The Security Settings parameters that the User can configure are defined below:

- ***AK Lifetime*.** This stands for Authorization Key lifetime. It is used when authentication and encryption is enabled. The key is periodically re-generated by the Base Station after a request is received from a Subscriber following expiration of this timeout. The default setting is 6048000 and it is not recommended to change this value.
- ***Enabled*.** This indicates whether the Security Feature has been enabled or not.
- ***TEK Lifetime*.** This stands for Traffic Encryption Key lifetime. The key is used when authentication and encryption is enabled. It is periodically re-generated by the Base Station after a request is received from a Subscriber following expiration of this timeout. It is not recommended to change the default value.

To view the Action Options, at the Main Web GUI Interface Screen select the ***Configuration*** Tab, select ***sector*** Main Menu Option and the *action* Main Menu Sub Element and ***Key Index 1***.

The action options are as follows:

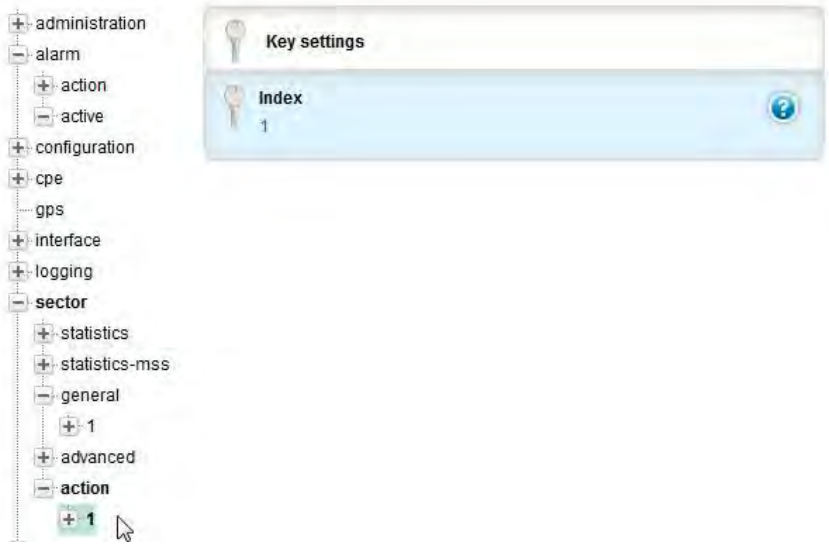


Figure 58 Sector Action Menu

- ***Subscriber Station.*** Allows user to perform abort ranging, deregister or reset on a CPE
- ***Reboot*.** Will perform a reboot of the entire sector
- ***Start Noise Measurement*.** Will put the sector in a special mode to measure noise and interference
- ***Start Radio Transmit*.** Will revert the sector back in the radio transmit mode

Figure 59 Abort Ranging Request

To perform the Subscriber-Station (or CPE) Action Options, at the Main Web GUI Interface Screen select the ***Configuration*** Tab, select ***sector*** Main Menu Option and the *action* Main Menu Sub-Element and ***Key Index 1*** followed by ***subscriber-station*** and one of the options below:

- ***abort.*** Specify a CPE via its MAC Address. Hit Perform and the current ranging operation will cease, and the CPE will attempt to re-enter the network. Refer to Figure 60.
- ***deregister*.** Specify a CPE via its MAC Address. Hit Perform and the current CPE will be deregistered from the sector. Refer to Figure 61.
- ***reset*.** Will put the sector in a special mode to measure noise and interference (Figure 61)

Figure 60 De-register CPE

Figure 61 Reset CPE Action

To perform the Sector Action Options, at the Main Web GUI Interface Screen select the ***Configuration*** Tab, select *sector* Main Menu Option and the ***action*** Main Menu Sub Element and ***Key Index 1*** followed by ***subscriber-station*** and one of the options below:

Figure 62 Reboot Sector Action

- ***Reboot.*** Hit Perform and the current sector will be rebooted (Figure 62)
- ***Start-Noise Measurement*.** Hit Perform and the action will put the sector in a special mode to measure noise and interference (Figure 63), results will be available after a short time
- ***Start-radio-transmit*.** Will put the sector in a special mode to measure noise and interference (Figure 64)

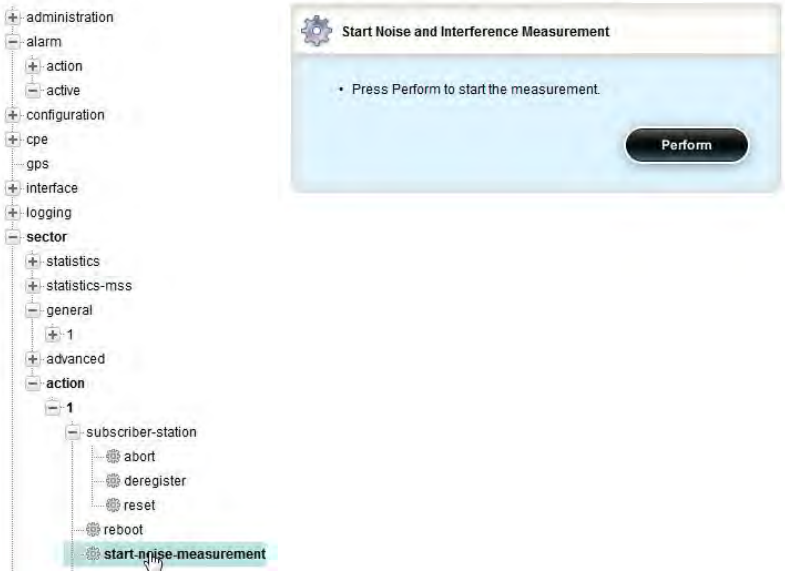


Figure 63 Start Noise Measurement

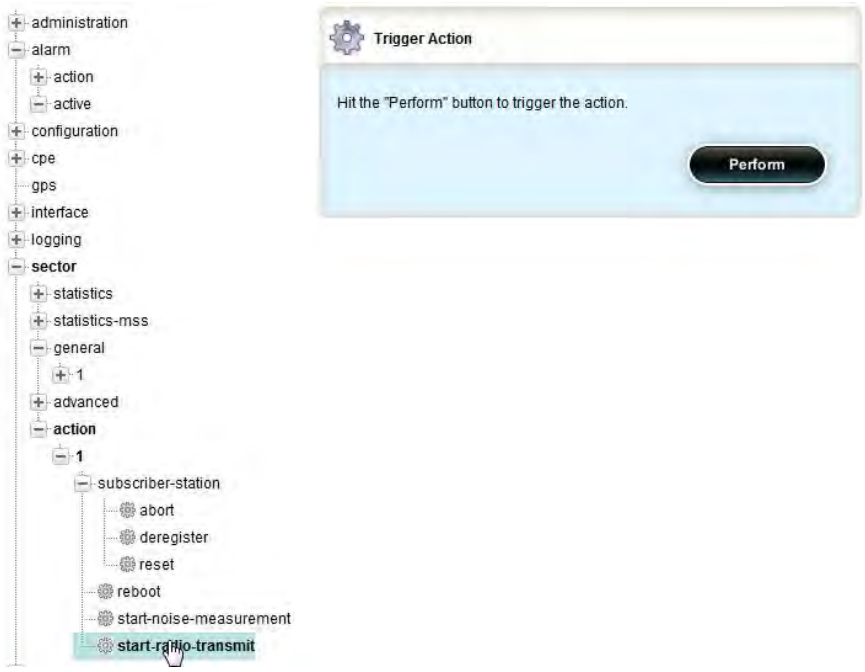


Figure 64 Radio Transmit Sector Action

3.5.3.3 System Settings

At the Main Web GUI Interface Screen select the ***Configuration*** Tab and then select ***system*** Main Menu Option. This will display the System Settings window. The system menu option has three further sub elements, these being (Figure 65):

- ***Base-Station*.** This details various Base Station parameters
- ***Reset*.** This is a means for the User to default the Base Station back to its "out of the box" initial configuration values or default configurations
- ***Interface*.**

Figure 65 System Settings

The System display is split into seven main grouping sections. These sections do not fit onto one screen and therefore the User must scroll down to view etc. An indication as to whether there are any User configurable parameters included in the grouping is provided. If the User wants to configure any of the parameters, then they must enter the Edit Mode (select Edit Private or Edit Exclusive) and edit as necessary. The methods to Edit the parameters will be offered via a drop-down menu of choices, an enabling of a check box or editing of a notepad icon.

The parameters that the User can configure and the relevant grouping section that they belong to are outlined below. After making the various configuration changes, the User will need to "**Commit**" and "**Save**" the changes.

- ***System Console Settings*** (Figure 66)
  - ***Baudrate.*** This is the baud rate that is configured for serial connection via the Base Station Console Port. The default is 38400 and the available options are 115200, 57600, 38400, 19200 and 9600.
- ***System Miscellaneous Settings***
  - ***Hostname.*** This is a free format text field for the User to specify a hostname.
  - ***Led-enabled.*** The User can enable or disable the LED indicators for the Base Station.

- ***System General Settings***
  - ***Name.*** This is a free format text field for the User to specify a name to the Base Station.
  - ***Location.*** This is a free format text field for the User to specify a location to the Base Station.
  - ***Contact.*** This is a free format text field for the User to specify a contact for the Base Station.
  - ***Uptime.***

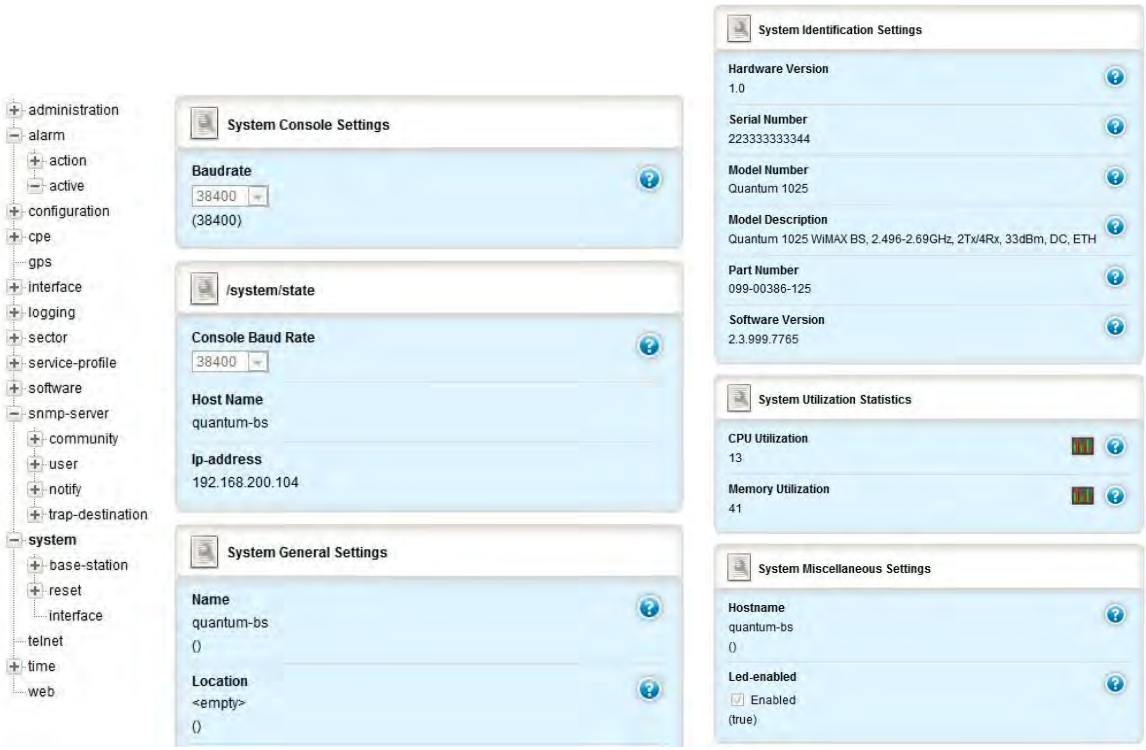


Figure 66 System Console Settings

At the Main Web GUI Interface Screen select the ***Configuration*** Tab, select ***system*** Main Menu Option and then the ***base-station*** Main Menu Sub-Element. This will display the External ASN-Gateway Settings window (Figure 67).

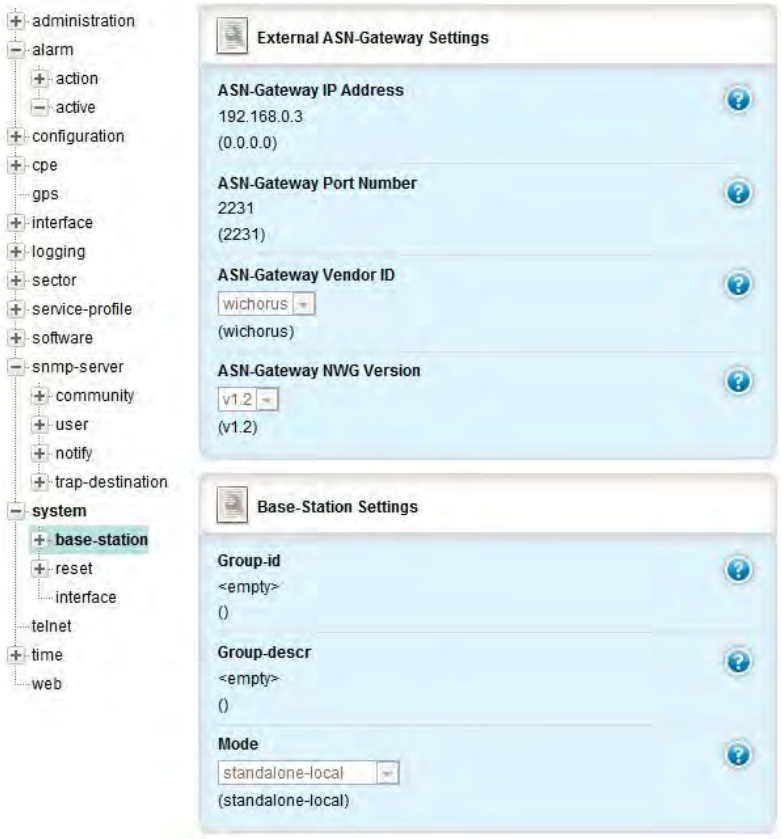


Figure 67 System External ASN Gateway Settings

The System display is split into several grouping sections. These sections do not fit onto one screen and therefore the User must scroll down to view etc. An indication as to whether there are any User configurable parameters included in the grouping is provided. If the User wants to configure any of the parameters, then they must enter the Edit Mode (select Edit Private or Edit Exclusive) and edit as necessary. The methods to Edit the parameters will be offered via a drop-down menu of choices or editing of a notepad icon.

- ***External ASN-Gateway Settings****.* These are the settings for any external ASN Gateway that is connected to the Base Station.
- ***Base-Station Settings****.* These are the settings for the Base Station.
- ***External Radius Server Settings****.* These are the settings for the external Radius Server, if configured.

The parameters that the User can configure and the relevant grouping section that they belong are outlined below. After making the various configuration changes, the User will need to "**Commit**" and "**Save**" the changes.

- ***External ASN-Gateway Settings.***
  - ***ASN-Gateway IP Address.*** This is the IP address of the ASN Gateway that the Base Station is connected to. An IP address has to be provided if the Base Station has been configured to operate in ASN Gateway mode.

- ***ASN-Gateway Port Number.*** This is the Port Number that the Base Station use to communicate with the ASN Gateway.
- ***ASN-Gateway Vendor ID***. This User has the option to select and store the vendor of the ASN Gateway. The current options are Wichorus and Cisco.
- ***ASN-Gateway NWG Version.*** This User has the option to select and store the protocol used to communicate with the ASN Gateway. The current options are v1.2 and v1.3.

- ***Base-Station Settings***
  - ***Group-id.*** This is a free format text field.
  - ***Group-descr.*** This is a free format text field.
  - **Mode.** This defines the mode of operation for the Base Station. The default option is standalone-local, and the available options are asngateway and standalone-AAA-prov.
- ***External Radius Server Settings*** **(Figure 69)**
  - ***Radius Server IP Address.*** This is the IP Address of the AAA server used for authentication/encryption purposes and provisioning when set to local-AAA provisioning. Applicable only in case of Stand-Alone Mode.
  - ***Radius Server Port Number***. This is the Port Number that the Base Station use to **communicate with the Radius Server.** Applicable only in standalone mode.
  - *Secret*. This is the radius "secret" that is shared between the Base Station and the Radius Server.
  - ***AAA Provision Realm.*** This is an optional parameter that can be used in case the base station operates in standalone-AAA-prov mode, where the base station will append the specified realm on every provisioning request to the server. This can simplify the configuration on the AAA side in cases where the MAC Address of the CPE is already used for authentication purposes.

    Default is empty, which means that the AAA provisioning request will contain only the MAC Address of the CPE.

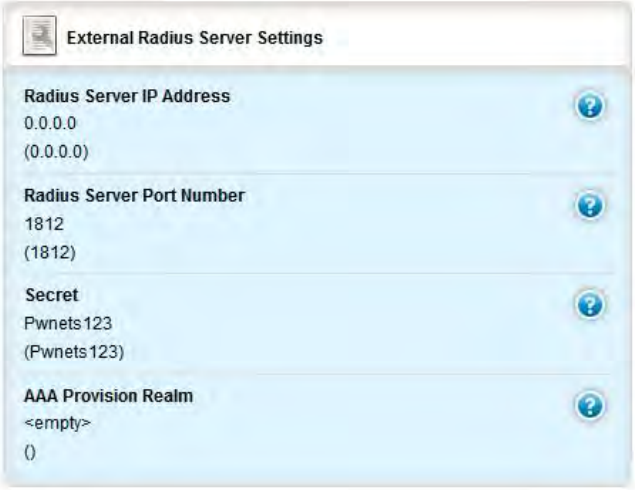


Figure 68 External Radius Server Settings

The system, base-station menu option has two further sub-elements, ***handover***, ***neighbor*** and ***wimax learning***.

- ***handover.*** This is where triggers are set for handover operation. By default, there are no triggers. For handover operation at least two triggers must be set, one for scanning and one for handover. This information is incorporated into DCD message sent by the base station. This may be left unconfigured if no handover is desired. For each trigger following needs to be configured (Figure 70):
    - **Trigger Index**: A user defined unique number between 1-8.
    - **Average Duration**: Trigger averaging duration is the time measured in number of frames over which the metric measurements are averaged.
    - **Trigger Type**: This defines trigger metric, CINR or RSSI
    - **Trigger Function**: This parameter specifies the function for the trigger type chosen earlier. Select one from the dropdown menu.
    - **Trigger Action**: This parameter specifies the action, scanning (MOB_SCAN_REQ) or handover (RSP_MOB_MSHO_REQ), to take when trigger criteria is met. Select from the dropdown menu.
    - **Trigger Value**: This parameter specifies the value for corresponding to the trigger type and function selected above.

Figure 69 Base Station Handover

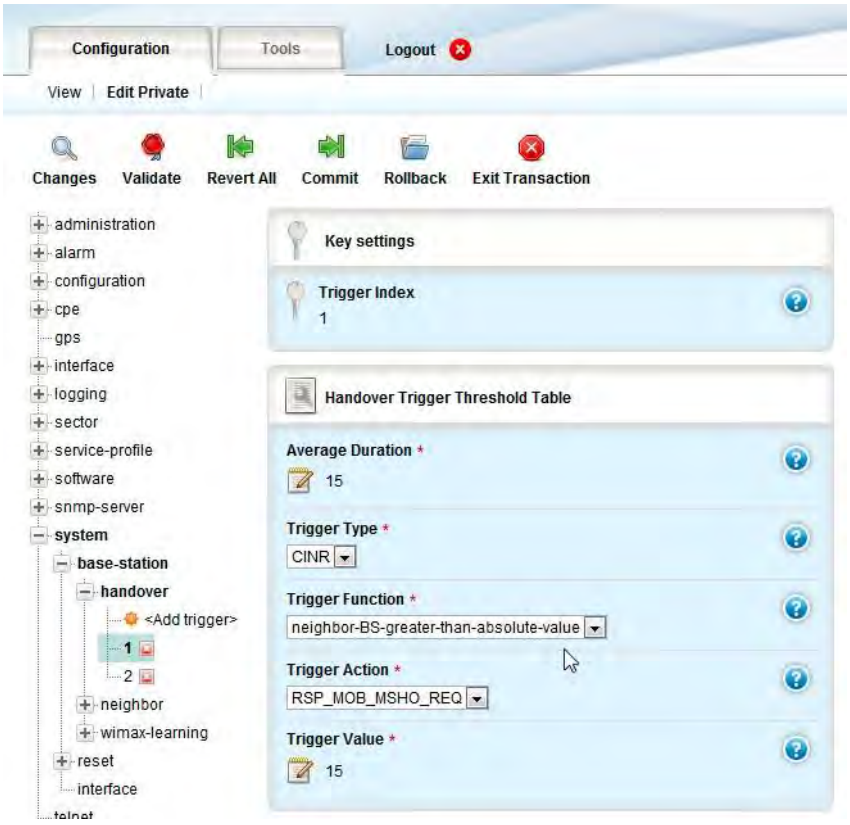


Figure 70 System Handover Trigger Setting

- ***Neighbor.*** This is the place to configure information about neighbor Base Stations (Figure 71). This is required for handover operation. The neighbor list is specified in Figure 72. This can be left unconfigured if no handover is required. For each neighbor, the following needs to be configured:
    - **BS id**: This is the BSID of neighbor bs. Use upper case letters only. BSID of the neighboring base stations should have same operator id as the serving base station, i.e. the upper 6 bytes should be same.
    - **IP Address**: This is the IP address of the neighbor base station.
    - **Preamble Index**: This is the preamble-index (or Cell-ID parameter) of the neighbor base station.
    - **BS Index**: This is a user defined number in the range of 1-254. The index of 255 has a special meaning. When this index is set to 255 then the neighbor will be considered as a non-Mercury base station, and Mercury base station will unconditionally accept the handover request. No backbone communication will take place.
    - **BS Frequency**: This is the frequency of the neighbor base station in KHz.

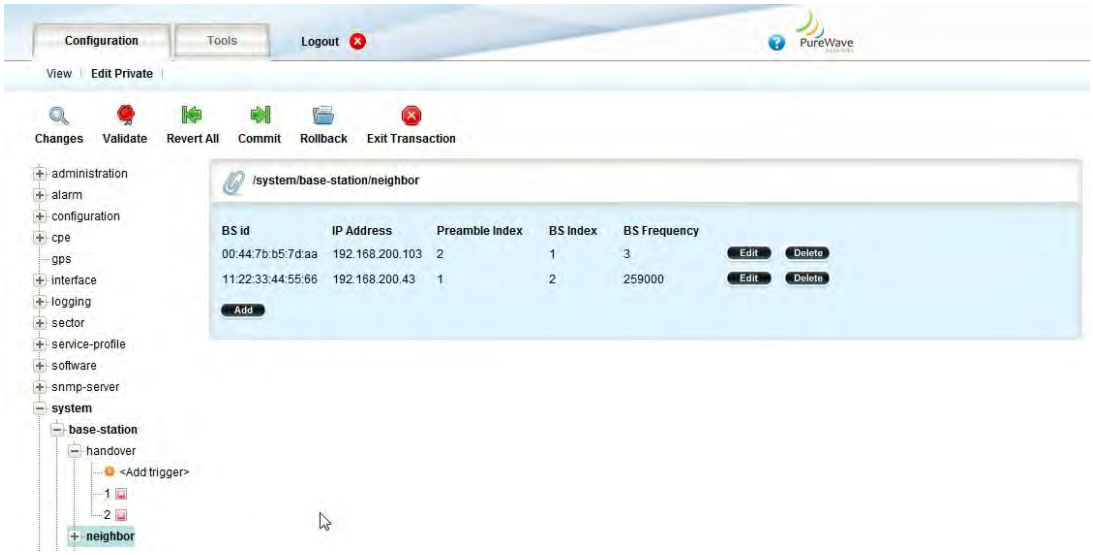


Figure 71 Base Station Neighbor Settings

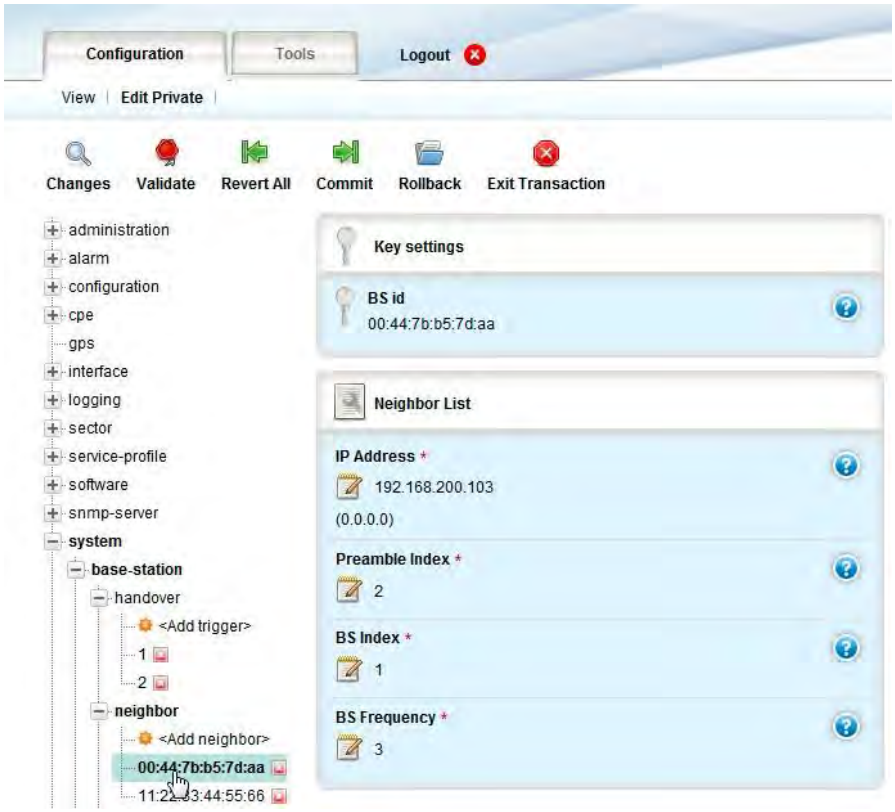


Figure 72 Base Station Neighbor List

- ***Wimax learning***. This learning table indicates the devices on the wireless side and their association with a CPE.

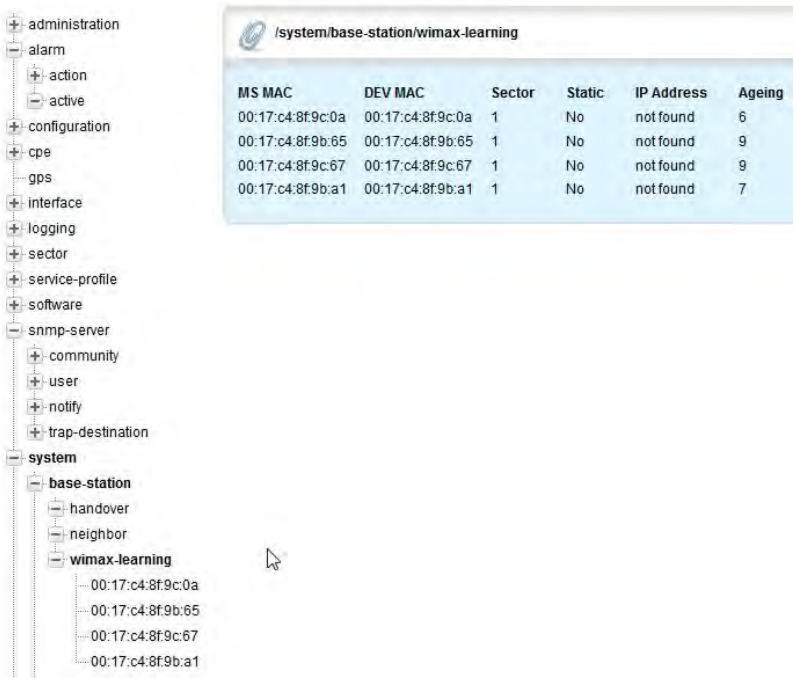


Figure 73 WiMAX Learning Table

The parameters in the learning table are as follows:

- *Sector*. Represents the Sector ID on which the device was learned. For Quantum 6600 this is always 1.
- *MAC*. Mac Address of the device learned in the bridge learning table
- *DEV MAC*. The MAC Address of the device(s) behind the CPE. This will be the MAC address of the mobile station (MS) if it operates in NAT Mode or is USB type. There can be up to 10 MAC addresses behind a CPE if the Base Station operates in Bridge Mode – Stand Alone. In case the Base Station operates in IP CS – Stand Alone mode the MAC address will always be the one of the MS. Each IP should be displayed as a separate entry.
- *IP Address*. The IP Addresses of the devices behind the CPE. This is relevant only in case the base station operates in IP CS Stand Alone mode. In other cases, this will not return any value. In case the CPE operates in NAT/Router mode or is of USB type this will be usually a single entry with the IP Address.
- *Static*. If the entry is manually provisioned or if the IP Address was obtained through DHCP Server. This is relevant only for IP CS Stand Alone mode.
- *Ageing*. Represent the time in seconds of the device since the last frame was received originating with the matching source MAC Address. Aging is not applicable to IP CS Stand along mode, where there is IP Address learned – No Ageing.

3.5.3.4 Resetting System to Factory Defaults

There are two options to reset the system back to default configuration

- ***defaultConfiguration***: clears the configuration but *retains* the IP addresses and Management VLAN configuration.
- ***factoryDefault***: restores the system back to factory defaults including IP addresses.

At the Main Web GUI Interface Screen select the ***Configuration*** Tab, select ***system*** Main Menu Option, ***reset*** Main Menu Sub-Element and then ***defaultConfiguration*** OR ***factoryDefault***. This provides the User with a reset system to factory defaults option (Figure 74). The User must select ***Perform*** Command Menu Option to erase the startup configuration and reboot the system. Afterwards the system will come up with the factory default configuration.

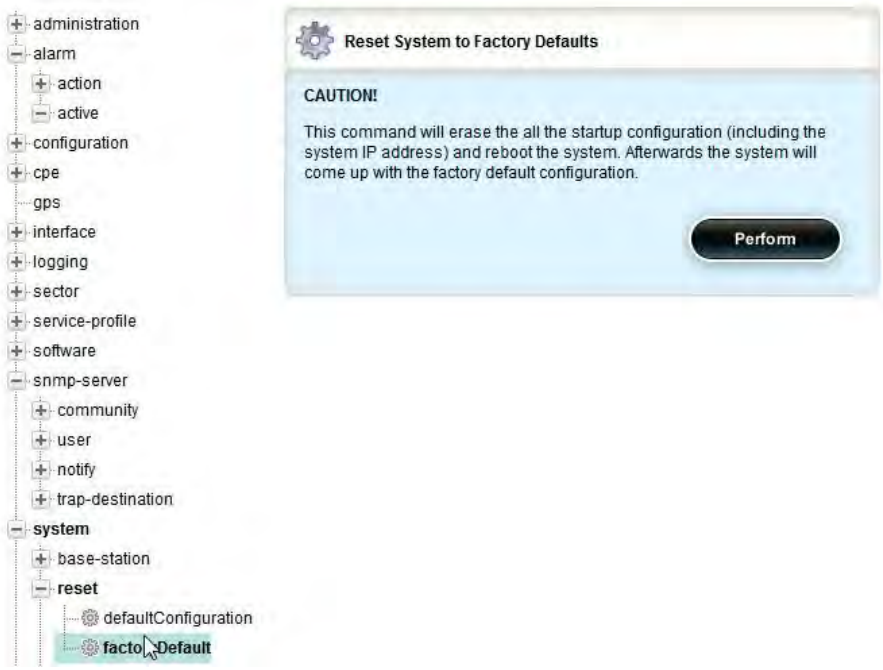


Figure 74 System Reset to Default Option

3.5.3.5 Resetting Interface to Factory Defaults

At the Main Web GUI Interface Screen select the ***Configuration*** Tab, select ***system*** Main Menu Option, ***reset*** Main Menu Sub-Element and then ***interface***. This provides the User with the options to configure the System Management Static IP Address and Management VLAN (Figure 75). If the User wants to configure any of the parameters, then they must enter the Edit Mode (select Edit Private or Edit Exclusive) and edit as necessary. The methods to Edit the parameters will be offered via editing of a notepad icon.

The parameters to configure for the Base Station Static Management IP Address are:

- *Address*
- *Netmask*
- *Default Gateway*
- *VLAN Enabled*
- *VLAN ID*
- *VLAN Priority*

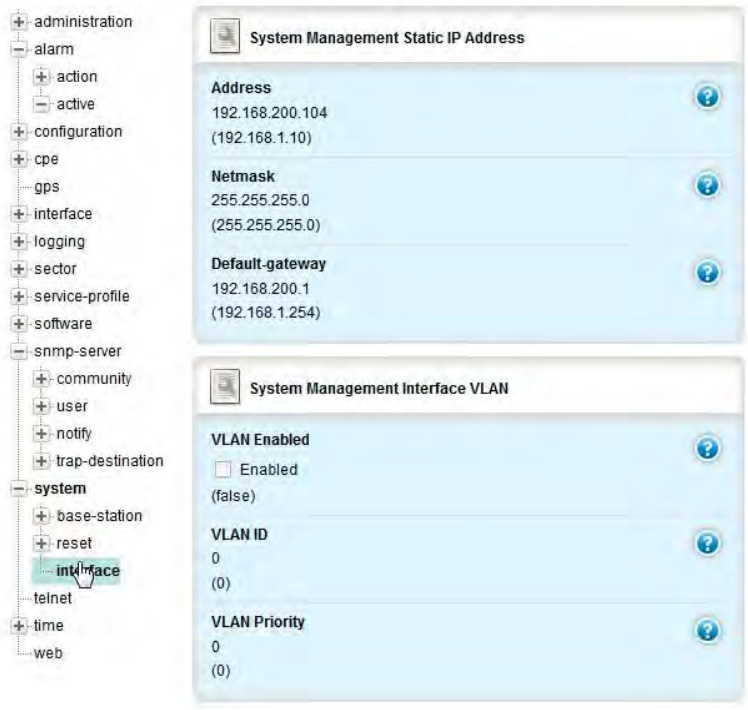


Figure 75 System Management Static IP Address and VLAN

3.5.3.6 GPS Settings

The use of a GPS for air frame synchronization is mandatory if more than one Base Station is installed in a geographical area where potential radio transmissions could interfere with one another. GPS is enabled or disabled via the ***GPS*** option.

At the Main Web GUI Interface Screen select the *Configuration* Tab and then select the ***gps*** Main Menu Option. This will display the GPS Settings and Status window (Figure 76). The ***gps*** Main Menu Option has no further sub-elements.

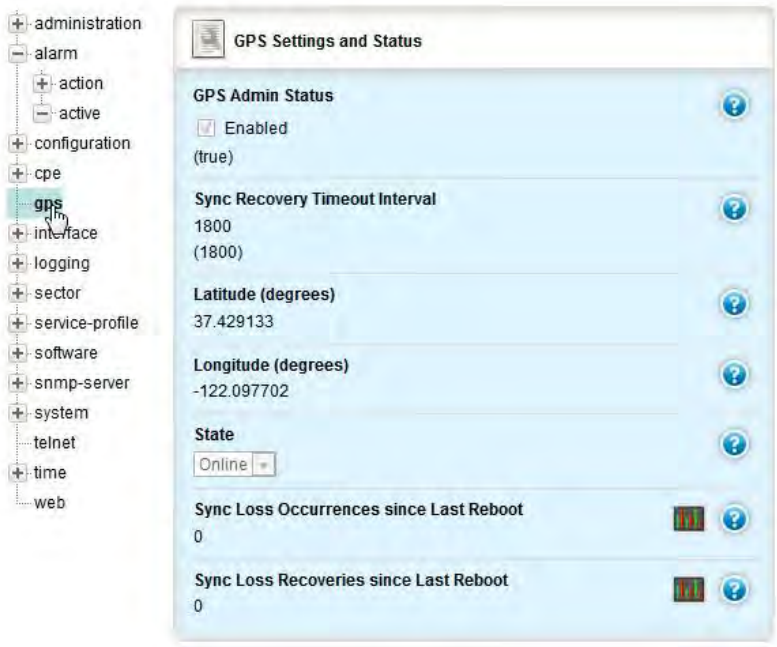


Figure 76 GPS Settings and Configuration

The GPS Settings display is split into one main group sections. An indication as to whether there are any User configurable parameters included in the group is provided. If the User wants to configure any of the parameters, then they must enter the Edit Mode (select Edit Private or Edit Exclusive) and edit as necessary. The methods to Edit the parameters will be offered via an enabling of a check box or editing of a notepad icon.

⚠	A GPS antenna MUST be connected to the Base Station before setting GPS Admin Status to “Enabled”

The GPS Settings and Status window contains:

GPS Admin Status. This is an indication of the GPS Admin Status. The options are enabled and disabled with disabled as the default.

- ***Sync Recovery Timeout Interval***. The Base Station has a Sync Recovery feature, whereby the Base Station Radio is automatically reset if GPS sync is lost for more than a specified timeout period. The timeout period (in seconds) is specified via the *Sync Recovery Timeout Interval* parameter. The default value is 1800 seconds.
- ***Latitude (degrees)***. This is the latitude location of the GPS receiver. This is not a User configurable parameter.
- ***Longitude (degrees)***. This is the longitude location of the GPS receiver. This is not a User configurable parameter.
- ***State***. This is an indication of the state of the GPS receiver. This is not a User configurable parameter.

- ***Sync Loss Occurrences since Last Reboot***. This is a cumulative count of the number of GPS sync losses since the Base Station was last reset. This is not a User configurable parameter.
- ***Sync Loss Recoveries since Last Reboot***. This is a cumulative count of the number of GPS sync recoveries since the Base Station was last reset. This is not a User configurable parameter.

The GPS will be in one of the states below from startup and until it is operational and providing synchronization to the base station.

- ***Offline***. The 1 PPS from the satellite signal is not detected, so basic synch lock has not occurred. This can be also seen as there should not be any coordinates if the GPS is "offline"
- ***INIT***: GPS state which dictates whether the BASE STATION will start transmission if the GPS is enabled.
    - ***INIT-Initializing***
    - ***INIT-Tracking-1-OSO***
    - ***INIT-Tracking-2-STO-Init***
    - ***INIT-Tracking-3-STO-Start***
- ***UP:*** GPS is operational (up).
    - ***UP-Tracking-Done***. Base Station will begin transmission
    - ***UP-Tracking-Hist***. Last GPS state indicating a steady state.
    - ***UP-Holdoff***
    - ***UP-ReAcquire***
    - ***UP-Retrack***
- ***DOWN***: GPS is not operational (down).
    - ***DOWN-Unreliable***
    - ***DOWN-Recovery***

3.5.3.7 Time Settings

It is important that the Base Station maintain an accurate date and time so that system logs are aligned and may be correlated with other network activity and trouble reports. Although the date and time must be initially set by the user, the Base Station supports the Network Time Protocol (NTP) to maintain its accuracy. The use of NTP is optional

At the Main Web GUI Interface Screen select the ***Configuration*** Tab and then select the ***time*** Main Menu Option. This will display the System Date and Time Settings and the display is split into one main group section (Figure 77). In addition, the time menu option has a single further sub-element.

The further sub element is:

- ***ntp***. These are the NTP time settings.

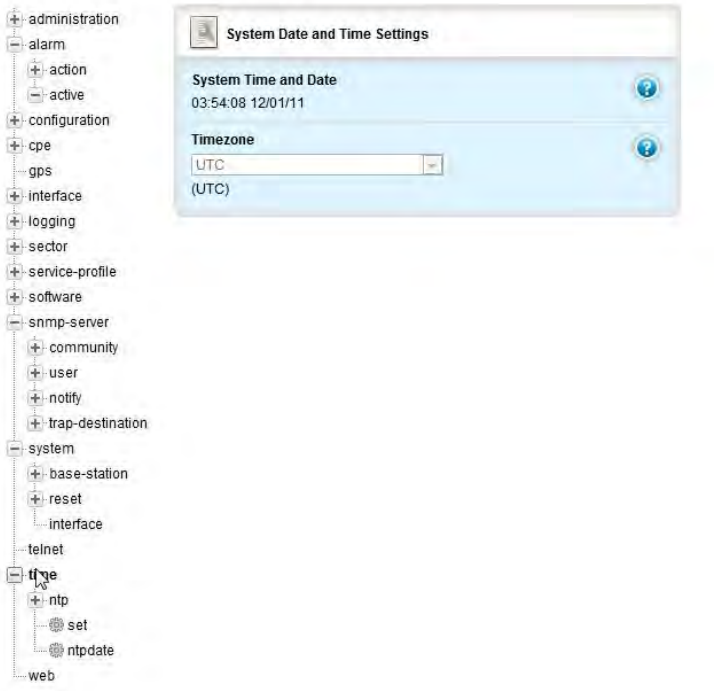


Figure 77 Time Settings

An indication as to whether there are any User configurable parameters included in the group is provided. If the User wants to configure any of the parameters, then they must enter the Edit Mode (select Edit Private or Edit Exclusive) and edit as necessary. The methods to Edit the parameters will be offered via drop down menu.

The System Date and Time Settings window contains:

- ***System Time and Date***. This is an indication of current date and time. This is not a User configurable parameter.
- ***Timezone***. This is an indication of the timezone. The Use is free to select their respective timezone and multiple options are available via the dropdown menu.

To view the Network Time Protocol Settings then at the Main Web GUI Interface Screen, select the ***Configuration*** Tab, select ***time*** Main Menu Option and then ***ntp*** Main Menu Sub-Element. The display is split into two main grouping sections.

- ***Network Time Protocol Settings***. This is an indication as to whether NTP has been enabled. The options are enabled and disabled with disabled as the default.
- ***NTP Server Settings***. This is an indication of the IP address, the NTP protocol version and whether the server is enabled of the NTP server. If the User wants to configure the NTP settings then they can edit, delete or add another NTP server. If the User enters the Edit mode for this parameter, then a further sub element with two more windows appear and the User can edit as required. The User can configure:
    - ***Ip-address***. This is the IP Address of the NTP Server.
    - ***Version***. This is the protocol version of the NTP Server.
    - ***Enabled***. This indicates whether the NTP Server is enabled.

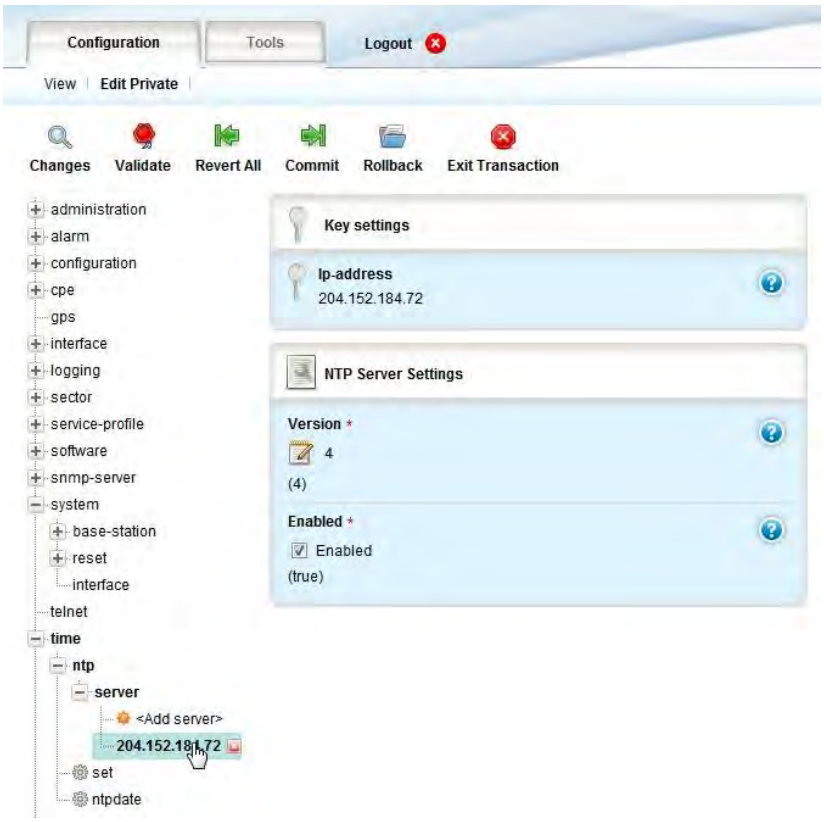


Figure 78 Time NTP Server Settings

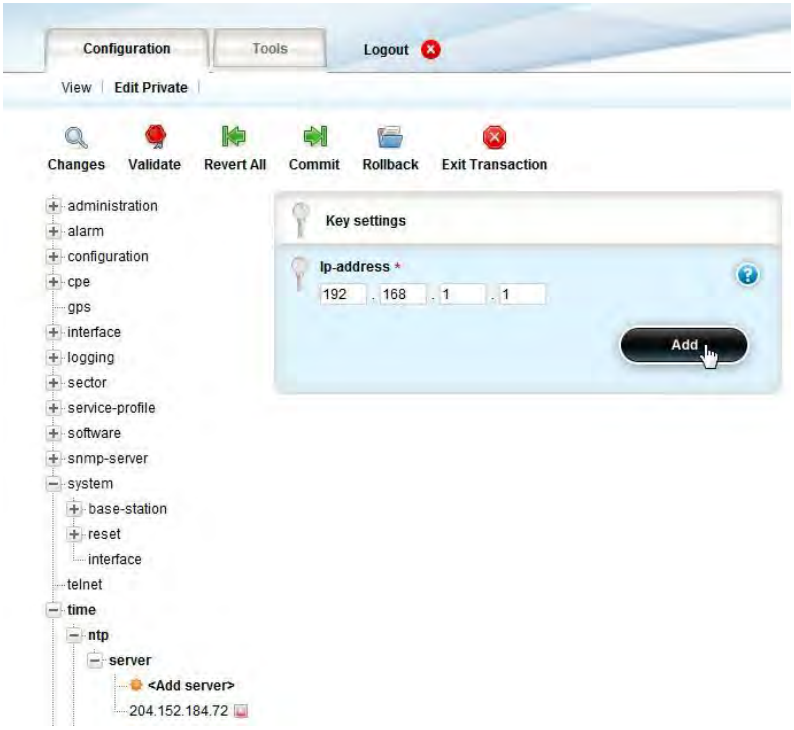


Figure 79 Time NTP Server Configuration

To view the current System Time and Date Settings then at the Main Web GUI Interface Screen select the ***Configuration*** Tab, select ***time*** Main Menu Option and then the ***set*** Main Menu Sub-Element. The display is split into two main grouping sections. (Figure 80).

- ***Set System Time and Date***. This is a text box that contains the ***Perform*** Command Menu Option.
- ***Time and Date***. The User is free to configure the Time and Date. The dialog time is specified in 24-hour format and includes milliseconds ("Ms"), which may simply be set to 0. TzH is the time zone hours offset from Coordinated Universal Time (UTC) and is between -23 and +23. TzM is the time zone minutes offset from Coordinated Universal Time (UTC) and is between 0 and 59. Once these parameters have been configured, the User must select the ***Perform*** Command Menu Option for the changes to be affected.

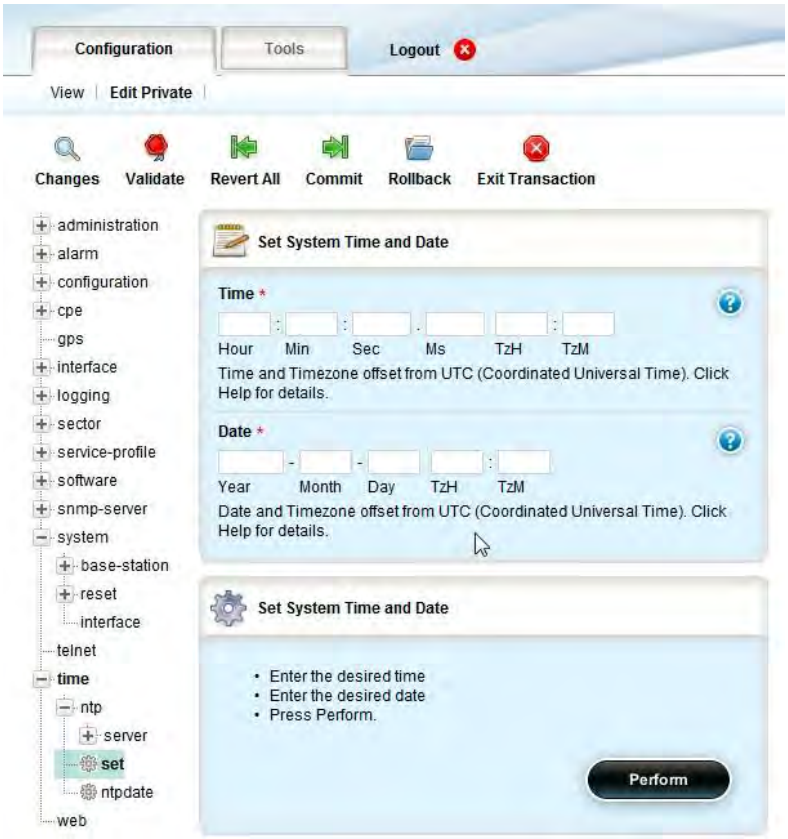


Figure 80 Time NTP Server System Set

To view the NTP Time/Date Synchronization then at the Main Web GUI Interface Screen select the ***Configuration*** Tab, select ***time*** Main Menu Option, then ***ntp*** Main Menu SubElement and then ***ntpdate***. The display is split into two main grouping sections (refer to Figure 81).

- ***NTP Time/Date Synchronization***. This command will perform a one-time synchronization to the selected NTP server. To apply the User simply needs to select the ***Perform*** command button.
- ***NTP Time/Date Synchronization***. The User can configure the NTP Server IP address to perform the one-time synchronization with.

Figure 81 Time NTP Server Synchronization Update

3.5.3.8 Telnet Settings

At the Main Web GUI Interface Screen select the ***Configuration*** Tab and select the ***telnet*** Main Menu Option. This will display the ***/telnet/server*** Settings and the display is split into one main group section (Figure 82). There is no further sub-element associated with this option.

The /telnet/server settings are:

- ***Enabled***. This indicates whether the telnet option has been enabled or not. This is a User configurable value that is edited via a check box.

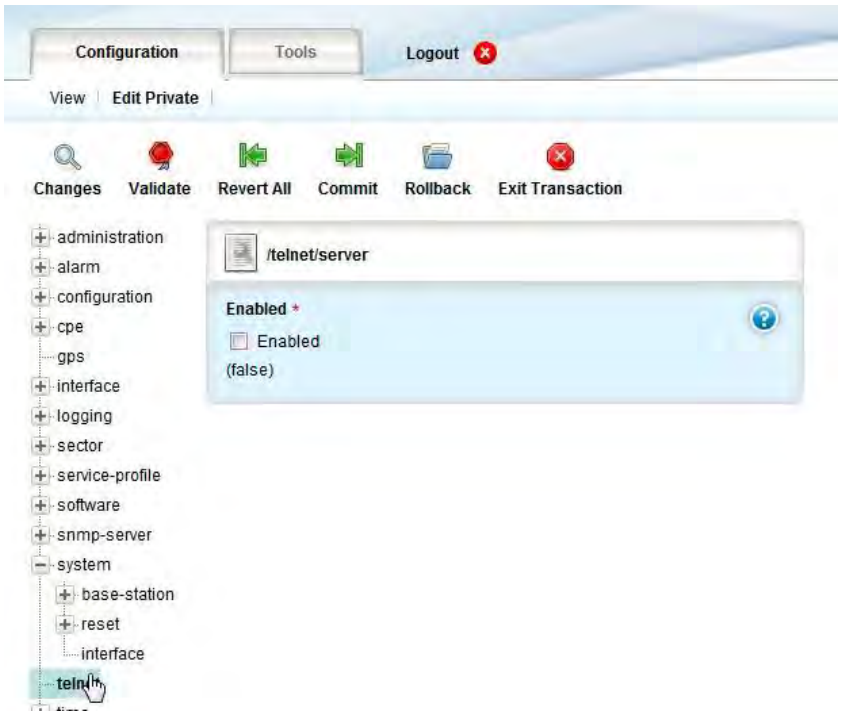


Figure 82 Telnet Server Enabled

3.5.3.9 Web Server Settings

At the Main Web GUI Interface Screen select the ***Configuration*** Tab and select the ***web*** Main Menu Option. This will display the web Settings and the display is split into two main grouping sections (Figure 83). The main grouping sections are:

- ***Web Server HTTP Support***. This indicates the Base Station HTTP options. The configuration options are:
  - ***Enabled***. This indicates whether the HTTP Support option has been enabled or not. This is a User configurable value that is edited via a check box. The default configuration is disabled.
  - ***Port Number***. This is the port number that the HTTP Server inside the Base Station will listen on and accept connections.
- ***Web Server HTTPS Support***. This indicates the Base Station HTTP options. The configuration options are:
  - ***Enabled***. This indicates whether the HTTPS Support option has been enabled or not. This is a User configurable value that is edited via a check box. The default option is enabled.
  - ***Port Number***. This is the port number that the HTTPS Server inside the Base Station will listen on and accept connections.

Figure 83 Web Server HTTP Support

3.5.3.10 Configuration Settings

All the Base Station configuration parameters are contained and stored local on the Base Station in flash memory, via a number of configuration files. The User has the complete control to perform a variety of functions such as copy, move, delete and restore etc. on these files. This presents a User with an option, in the event that they would like to reconfigure a Base Station or the Subscriber CPE profiles they can copy and export a configuration file which can then easily be edited and downloaded back onto the Base Station. This is an alternative approach to the screen by screen configuration method that is detailed in this User Guide.

At the Main Web GUI Interface Screen select the ***Configuration*** Tab and select the ***configuration*** Main Menu Option. This will display the configuration Settings and the display is split into two main grouping sections (Figure 76). There are ten Main Menu Sub-Elements associated with the ***configuration*** Main Menu Option. The main grouping sections are:

- ***Configuration File Operation Status***. This indicates the Configuration File operation status when the User is downloading or uploading a configuration file. The parameters that are displayed are as follows.
    - *State*. This indicates execution state of the configuration command. It is not a configurable parameter and simply states the current status, for example Idle.

    - *Download Progress*. This provides an indication of the completion percentage of the configuration file that is being downloaded. This is not a configurable parameter.
    - *Upload Progress*. This provides an indication of the completion percentage of the configuration file that is being uploaded. This is not a configurable parameter.
- ***Configuration Files.*** This is a list of the configuration files on the Base Station. There is no configurable parameters for these files and the information that is presented for each file is:
    - ***Name***.
    - ***Size***. The size of the file is in bytes.
    - ***Modified***. This is the date and time that the file was last modified.

The ten Main Menu Sub-Elements are essentially the actions that can be performed on a configuration file. The User is not required to be in Edit Mode to perform any of these actions, the action is presented to them directly at each Main Menu Sub-Element option. These are:

- ***Copy***
- ***Move***
- ***Delete***
- ***Export***
- ***Import***
- ***Write***
- ***Restore***
- ***Download***
- ***Upload***
- ***Files***

The Main Menu Sub-Elements will be examined in detail. The same display elements are presented when the User navigates to each of these 10 Main Menu Sub-Elements. The display is split into two main grouping sections (Figure 84).

- The top grouping section provides a description and instructions of the action.
- The bottom grouping section provides the mechanism to perform the action.

Another common theme throughout the Main Menu Sub-Element is the ability to select a configuration file for an action. The relevant files are presented to the User via a drop-down menu or the files are listed under the files Main Menu Sub-Element option. To view the files then at the Main Web GUI Interface Screen, select the ***Configuration*** Tab and select the ***files*** Main Menu Option. This will display all the relevant files.

The explanation for each file is:

- ***.cnf (configuration) files*** are created by the export command and can only be read by the import command. The data in the file is saved as a series of CLI commands. This file is in ASCII format and can be edited within a text editor.
    - ***profile.cnf*** file is the Base Station configuration file
    - ***cpe.cnf*** file is the Subscriber CPE configuration file

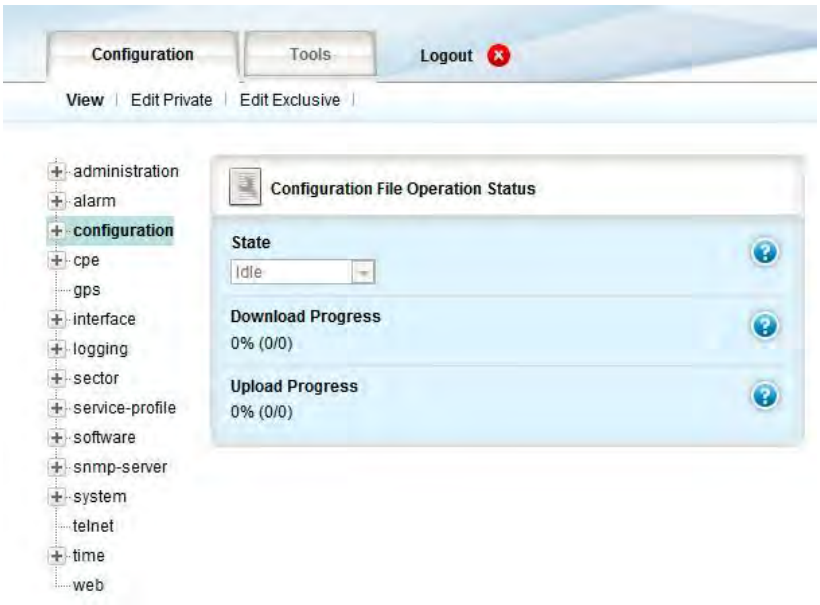


Figure 84 Configuration Settings

At the Main Web GUI Interface Screen select the *Configuration* Tab, then *configuration* Main Menu Option and then the ***copy*** Main Menu Sub-Element. This will display window to copy a configuration file.

Figure 85 Configuration Copy Settings

The procedure to copy a file is:

1. Select the file to be copied from the drop-down menu of the ***Existing File Name*** field (Figure 85).
2. Enter the copied file name in the ***Copied File Name*** field.

3. Enable the ***Force*** field if the User wants to overwrite an existing file on the Base Station.
4. The User must then press the ***Perform*** Command Menu Option.
5. The relevant file will now be copied, and the results of this action will be displayed as below.

Figure 86 Configuration Copy Successful

At the Main Web GUI Interface Screen select the ***Configuration*** Tab, then ***configuration*** Main Menu Option and then the ***move*** Main Menu Sub-Element. This will display window to move or rename a configuration file (Figure 87).

Figure 87 Configuration Move Settings

The procedure to rename a file is:

1. Select the file to be renamed from the drop-down menu of the ***Existing File Name*** field.
2. Enter the new file name in the ***New File Name*** field.
3. The User must then press the ***Perform*** Command Menu Option.
4. The relevant file will now be renamed, and the results of this action will be displayed.

At the Main Web GUI Interface Screen select the ***Configuration*** Tab, then ***configuration*** Main Menu Option and then the ***delete*** Main Menu Sub-Element. This will display window to delete a configuration file (Figure 88).

The procedure to delete a file is:

Figure 88 Configuration Delete Settings

1. Select the file to be renamed from the drop-down menu of the ***Filename*** field.
2. The User must then press the ***Perform*** Command Menu Option. A prompt box will now appear, and the User is requested to confirm "Do you really want to delete the file?".
3. The relevant file will now be renamed, and the results of this action will be displayed.

At the Main Web GUI Interface Screen select the ***Configuration*** Tab, then ***configuration*** Main Menu Option and then the ***export*** Main Menu Sub-Element. This will display window to export a configuration file (Figure 89). The export option creates an ASCII file that can be physically edited by the User. The file will be stored in flash on the Base Station and the User will have to upload it off the Base Station.

The procedure to export a file is:

Figure 89 Configuration Export Settings

1. Select the CLI export filter from the drop-down menu of the ***CLI Export Filter***. The options are:
    a. All. This will export the entire configuration database.
    b. BS-Configuration. Base Station configuration database only. This excludes CPE and Service-profiles.
    c. CPE. This will export the Subscriber CPE provisioning database only.
    d. Service-Profile. This will export the Service Profile database only.
2. Enter the destination filename to export the database in the ***Filename*** field.
3. The User must then press the ***Perform*** Command Menu Option.
4. The relevant file will now be created, and the results of this action will be displayed.

At the Main Web GUI Interface Screen select the ***Configuration*** Tab, then ***configuration*** Main Menu Option and then the ***import*** Main Menu Sub-Element. This will display window to import a configuration file (Figure 90). The import option will import a configuration into the running configuration.

⚠	Overwriting the configuration file can have serious consequences. The User must proceed with care.

Figure 90 Configuration Import Settings

The procedure to import a file to the Base Station:

1. Select the filename to import into the running configuration from the drop-down menu of the ***Import Filename***.
2. If the User enables the ***Overwrite*** field, then this will replace the existing CPE configuration data with the imported data. This will only work with files created with the export CPE option. Trying to load other files with the overwrite option set will result in an error message.
3. If the User does not enable the ***Overwrite*** field, then the imported data will be merged with the existing configuration.
4. The User must then press the ***Perform*** Command Menu Option.

	The Import command can take several minutes to complete. Please wait until this process is completed before going on to make any other configuration changes.

At the Main Web GUI Interface Screen select the ***Configuration*** Tab, then ***configuration*** Main Menu Option and then the ***write*** Main Menu Sub-Element. This will display window to write a configuration file (Figure 91). The write procedure will copy the running configuration to startup. The new startup configuration will be effective at the next reboot of the Base Station.

	Please note that changes will not be persistent and survive a restart unless the write command is issued after the changes are made.

Figure 91 Configuration Write Settings

The procedure to write the configuration is:

1. The User must then press the ***Perform*** Command Menu Option. A prompt box will now appear, and the User is requested to confirm "Do you really want to write the file?".
2. The relevant configuration will now be written, and the results of this action will be displayed.

At the Main Web GUI Interface Screen select the ***Configuration*** Tab, then ***Configuration*** Main Menu Option and then the ***restore*** Main Menu Sub-Element. This will display window to restore a configuration file (Figure 92). The procedure will restore a binary backup of the entire database. This procedure will require a reboot of the Base Station.

Figure 92 Configuration Restore Settings

The procedure to restore a database is:

1. Select the filename to restore a binary backup of the database in the ***Filename*** field.

2. The User must then press the ***Perform*** Command Menu Option. A prompt box will now appear, and the User is requested to confirm "Do you really want to delete the file?".
3. The relevant file will now be renamed, and the results of this action will be displayed.

At the Main Web GUI Interface Screen select the ***Configuration*** Tab, then ***configuration*** Main Menu Option and then the ***download*** Main Menu Sub-element. This will display window to download a configuration file to a remote server (Figure 93). Prior to downloading the file, the User must ensure that an FTP Server has been configured and is running. There are several free commercially available FTP Servers that can be used. A key step in the process is to ensure that the URL for the file is set to be the FTP Home directory. For the purposes of upload and download, think of the Base Station as client in relation to the FTP as the server. The download process will therefore download from the Server to the Base Station.

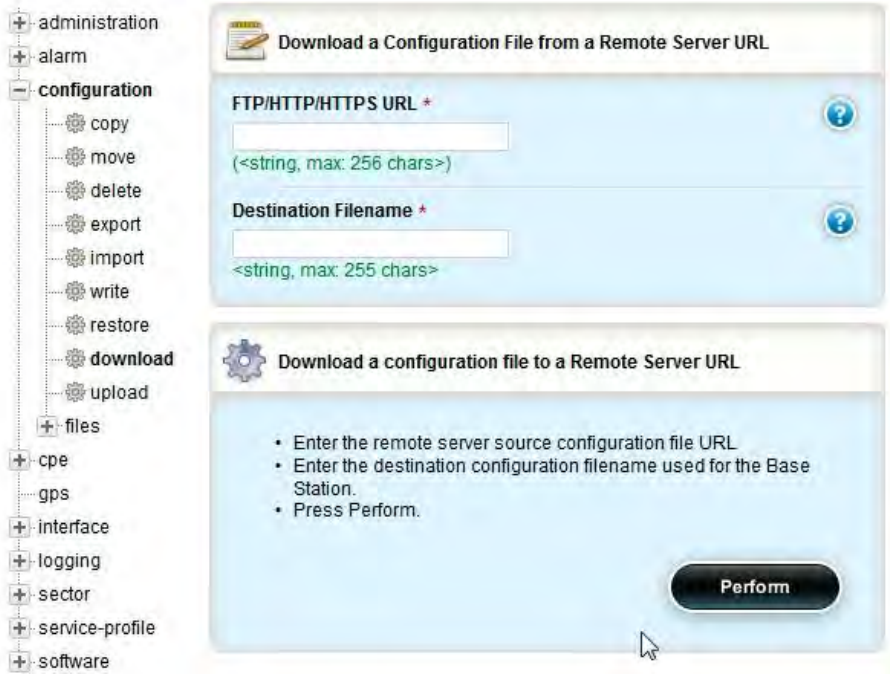


Figure 93 Configuration Download Settings

The procedure to download a file from a remote server is:

1. Enter the remote server source configuration URL in the *FTP/HTTP/HTTPS URL* field. Acceptable examples are:
    a. ftp://192.168.10.1/filename
    b. http://my.host-name.com/dir/filename
    c. ftp://username:password@noc.big_co.com:2323/dir/filename
2. Enter the destination configuration used filename used for the Base Station is the ***Destination Filename*** field.
3. The User must then press the ***Perform*** Command Menu Option. A prompt box will now appear, and the User is requested to confirm "Do you want to download the file?".
4. The relevant file will now be downloaded, and the results of this action will be displayed.

At the Main Web GUI Interface Screen select the ***Configuration*** Tab, then ***configuration*** Main Menu Option and then the ***upload*** Main Menu Sub-Element. This will display window to upload a configuration file to a remote server (Figure 94). Prior to uploading the file, the User must ensure that an FTP Server has been configured and is running.

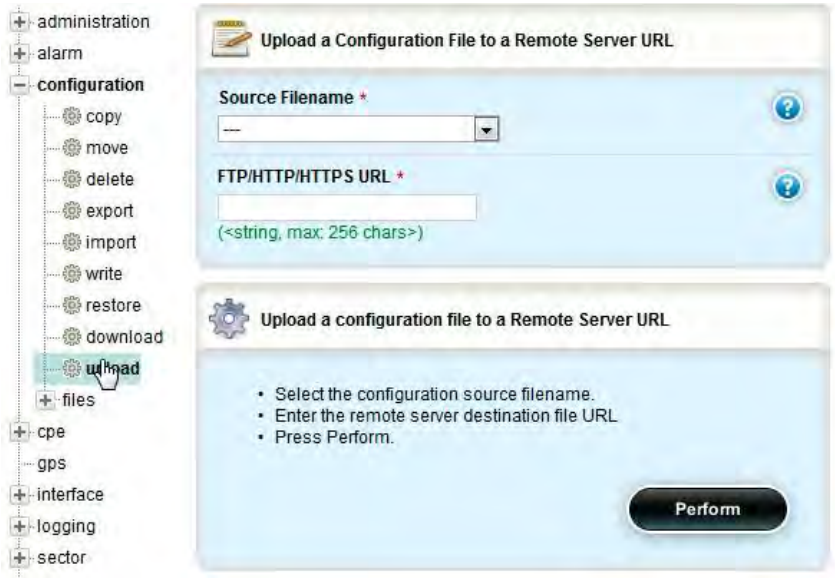


Figure 94 Configuration Upload Settings

The procedure to upload a file to a remote server is:

1. Enter the configuration source filename in the ***Source Filename*** field.
    a. ftp://192.168.10.1/filename
    b. http://my.host-name.com/dir/filename
    c. ftp://username:password@noc.big_co.com:2323/dir/filename
2. Enter the remote server destination file URL in the ***FTP/HTTP/HTTPS URL*** field. Acceptable examples are:
3. The User must then press the ***Perform*** Command Menu Option. A prompt box will now appear, and the User is requested to confirm "Do you want to upload the file?".
4. The relevant file will now be uploaded, and the results of this action will be displayed.

	To ensure that the User has a stored backup of the running configuration file, then the User would ***export*** and then ***upload*** the relevant files. To restore a previously stored filed from its remote location, then the User would ***download*** and then ***import.***

The procedure to upload a file to a remote server is:

1. Enter the configuration source filename in the Source Filename field.
2. Enter the remote server destination file URL in the ***FTP/HTTP/HTTPS URL*** field. Acceptable examples are:
    a. ftp://192.168.10.1/filename
    b. http://my.host-name.com/dir/filename
    c. ftp://username:password@noc.big_co.com:2323/dir/filename

3. The User must then press the ***Perform*** Command Menu Option. A prompt box will now appear, and the User is requested to confirm "Do you want to upload the file?".
4. The relevant file will now be uploaded, and the results of this action will be displayed.

To ensure that the User has a stored backup of the running configuration file, then the User would ***export*** and then ***upload*** the relevant files. To restore a previously stored file from its remote location, then the User would ***download*** and then import.

3.5.4 Connecting a Subscriber Station

The procedures for provisioning each make and model of Subscriber CPE device vary and hence are beyond the scope of this document. However, Mercury have prepared general documentation that details recommend procedures to configure specific Subscriber units. Please refer to this documentation for further details.

	When a Subscriber CPE is powered on and configured for an appropriate Base Station, if that Base Station is configured for autoprovisioning, the Subscriber CPE will automatically connect to the Base Station and it will be assigned the default Client Profile (Client Profile 1).

The User however has the complete flexibility to pre-configure the Subscriber CPE and has the capability to assign it to a specific Client Profile.

The procedure to configure a Subscriber CPE is:

1. For the Subscriber CPE that you wish to provision please record the Subscriber MAC address. This is written on the CPE label.
2. At the Main Web GUI Interface Screen select the ***Configuration*** Tab and then the ***cpe*** Main Menu Option. This will display a list of all Subscriber CPEs that have been specifically configured on the Base Station (Figure 95). If there are none listed, then none have been configured.

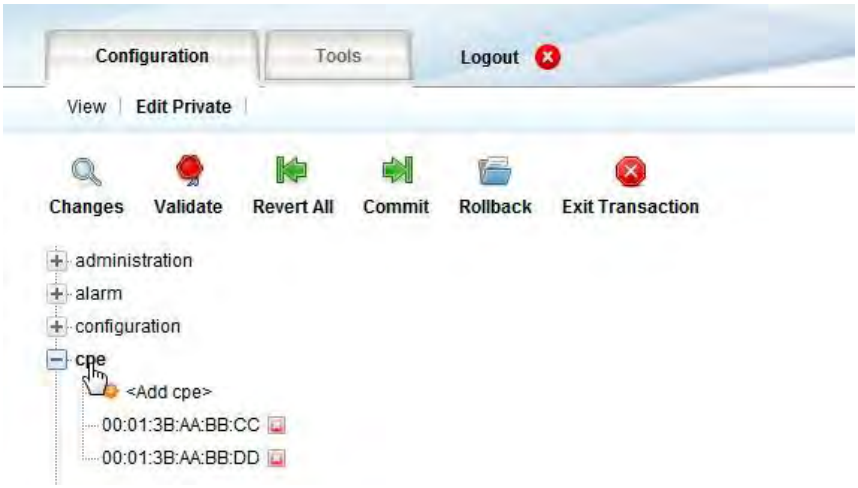


Figure 95 CPE Main Menu Option

3. The User now must enter the Edit Mode (select Edit Private or Edit Exclusive). The <***Add cpe***> option will appear (refer to Figure 96).

Figure 96 Add Subscriber CPE Option

4. The User must select the <***Add cpe***> option. A ***Key Settings*** window will appear. The User is prompted to enter the Subscriber CPE ***MAC Address***. The MAC Address must be entered in ***Upper Case*** letters only and using a colon (:) to separate the digits, e.g. 00:17:C4:8F:9B:34. If the User selects the "*?*" Command Menu Option within the window then a reminder prompt will be displayed. Once the MAC Address has been entered the User must select the Add command button (Figure 97).

Figure 97 Add Subscriber CPE MAC Address

5. The User will now be presented with the Subscriber configuration options. The options to select are (Figure 98):

- ***Convergence Sublayer Type***. The User can select from a drop-down menu. The default option is Ethernet CS and the available options are:
  - **IPV4_CS.**
  - **ETHERNET_CS** . This is the default setting; the Base Station operates in Standalone mode.
- ***Client Profile***. This profile can be selected from a drop-down menu. The User can select <unset> or from one of the user configured profiles (1 through 64).
- ***IP Address***. Applicable/Visible only when the CPE is configured for IPV4_CS Convergence Sublayer mode and the base station operated in Stand Alone mode. 0.0.0.0 value (default) means that the

CPE will obtain its IP address through DHCP Server. When changed from the defaults value a static IP address is used for the Provisioning. The CPE device's WAN interface must be configured with the same IP address.

- ***IP Netmask***. Applicable/Visible only when the CPE is configured for IPV4_CS Convergence Sublayer mode and the base station operated in Stand Alone mode. Defines the Subnet Mask. Currently only a single IP Address is possible, thus the default value of 255.255.255.25.255 should not be changed!
- ***Customer ID***. This is a free format text field that enables the User to uniquely define a Subscriber. This is edited by selecting the notepad icon.
- ***Maximum Uplink Rate***. The *User can s*elect the maximum uplink modulation rate. This will effectively provide a cap on the maximum data traffic rate. This direction is defined as the Subscriber to Base Station. This is selected via the drop-down menu and the options are:
    - **QAM64 5/6**
    - **QAM64 3/4**
    - **QAM64 2/3**
    - **QAM64 1/2**
    - **QAM16 3/4**
    - **QAM16 1/2**
    - **QPSK 3/4**
    - **QPSK 1/2**
- ***Maximum Downlink Rate***. The User can select the maximum downlink modulation rate. This will effectively provide a cap on the maximum data traffic rate. This direction is defined as the Base Station to Subscriber. This is selected via the drop-down menu and the options are:
    - **QAM64 5/6**
    - **QAM64 3/4**
    - **QAM64 2/3**
    - **QAM64 1/2**
    - **QAM16 3/4**
    - **QAM16 1/2**
    - **QPSK 3/4**
    - **QPSK 1/2**
- ***Vlan-profile***. Select and apply a default Vlan-profile to the CPE.

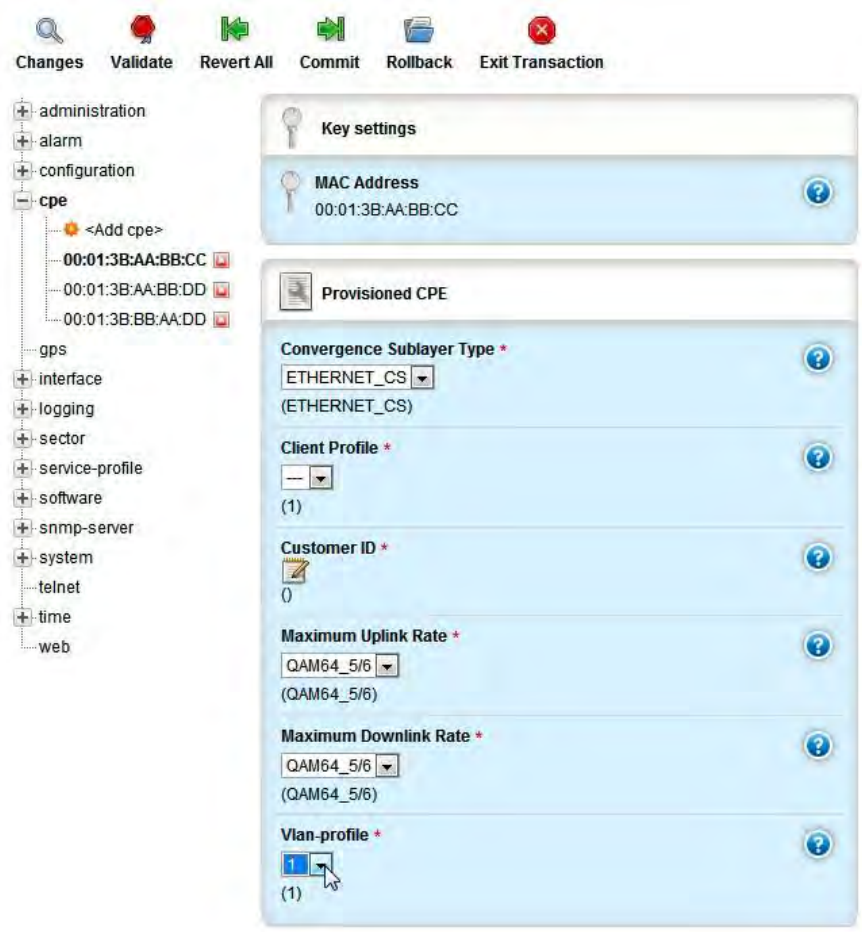


Figure 98 Add Subscriber CPE Settings

6. Once the Subscriber options have been selected, the User can then Validate the changes. The User simply selects the Validate command button. A window indicating whether the Validation is successful or not will appear (Figure 99). If successful, then the User has to select the OK command button.

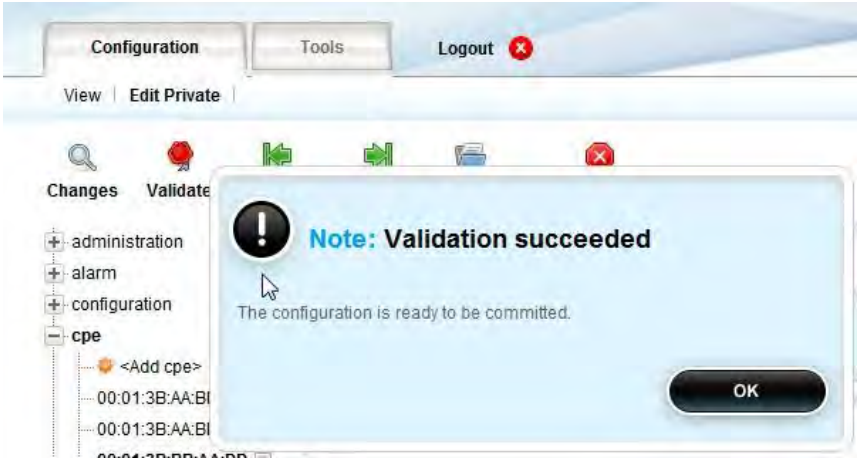


Figure 99 Add Subscriber CPE Validation

7. After performing the Validation, the final step is to execute the Commit procedure. The User must select the Commit command button. A window prompting the User to commit the changes will appear. To affect the commit the User must select the OK command button (Figure 100). A further window indicating that the commit changes succeeded will appear.

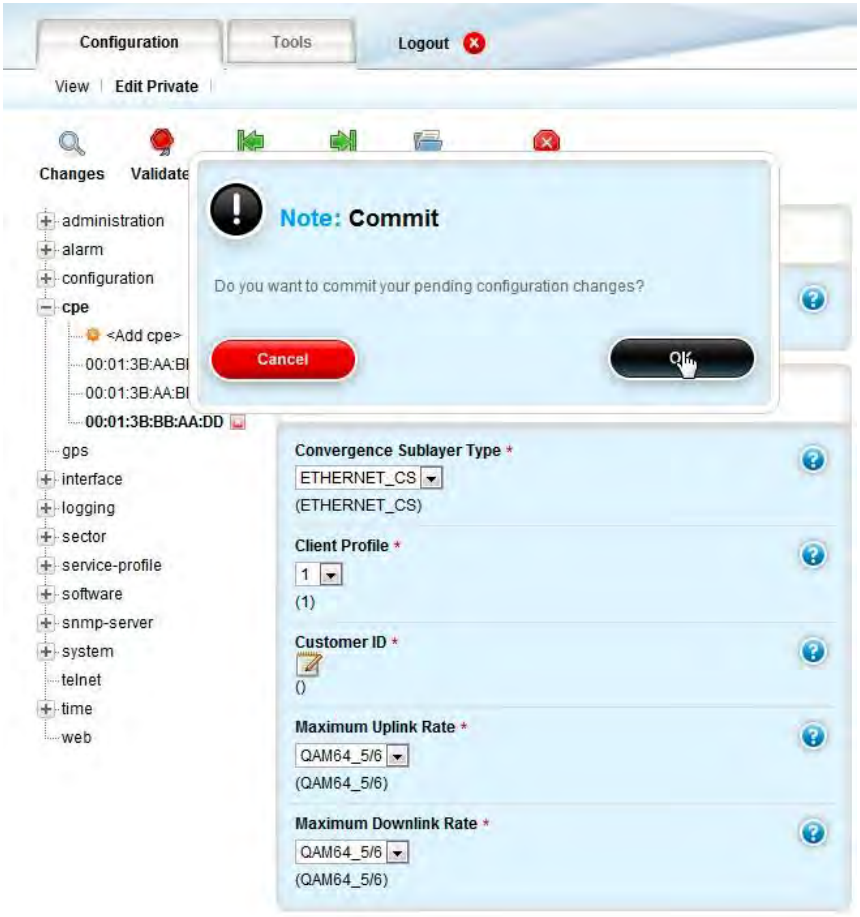


Figure 100 Add Subscriber CPE Commit

8. The Subscriber configuration details will now be displayed.

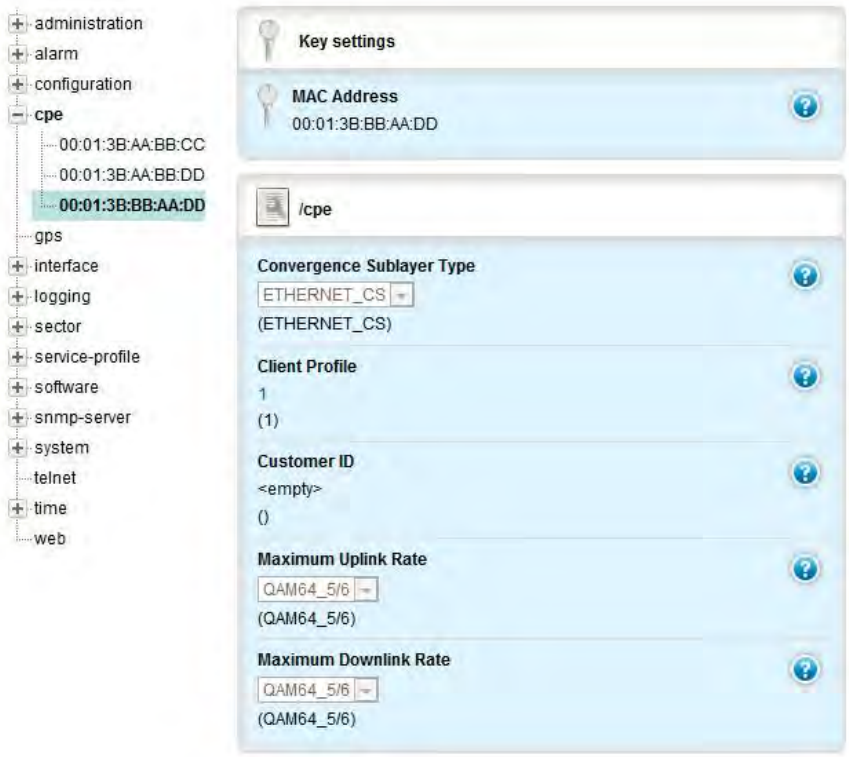


Figure 101 Subscriber CPE Configured Settings

9. If the User wants to delete a previously configured Subscriber, then the option to delete is available. When the User is in the Edit Mode, there is a red cross box positioned next to the end of the Subscriber MAC Address listing. If the User positions the cursor over the box, then the message “Remove cpe” appears (Figure 102). The User simply selects this box. The User must then commit the changes.

Figure 102 Subscriber CPE Delete

3.5.5 Subscriber CPE Client Profiles

The process to create a QoS (Quality of Service) Client Profile on the Subscriber CPE is relatively straightforward. The basic concept flow diagram is detailed in **Figure 103.**

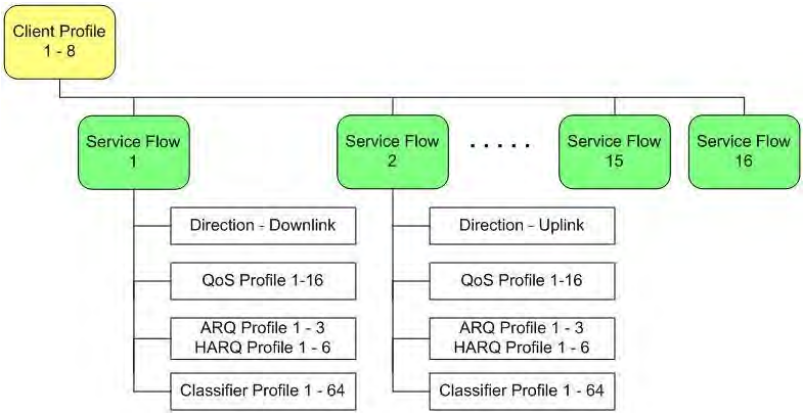


Figure 103 Subscriber CPE Provisioning Flow Concepts

The Service Profile system using Client Profiles, creates multiple data connections that suit the need of the Operator or Service Level Agreements. The Client Profile is the top level in a complex hierarchy that provides a large degree of flexibility in service offerings.

Client Profiles are assigned to individual Subscriber CPE's and within each client profile there is the ability to throttle throughput and organize types of traffic into specific connection types. The use of ARQ/HARQ is also contained within this system.

The Subscriber CPE Client Profile contains a Service Flow for both the uplink and the downlink directions. The Service Flow is created from the following components:

- The direction of flow of traffic
- The specific Quality of Service (QoS) type, e.g. Best Effort (BE) or Unsolicited Grant Service (UGS) and the bandwidth rates applied to a service flow
- ARQ and/or HARQ definitions. These are the error recovery mechanisms.
- Packet Classifiers. This will classify on a packet by packet basis depending on the defined classification criteria. For example, the conditions under which the packet is to be transported and/or which Service flow it is to be assigned.

A Client Profile is a set a Service Flows that correspond to a specific Service Level Agreement assigned to a customer. Each Client Profile supports up to 16 service flows and each service flow is unidirectional. A set of service flows includes an Uplink and a Downlink direction.

	Tip: When designing Client Profiles, it is important to understand how the throughput rating mechanism works. In the event of contradicting parameters being set, the system will allocate to a Subscriber CPE the lower of the parameters. For example, assume a conflict between the Client Profile setting the maximum uplink rate of 2Mbps and the QoS Profile setting the maximum sustained rate to 1Mbps. In this example, the system will limit the uplink rate to 1Mbps.

Figure 104 demonstrates a typical "Best Effort" type of Client Profile. Consider a packet that is flowing in the downlink direction (i.e. Base Station to Subscriber CPE). The same concept applies in the uplink direction.

- A packet flow from the network and into the Base Station. It is destined for the Subscriber CPE.
- The packet is then processed by the Classifiers rules that have been defined. In this example these are the Downlink Packet Classifier.
- If the packet is subject to the Classifier rule, then it is processed and classified as defined by that rule. Packets that are not subject to the rule are then identified as a Non-Classified Packet.
- The Non-Classified Packets are then passed out of the Base Station and are now subject to the relevant Service Flow definitions. In this example this would be Best Effort.

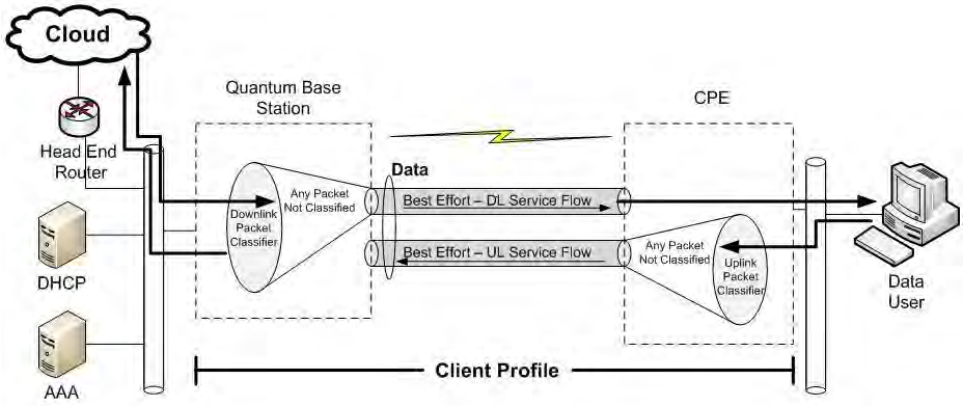


Figure 104 Typical Best Effort Client Profile

Figure 98 demonstrates a more complex but still typical "Voice and Data" type of application.

- In this example these is a VoIP Packet Classifier defined. This has been associated to an eRTPS Service Flow. Non-Classified packets have been set to a Best Effort Service Flow.
- Any packet that enters from the Network will be tested against the Classifier rules. A VoIP packet will therefore be transmitted downlink via eRTPS and everything else via Best Effort.

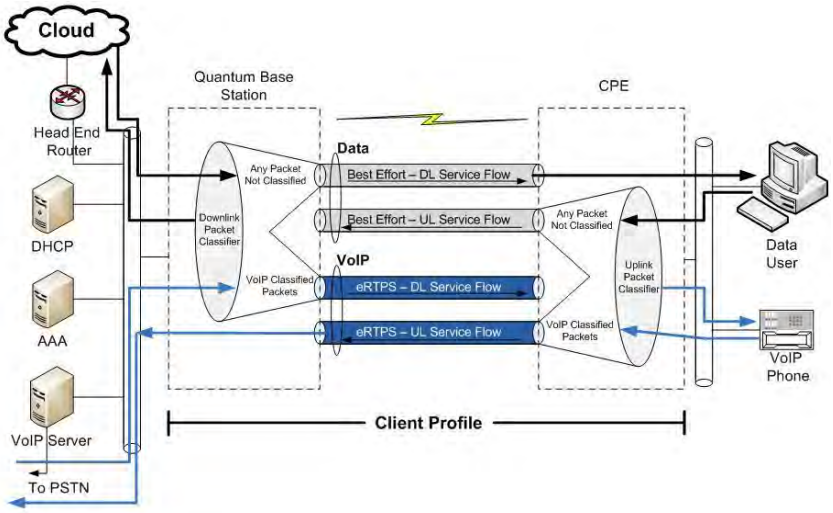


Figure 105 Typical Voice and Data Client Profile

	By default, the Base Station is pre-configured with several profiles for Classifier, HARQ, ARQ, QoS and Client. The User has the complete freedom and flexibility to use these pre-defined profiles or they can edit accordingly.

At the Main Web GUI Interface Screen select the ***Configuration*** Tab and then the ***serviceprofile*** Main Menu Option. This window details the information for the service profile Main Menu Option. There are five Main Menu Sub-Elements and window is split into five main grouping sections (Figure 106). The five main grouping sections provide a summary of the information that can be obtained by selecting and navigating down into the Main Menu Sub-Element level.

Figure 106 Service Profile Menu Option

The Main Menu Sub-Elements are:

- ***cls-profile***. These are the Classifier profiles.
- ***harq-profile***. These are the Hybrid ARQ (automatic recovery) profiles.
- ***arq-profile***. These are the ARQ profiles.
- ***qos-profile***. These are the Quality of Service profiles.
- ***client-profile***. These are the Client profiles.
- ***vlan-profile***. VLAN configuration profiles.

This just provides an indication of the information that is displayed. A description of the variables will be provided when the Main Menu Sub-Elements are described. The five main grouping sections are:

- ***Classifier Profiler***. The User can define up to 64 Classifier profiles. A list of profiles (up to 16 at a time) and the following information is displayed for each Classifier:
  - ***Profile #***
  - ***Name***
  - ***Description***
  - ***Cls-priority***
  - ***Cls-priority-used***
  - ***Eth-type***
  - ***Eth-type-used***
  - ***Ip-tos-dscp***
- ***Hybrid ARQ Profile***. The User can define up to 6 profiles and the following information is displayed for each profile:
  - ***Profile #***
  - ***Name***
  - ***Description***
  - ***Enable***
  - ***Channel-mapping***
  - ***Num-retries***
  - ***Pdu-sn-support***
- ***ARQ Profile***. The User can define up to 3 profiles and the following information is displayed for each profile. It is recommended to keep default values.
  - ***Profile #***
  - ***Name***
  - ***Description***
  - ***Enable***
  - ***Deliver-in-order***
  - ***Window-size***
  - ***Timeout-tx-delay***
  - ***Timeout-rx-delay***
  - ***Block-lifetime***
  - ***Sync-loss***
  - ***Purge-timeout***
  - ***Block-size***
  - ***Ack-processing-time***
- ***QoS Profile***. The User can define up to 32 profiles and the following information is displayed for each QoS profile:
  - ***Profile #***
  - ***Name***
  - ***Max-sustained-traffic-rate***
  - ***Max-latency***
  - ***Data-delivery-service***
  - ***Traffic-priority***
  - ***Max-traffic-burst***

- ***Min-reserved-traffic-rate***
- ***Tolerated-jitter***
- ***Unsolicited-grant-interval***
- ***Unsolicited-poll-interval***

- ***Client Profile***. The User can define up to 64 profiles and the following information is displayed for each Client profile:
  - ***Profile #***
  - ***Description***
  - ***Max-dl-rate***
  - ***Max-pps***
  - ***Max-ul-rate***
  - ***Min-dl-reserved-rate***
  - ***Min-ul-reserved-rate***

At Main Web GUI Interface Screen select the ***Configuration*** Tab and then the ***serviceprofile*** Main Menu Option. If the User now enters the Edit Mode, then they can either Edit or Delete any of all the profiles that have been configured as a default. If the User decides to Edit any of these profiles, then they are immediately navigated to the relevant Main Menu Sub-Element level.

The information that is presented at the *service-profile* Main Menu Option level is simply a summary of what is available for each of the profiles. The User can navigate to the respective Main Menu Sub-Element level for full viewing and configuration capabilities.

	If the User wants to configure any of the parameters, then they must enter the Edit Mode (select Edit Private or Edit Exclusive) and edit as necessary. The methods to Edit the parameters will be offered via a drop-down menu of choices, an enabling of a check box or editing of a notepad icon. These Profiles will now be described in detail.

These Profiles will now be described in detail.

3.5.5.1 Classifier Profile

This profile will classify on a packet by packet basis depending on the defined classification criteria. For example, the conditions under which the packet is to be transported and/or which Service flow it is to be assigned.

At Main Web GUI Interface Screen select the ***Configuration*** Tab, then the ***service-profile*** Main menu Option and then the ***cls-profile*** Main Menu Sub-Element. This User is presented with all the 64 preconfigured default profiles. These are displayed 16 at a time. To physically view all the profile configuration parameters then the User must select a profile and two main grouping sections are presented (Figure 107).

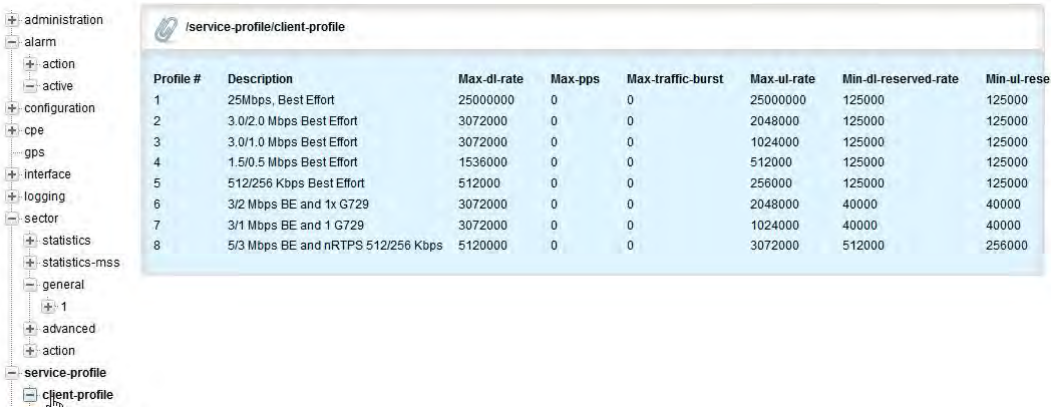


Figure 107 Service Profile Client Profile

The main grouping sections are:

- ***Key settings***. This simply displays:
  - ***Profile #***
- ***Classifier Profile***. This displays all that the available configuration parameters. These are:
  - ***Name***. This is the profile name and it is a text field
  - ***Description***. This is the profile description and it is a text field.
  - ***Cls-priority***. This User can assign a priority to the classifier. The priority is assigned as a number in the range 0 to 255. The default priority is 0 (no priority).
  - **Cls-priority-used**. This is a check box to enable/disable the priority rule.
  - ***Eth-type***. This is the Ethernet Type. This is assigned as a number in the range 1501 to 65535. This represents the value in decimal format.
  - ***Eth-type-used***. This is a check box to enable/disable the Ethernet Type rule.
  - ***Ip-tos-dscp***. This is the IP TOS Descriptor. This is assigned as a number in the range 0 (default) to 63.
  - ***Ip-tos-dscp-used***. This is a check box to enable/disable the IP TOS Descriptor rule.
  - ***Ip-protocol.*** This is the IP Protocol. This is assigned as a number in the range 0 (default) to 255.
  - ***Ip-protocol-used***. This is a check box to enable/disable the IP Protocol rule.
  - ***Dest-ip-addr-prfx***. This is the IP Destination Address and Prefix (mask length). Configuration examples are 192.0.0.0/2, 192.168.0.0/3, 192.1468.254.0/23 and 192.168.1.1/32.
  - ***Dest-ip-addr-used***. This is a check box to enable/disable the IP Destination Address rule.
  - ***Src-ip-addr-prfx.*** This is the IP Source Address and Prefix (mask length). Configuration examples are 192.0.0.0/2, 192.168.0.0/3, 192.1468.254.0/23 and 192.168.1.1/32.
  - ***Src-ip-addr-used.*** This is a check box to enable/disable the IP Source Address rule.
  - ***Dest-port-start.*** This is the Destination Port Low Limit. This is assigned as a number in the range 0 (default) to 65535.
  - ***Dest-port-end.*** This is the Destination Port High Limit. This is assigned as a number in the range 0 (default) to 65535.
  - ***Dest-ip-port-used.*** This is a check box to enable/disable the Destination Port rule.

- ***Src-port-start.*** This is the Source Port Low Limit. This is assigned as a number in the range 0 (default) to 65535.
- ***Src-port-end.*** This is the Source Port High Limit. This is assigned as a number in the range 0 (default) to 65535.
- ***Src-ip-port-used.*** This is a check box to enable/disable the Source Port rule.
- ***Vlan-id.*** This is the VLAN ID Tag. This is assigned as a number in the range 0 (default) to 4095.
- ***Vlan-id-used.*** This is a check box to enable/disable the VLAN ID rule.
- ***Vlan-user-priority-low.*** This is the VLAN User Priority Low Byte. This is assigned as a number in the range 0 (default) to 7.
- ***Vlan-user-priority-high.*** This is the VLAN User Priority High Byte. This is assigned as a number in the range 0 (default) to 7.
- ***Vlan-user-priority-used.*** This is a check box to enable/disable the VLAN User Priority rule.
- ***Mac-addr-option.*** This is a drop-down list to specify if a MAC address will be used for classification. The default value is auto. Other options include CPE_MAC or OUI (Organizationally Unique Identifier). The OUI is a unique 24-bit string assigned to hardware manufacturers.
- ***Mac-addr-oui.*** If OUI is specied in the Mac-addr-option, then this field will be visible. It will allow a 24-bit string to be specified to identify the hardware manufacturer.
- ***Allow-arp.*** This is a check box to enable/disable the ARP broadcasts.

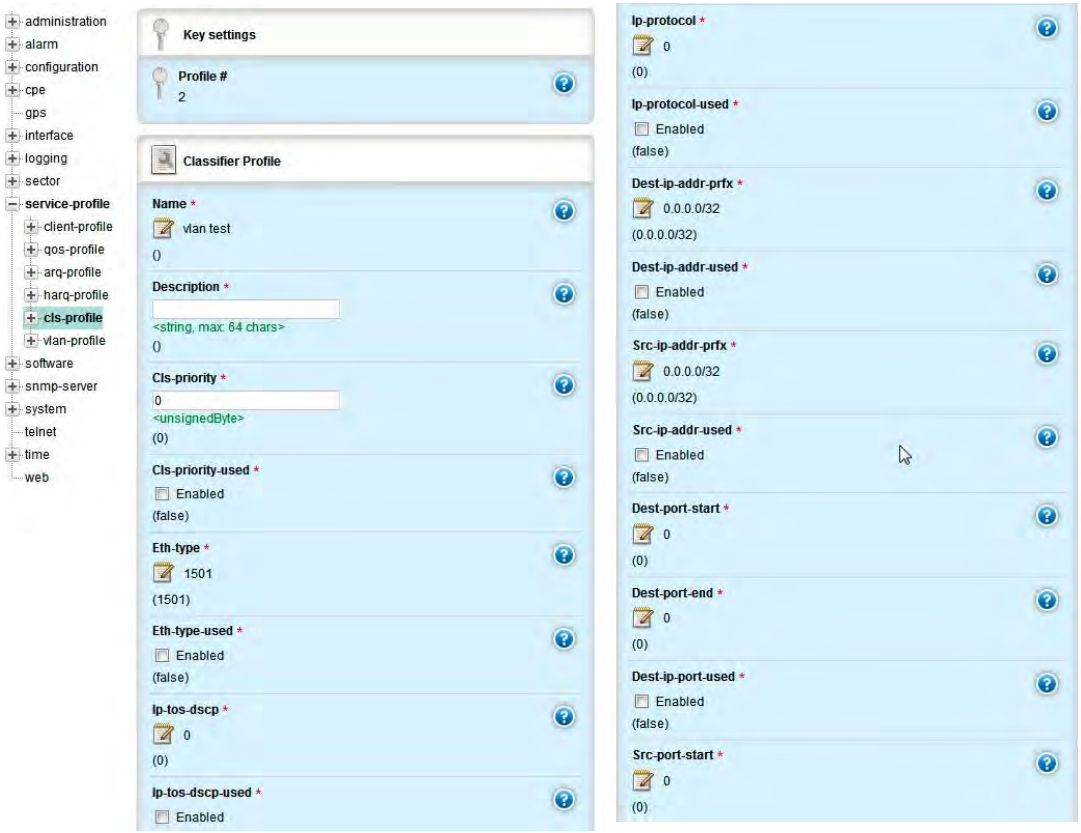


Figure 108 Classifier Profile

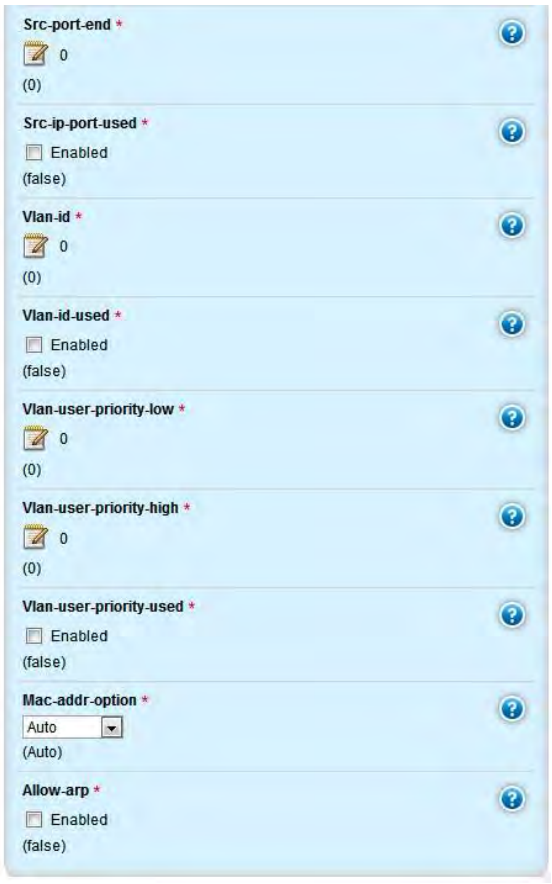


Figure 109 Classifier Profile Continued

The System is pre-configured with 64 default profiles. If the User wants to add any of their own configurations, they must delete a profile before they can add and configure a new one.

When in Edit mode, the User is presented with (Figure 110):

- *<Add cls-profile>.* If the User selects this option and there is available profile to be added, then they can simply add and then they will be dropped directly into the configuration window.
- A List of all the profiles with a red box beside each profile. If the User navigates to the red icon, then this will present the User with the ability to delete the profile.

Figure 110 Service Profile Classifier Profile Edit Capability

3.5.5.2 HARQ Profile

At the Main Web GUI Interface Screen select the *Configuration* Tab, then the ***serviceprofile*** Main Menu option and then the ***harq-profile*** Main Menu Sub-Element. This User is presented with all the 6 preconfigured default profiles. To physically view all the profile configuration parameters then the User must select a profile and two main grouping sections are presented (Figure 111).

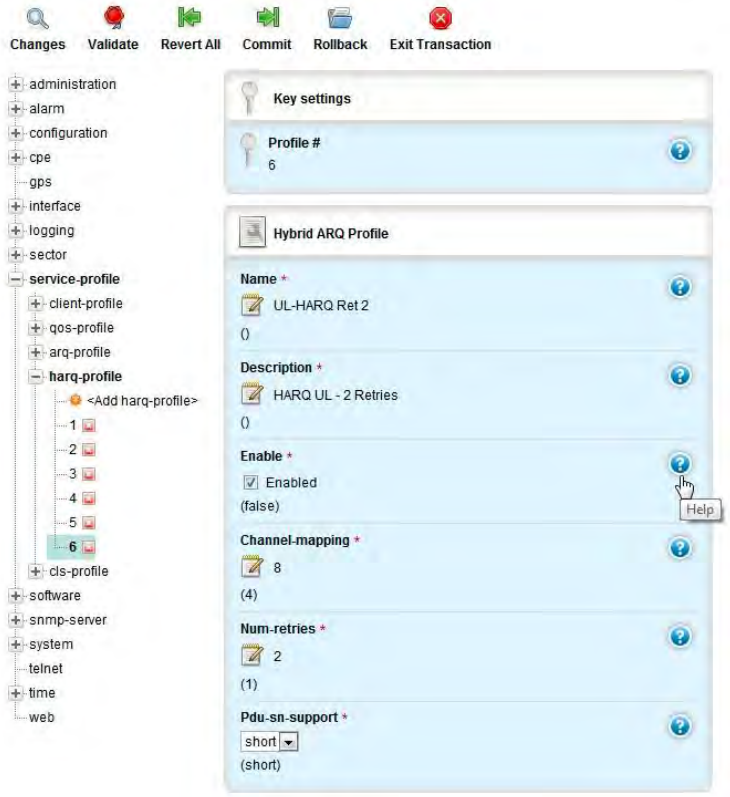


Figure 111 Service Profile HARQ Profile

The main grouping sections are:

- ***Key settings***. This simply displays:
  - ***Profile #***
- ***Hybrid ARQ Profile***. This displays all that the available configuration parameters. These are:
  - ***Name***. This is the profile name and it is a text field
  - ***Description***. This is the profile description and it is a text field
  - ***Enable***. This is a check box to enable/disable the HARQ function
  - ***Channel-mapping***. This is the HARQ Map Length. This is assigned as a number in the range 0 to 16 with a default of 4
  - ***Num-retires***. This is the HARQ Number of Retries. This is assigned as a number in the range 0 to 16 with a default of 1
  - ***Pdu-sn-support***. This is the HARQ PDU Sequence Number Support. The options are none, short (default) and long for reordering control. PDN sequence number is used to re-order HARQ bursts on the receiver. Short uses 3-byte sequence number and the long uses 4 byte. In general long is better in DL and short is enough in the UL. It is recommended to keep the default settings.

The System is pre-configured with 6 default profiles. If the User wants to add any of their own configurations, they must delete a profile before they can add and configure a new one.

When in Edit mode, the User is presented with (Figure 112):

- ***<Add harq-profile>***. If the User selects this option and there is available profile to be added, then they can simply add and then they will be dropped directly into the configuration window.
- A List of all the profiles with a red box beside each profile. If the User navigates to the red icon, then this will present the User with the ability to delete the profile.

Figure 112 Service Profile HARQ Profile Edit Capability

3.5.5.3 ARQ Profile

At the Main Web GUI Interface Screen select the ***Configuration*** Tab, then the ***serviceprofile*** Main Menu option and then the ***arq-profile*** Main Menu Sub-Element. This User is presented with all the 3 preconfigured default profiles. To physically view all the profile configuration parameters then the User must select a profile and two main grouping sections are presented (Figure 113).

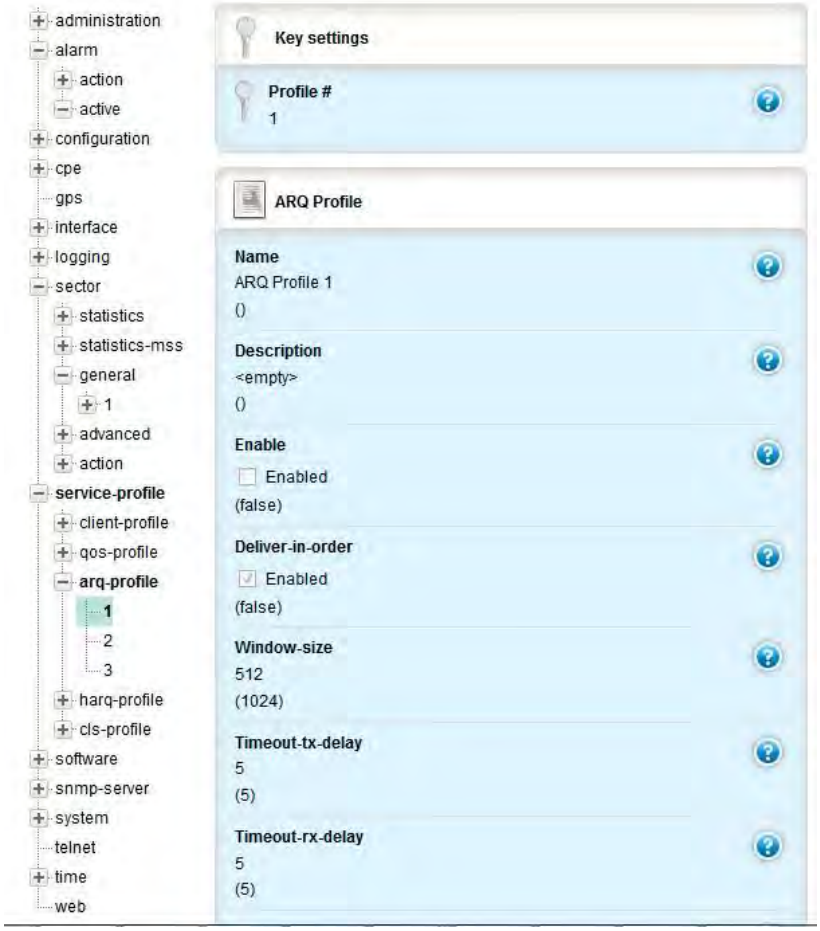


Figure 113 Service Profile ARQ Profile

The main grouping sections are:

- ***Key settings.*** This simply displays:
  - ***Profile #***
- ***ARQ Profile***. This displays all that the available configuration parameters. These are:
  - ***Name***. This is the profile name and it is a text field
  - ***Description***. This is the profile description and it is a text field.
  - ***Enable***. This is a check box to enable/disable the ARQ profile.
  - ***Deliver-in-order.*** This is a check box to enable/disable the ARQ deliver in order option.
  - ***Window-size.*** This is the ARQ Window Size. This is assigned as a number in the range 1 to 1024 (default).
  - ***Timeout-tx-delay.*** This is the ARQ Transmit Retry Timeout Delay. This is assigned in units of 5msec in the range 0 to 1310 with a default of 5 (25msec).

- ***Timeout-rx-delay***. This is the ARQ Receive Retry Timeout Delay. This is assigned in units of 5msec in the range 0 to 1310 with a default of 5 (25msec).
- ***Block-lifetime***. This is the ARQ Transmit Retry Timeout Delay. This is assigned in units of 5msec in the range 0 to 1310 with a default of 5 (25msec).
- ***Sync-loss***. This is the ARQ Sync Loss Timeout. This is assigned in units of 5msec in the range 0 to 1310 with a default of 120 (600msec).
- ***Purge-timeout***. This is the ARQ Purge Timeout. This is assigned in units of 5msec in the range 0 to 1310 with a default of 32 (160msec).
- ***Block-size***. This is the ARQ Block Size. The options are 16, 32, 64, 128 (default), 256, 512 and 1024.
- ***Ack-processing-time***. This is the ARQ Acknowledge Processing Time. This is assigned as a number in msec in the range 0 (default) to 255.

The System is pre-configured with 6 default profiles. If the User wants to add any of their own configurations, they must delete a profile before they can add and configure a new one.

When in Edit mode, the User is presented with:

- ***<Add arq-profile>***. If the User selects this option and there is available profile to be added, then they can simply add and then they will be dropped directly into the configuration window.
- A List of all the profiles with a red box beside each profile. If the User navigates to the red icon then this will present the User with the ability to delete the profile (Figure 114).

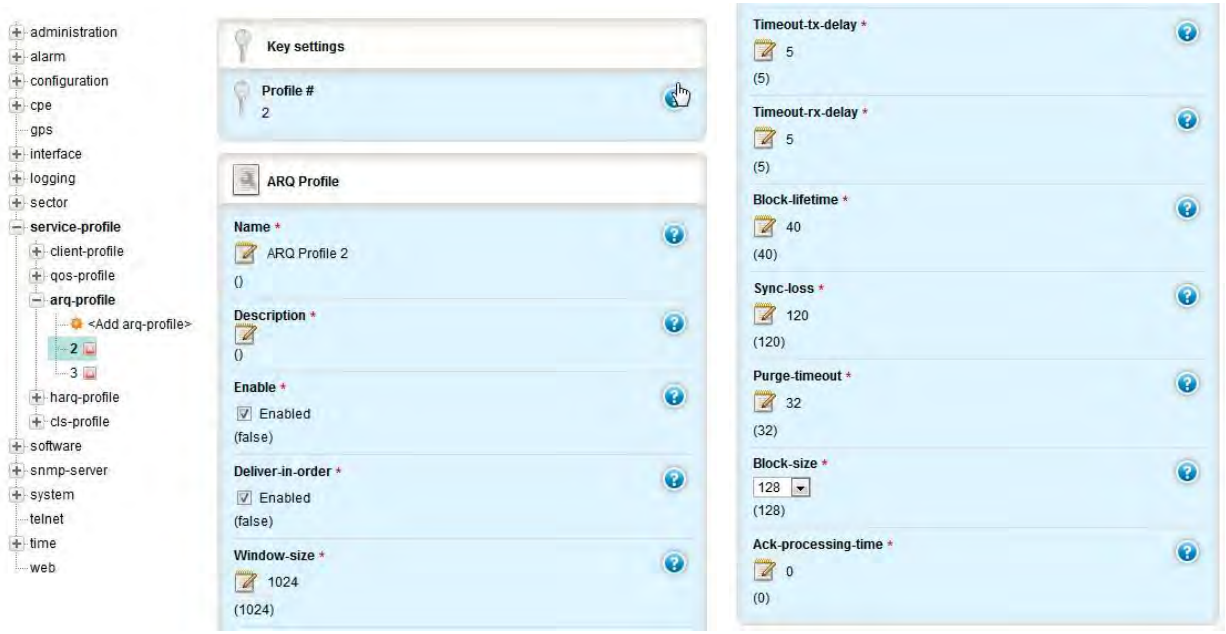


Figure 114 Service Profile ARQ Profile Edit Capability

3.5.5.4 Quality of Service, QoS Profile

A QoS Profile contains all information in regards to QoS type, latency, throughput and etc.
These Profiles are independent of direction and can be applied to multiple service flows. The types of QoS that are offered are:

- Best Effort or BE. Alternatively this is described as MIR or Maximum Information Rate.
- Unsolicited Grant Service or UGS. An alternative for this is CIR or Committed Information Rate.
- Extended Real-Time Polling Service or eRTPS. This is also known as Dynamic CIR.

Best Effort is by far the most used QoS type that is configured in most deployments. This Qos type is 'bursty' in nature and provides for up to a maximum rate. As an example, it could provide for internet speeds of up to 3 Mbps. The disadvantage of a Best Effort Service is that it does not provide any guarantee that the configured throughput will be achieved. A Base Station will offer throughput to BE configured Subscribers if there is bandwidth available and there are no other CIR configured Subscribers demanding throughput

Unsolicited Grant Service connections provide for a dedicated and guaranteed Service Level Agreement. It is typically used for applications that require constant bit rate services such as VoIP. Any traffic assigned to a UGS service flow will be allocated for the sole use by that Subscriber. The allocated traffic for this UGS will be removed from the available 'pool' of throughput for the Base Station to which the Subscriber has been configured. UGS connections typically provide low latency which is ideal for VoIP applications.

Extended Real-Time Polling Service is a QoS type that is very similar to UGS. Traffic is allocated for the sole use by a Subscriber CPE but only when the Subscriber CPE requests traffic. However, when traffic is

not being requested by the Subscriber, the allocated eRTPS bandwidth can be used by any other Subscriber. The eRTPS is the preferred QoS type for VoIP applications due to the dynamic resource control.

There are 32 QoS profiles that have been pre-configured and stored in the Base Station.
These can be viewed at the summary level (Figure 115). At Main Web GUI Interface Screen select the ***Configuration*** Tab and then select the ***service-profile*** Main Menu Sub-Element.

For full examination and configuration of the QoS profiles then the User needs to navigate into the Main Menu Sub-Element level.

QoS Profile

Profile #	Name	Description	Max-sustained-traffic-rate	Max-latency	Data-delivery-service	Traffic-priority	Max-traffic
1	Unlimited BE	Unlimited BE	25000000	200	BE_Service	5	0
2	256Kbps BE	256Kbps BE	256000	200	BE_Service	5	0
3	384Kbps BE	384Kbps BE	384000	200	BE_Service	5	0
4	512Kbps BE	512Kbps BE	512000	200	BE_Service	5	0
5	1Mbps BE	1Mbps BE	1024000	200	BE_Service	5	0
6	1.5Mbps BE	1.5Mbps BE	1536000	200	BE_Service	5	0
7	2Mbps BE	2Mbps BE	2048000	200	BE_Service	5	0
8	3Mbps BE	3Mbps BE	3072000	200	BE_Service	5	0
9	5Mbps BE	5Mbps BE	5120000	200	BE_Service	5	0
10	VoIP - G711	VoIP - G711 eRTPS	110000	60	eRTP_Service	5	110000
11	VoIP - G729	VoIP - G729 eRTPS	40000	60	eRTP_Service	5	40000
12	VoIP - G729 x2	VoIP - G729 x2 eRTPS	80000	60	eRTP_Service	5	80000
13	VoIP - UGS	VoIP - G711 Premium UGS	110000	60	UGS_Service	5	110000
14	3MIR/0.5CIR	3MIR/0.5CIR Mbps nRTPS	3072000	200	nRTP_Service	5	0
15	1.5MIR/0.256CIR	1.5MIR/0.256CIR Mbps nRTPS	1536000	200	nRTP_Service	5	0
16	1.5Mbps - RTPS	1.5Mbps RTPS - Streaming	1544000	200	RTP_Service	5	0

Figure 115 Default Quality of Service Profiles

At the Main Web GUI Interface Screen select the ***Configuration*** Tab, then the ***serviceprofile*** Main Menu Option and then the ***qos-profile*** Main Menu Sub-Element. This User is presented with all the 32 preconfigured default profiles (Figure 116). To physically view all the profile configuration parameters then the User must select profile and two main grouping sections are presented.

Figure 116 Quality of Service Profiles

The main grouping sections are:

- ***Key settings***. This simply displays:
  - ***Profile #***
- ***QoS Profile***. This displays all that the available configuration parameters. These are:
  - ***Name***. This is the profile name and it is a text field.
  - ***Description***. This is the profile description and it is a text field.
  - ***Max-sustained-traffic-rate***. This is a Maximum Sustained Traffic Rate. This is assigned in bits per second in the range 0 to 4294967295.
  - ***Max-latency***. This is a Maximum Latency. This is assigned in milliseconds in the range 0 to 65535.
  - ***Data-delivery-service***. This is the Data Delivery Service. The options that are available via a dropdown menu are UGS_Service, RTP_Service, nRTP_Service, BE_Service and eRTP_Service.
  - ***Traffic-priority***. This is the Traffic Priority Level. This is assigned as a number in the range 0 (default) to 7.
  - ***Max-traffic-burst***. This is a Maximum Traffic Burst Size. This is assigned in bits per second in the range 0 to 4294967295.
  - ***Min-reserved-traffic-rate***. This is a Minimum Reserved Traffic Rate. This is assigned in bits per second in the range 0 to 4294967295.
  - ***Tolerated-jitter***. This is a Tolerated Jitter. This is assigned in milliseconds in the range 0 to 65535.
  - ***Unsolicited-grant-interval***. This is a Unsolicited Grant Interval and is only relevant for UGS. This is assigned as a number in the range 0 to 65535.
  - ***Unsolicited-poll-interval***. This is a Unsolicited Poll Interval and is only relevant for nonUGS service classes. This is assigned as a number in the range 0 to 65535.

The System is pre-configured with 32 default profiles. If the User wants to add any of their configurations, they must delete a profile before they can add and configure a new one.

When in Edit mode, the User is presented with (Figure 117):

- ***<Add qos-profile>***. If the User selects this option and there is available profile to be added then they can simply add and then they will be dropped directly into the configuration window.
- A List of all the profiles with a red box beside each profile. If the User navigates to the red icon then this will present the User with the ability to delete the profile.

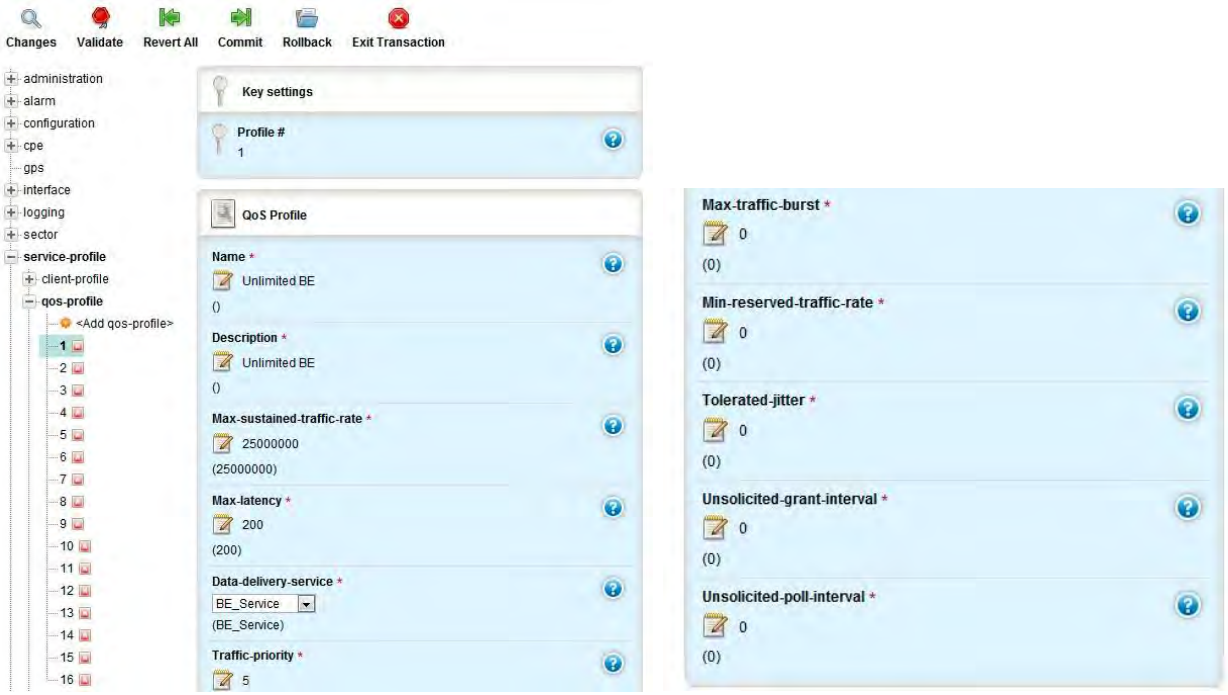
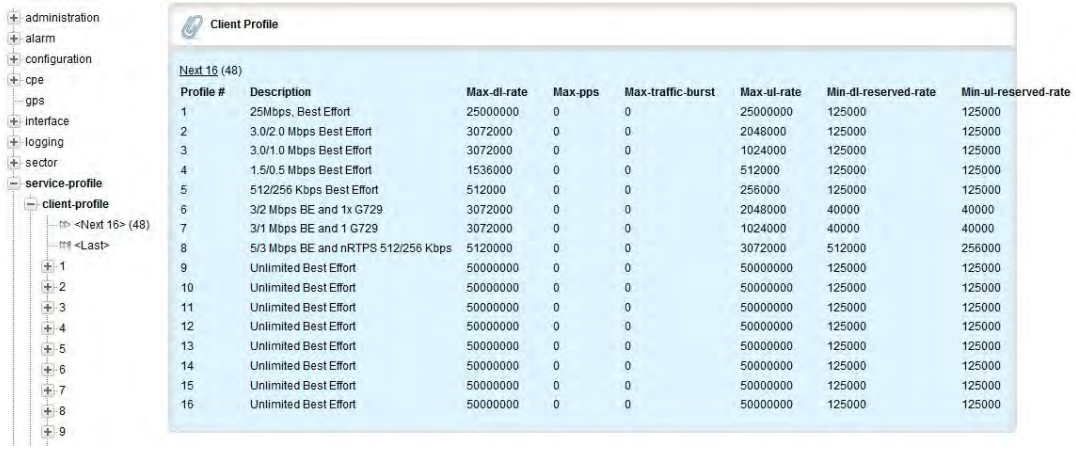


Figure 117 Quality of Service Edit Capability

3.5.5.5 Client Profile

A Client Profile is a set of Service Flows that correspond to a specific Service Level Agreement assigned to a customer. The system allows up to 64 Client Profiles and each Profile must be configured with an Uplink and a Downlink Service Flow.

At Main Web GUI Interface Screen select the ***Configuration*** Tab, then the ***service-profile*** main menu option for a summary page (Figure 118).



Profile #	Description	Max-dl-rate	Max-pps	Max-traffic-burst	Max-ul-rate	Min-dl-reserved-rate	Min-ul-reserved-rate
1	25Mbps, Best Effort	25000000	0	0	25000000	125000	125000
2	3.0/2.0 Mbps Best Effort	3072000	0	0	2048000	125000	125000
3	3.0/1.0 Mbps Best Effort	3072000	0	0	1024000	125000	125000
4	1.5/0.5 Mbps Best Effort	1536000	0	0	512000	125000	125000
5	512/256 Kbps Best Effort	512000	0	0	256000	125000	125000
6	3/2 Mbps BE and 1x G729	3072000	0	0	2048000	40000	40000
7	3/1 Mbps BE and 1 G729	3072000	0	0	1024000	40000	40000
8	5/3 Mbps BE and nRTPS 512/256 Kbps	5120000	0	0	3072000	512000	256000
9	Unlimited Best Effort	50000000	0	0	50000000	125000	125000
10	Unlimited Best Effort	50000000	0	0	50000000	125000	125000
11	Unlimited Best Effort	50000000	0	0	50000000	125000	125000
12	Unlimited Best Effort	50000000	0	0	50000000	125000	125000
13	Unlimited Best Effort	50000000	0	0	50000000	125000	125000
14	Unlimited Best Effort	50000000	0	0	50000000	125000	125000
15	Unlimited Best Effort	50000000	0	0	50000000	125000	125000
16	Unlimited Best Effort	50000000	0	0	50000000	125000	125000

Figure 118 Client Profile Summary

For details navigate further to the ***client-profile*** main Menu Sub-Element. This User is presented with up to 64 profiles. To physically view all the profile configuration parameters then the User must actually select a profile and three main grouping sections are presented (Figure 119).

Figure 119 Client Profile

The main grouping sections are:

- ***Key settings***. This simply displays:
  - ***Profile #***
- ***Client Profile***. This displays all that the available configuration parameters. These are:
  - ***Description***. This is the profile description and it is a text field.
  - ***Max-dl-rate***. This is a Maximum Downlink Rate that is reserved for this client. This is assigned in bits per second in the range 0 to 4294967295.
  - ***Max-pps.*** This is a Maximum Packets per second. This is assigned as a number in the range 0 to 65535.
  - ***Max-traffic-burst***. This is a Maximum Client Traffic Burst. This is as a number in the range 0 to 4294967295.
  - ***Max-ul-rate***. This is a Maximum Uplink Rate for this client. This is assigned in bits per second in the range 0 to 4294967295.
  - ***Min-dl-reserved-rate***. This is a Minimum Downlink Rate that is reserved for this client. This is assigned in bits per second in the range 0 to 4294967295.
  - ***Min-ul-reserved-rate***. This is a Minimum Uplink Rate for this client. This is assigned in bits per second in the range 0 to 4294967295.
  - ***Name***. This is the profile name and it is a text field.
  - ***Num-sflow***. This is the Number of Service Flows for the Client Profile. This is as a number in the range 1 to 16.

- ***Priority.*** This is the Traffic Priority for this Client. This is assigned as a number in the range 1 to 8.
- ***Service Flow Profile***. This lists all the Service Flow Profiles. The configurable parameters for each Service Flow Profile are:
- ***Profile #.*** This is the number of the Service Flow profile.
- ***Name.*** This is the name of the Client profile.
- ***Description.*** This is the text description of the Client profile.
- ***Direction***. This is the direction of the traffic flow.
- ***Arq-profile-num.*** This is the number of the arq profile that has been assigned for this Service Flow Profile.
- ***Cls-profile-num.*** This is the number of the classifier profile that has been assigned for this Client Profile.
- ***Harq-profile-num.*** This is the number of the harq profile that has been assigned for this Client Profile.
- ***Qos-profile-num.*** This is the number of the QoS profile that has been assigned for this Client Profile.

To define a Client profile then the User must be in the Edit Mode. There are two ways to edit and configure a Client Profile.

1. At the Main Web GUI Interface Screen select the ***Configuration*** Tab, then the ***service-profile*** Main Menu Option and then the ***client-profile*** Main menu Sub Element. This User must then select the Client Profile that they wish to configure and scroll down to the bottom of the Window. They will be presented with the Service Flow Profile (Figure 120). If the User enters the Edit Mode, then at the end of each profile the ***Edit*** and ***Delete*** Command Menu Options will appear. The User can select the Edit Command Menu option and they will be navigated into the Edit Mode.

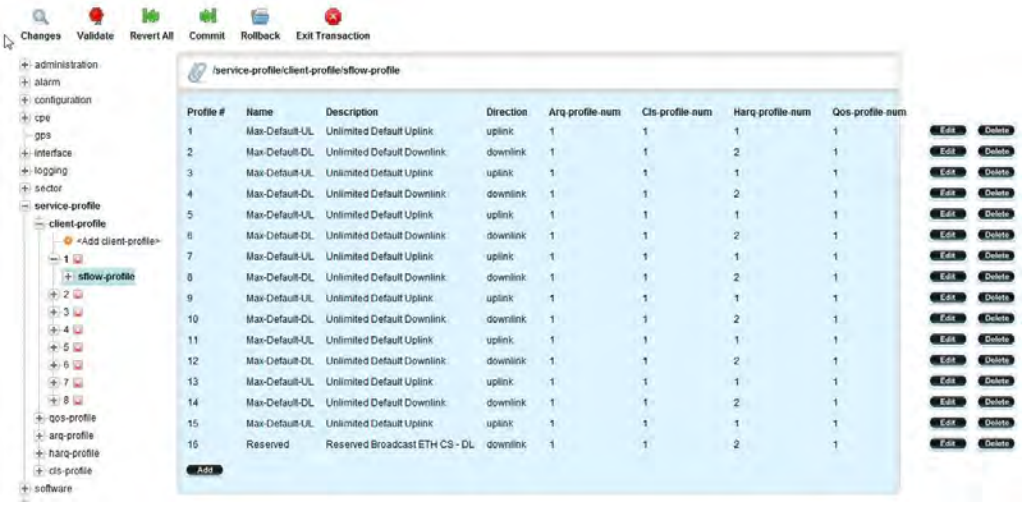


Figure 120 Client Profile Edit Capability

2. The User can navigate direct to the Service Flow Profile options. At the Main Web GUI Interface Screen select the ***Configuration*** Tab, then the ***service-profile*** Main Menu Option, then the ***client-profile*** Main Menu Sub-Element, then the relevant ***profile #,*** then ***sflow-profile*** and finally the ***relevant profile #.*** The User is presented with two main grouping sections. The User must be in

Edit Mode to configure any of the parameters (Figure 121). When in Edit Mode if the User navigates to the red icon then this will present the User with the ability to delete the profile.

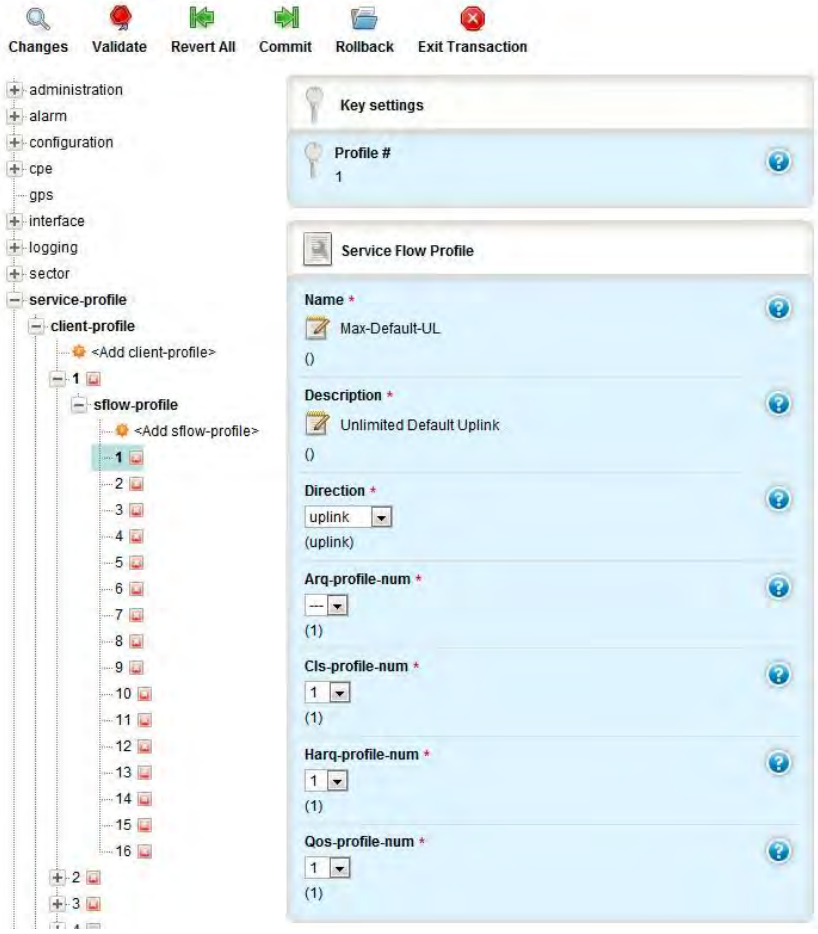


Figure 121 Client Profile Edit Full Capability

The main grouping sections are:

- ***Key settings***. This simply displays:
  - ***Profile #***
- ***Service Flow Profile***. This displays all that the available service flow parameters. These are:
  - ***Name***. This is the Service Flow name and it is a text field.
  - ***Description***. This is the Service Flow description and it is a text field.
  - ***Direction***. This is the direction of traffic flow for the Service Flow. The options are downlink or uplink.
  - ***Arq-profile-num***. This is the ARQ Profile Number that is used by this Service Flow. The options are any of the 3 ARQ profiles that have been configured in the ARQ Profile configuration (refer to section 3.5.5.3).
  - ***Cls-profile-num***. This is the CLS Profile Number that is used by this Service Flow. The options are any of the 64 CLS profiles that have been configured in the CLS Profile configuration (refer to section 3.5.5.1).

- ***Harq-profile-num***. This is the HARQ Profile Number that is used by this Service Flow. The options are any of the 6 HARQ profiles that have been configured in the HARQ Profile configuration (refer to section 3.5.5.2).
- ***Qos-profile-num***. This is the QoS Profile Number that is used by this Service Flow. The options are any of the 32 QoS profiles that have been configured in the QoS Profile configuration (refer to section 3.5.5.4).

3.5.5.6 CPE Provisioning Using a AAA Server

Alternatively, the AAA (authentication, authorization and accounting) Server may be used perform CPE provisioning. This will allow configuration of most of the CPE configuration parameters including

- CPE Configuration including MAC, CS Sublayer, Client Profile, Maximum Uplink and Downlink Rate
- IP Settings including IP Address, Subnet mask,
- Customer ID is not supported

To enable AAA provisioning, enable the option in the Web GUI. At the Main Web GUI Interface Screen select the ***Configuration*** Tab, then the ***system*** main menu option and then the ***base-station*** main Menu Sub-Element. This User is presented with the Base Station settings. To enable AAA provisioning, change the Mode from ***standalone-local*** to ***standalone-aaa-prov*** (Figure 122).

Additionally, the following parameters are required to be configured (Figure 123).

- AAA (Radius) server ip address,
- AAA (Radius) server port number
- AAA (Radius) server secret,
- Provisioning realm: This parameter distinguishes between AAA provisioning vs AAA authentication while editing “users” file on AAA server.

Mercury provides a customer specific AAA dictionary file which needs to be included with the AAA server and enable the service to properly format and send the provisioning information to the Base Station. Please contact Customer Support for further documentation on how to set-up and configure the AAA server.

Figure 122 AAA Server Configuration on Base Station

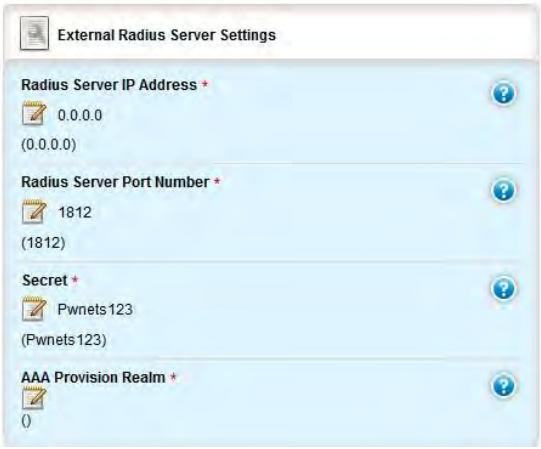


Figure 123 AAA Server Configuration on Base Station continued

3.5.5.7 Advanced VLAN Capabilities

The Quantum Base Station has advanced Virtual LAN (or VLAN) capabilities as defined by IEEE 802.1q and 802.1p. The VLAN tags are a numerical header applied to an Ethernet frame in order to segregate a physical Ethernet segment into logical networks. The advantages of using a VLAN are the following:

- Quality of Service (Qos) capabilities at Layer 2 allows different types of traffic to be placed on different VLANs for segmentation. E.g. Voice, video and data traffic can be assigned different VLANs
- Security to isolate user traffic from each other and keep management traffic separate
- Network Optimization to reduce broadcast storms and end user devices affecting the entire network.

3.5.5.8 VLAN for Management Traffic

VLAN Management may be configured on the Base Station. Care must be taken to ensure this is configured correctly. All management traffic will accept management VLAN only including the Web GUI, FTP, SNMP, Telnet, Radius, SSH, R6 Control path and NTP. See section 3.5.3.5 for further information on configuring the management VLAN.

3.5.5.9 VLAN for Data Traffic

In order to configure VLAN operations, the Base Station must be configured in Ethernet CS – Stand Alone Mode. There are three modes of operation available that are configured from the VLAN profile.

- Transparent mode where the CPE (or devices behind the CPE) are performing tagging and untagging
- Per CPE Basis (per-mss) where a specific VLAN ID is assigned to a specific CPE from the Base Station side. On the CPE side there is no device with VLAN support, and this is transparent to the user.
- Service Flow (per-sf) basis where individual service flows are assigned a specific VLAN ID. This is useful for enforcing QoS policies and requires advanced configuration, classification and planning for implementation.

Figure 124 VLAN Modes of Operation

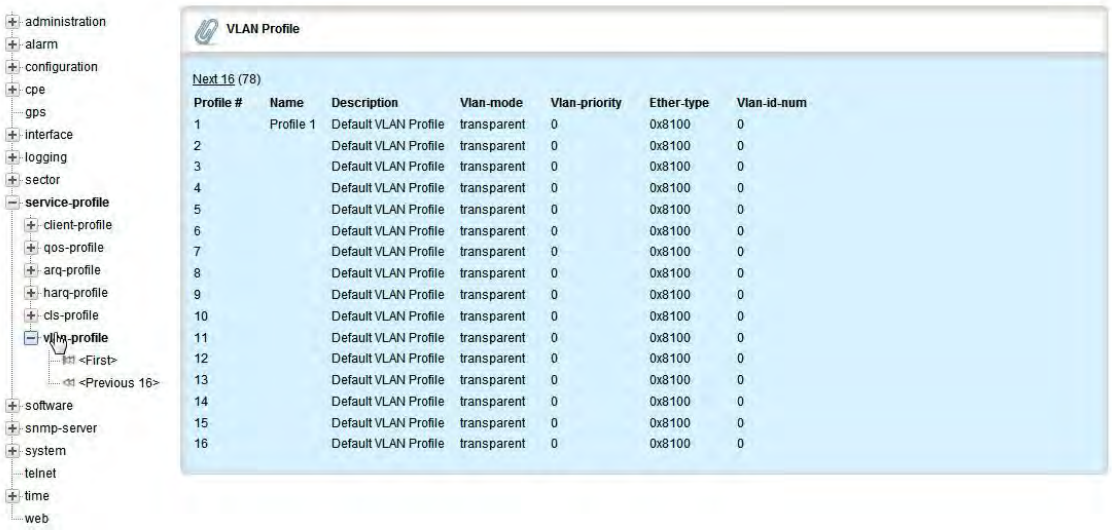


Figure 125 VLAN Profile List

To configure ***VLANs for data traffic***, select the ***Configuration*** Tab and then select the ***service profile*** Main Menu Option and then vlan-profile (Figure 125).

1. To enable first select ***Edit Private*** or ***Edit Exclusive***. This will place the User into the Edit mode The User can add a profile or modify an existing one (Figure 126).
2. Enter a profile number (as below) or select an existing profile to edit

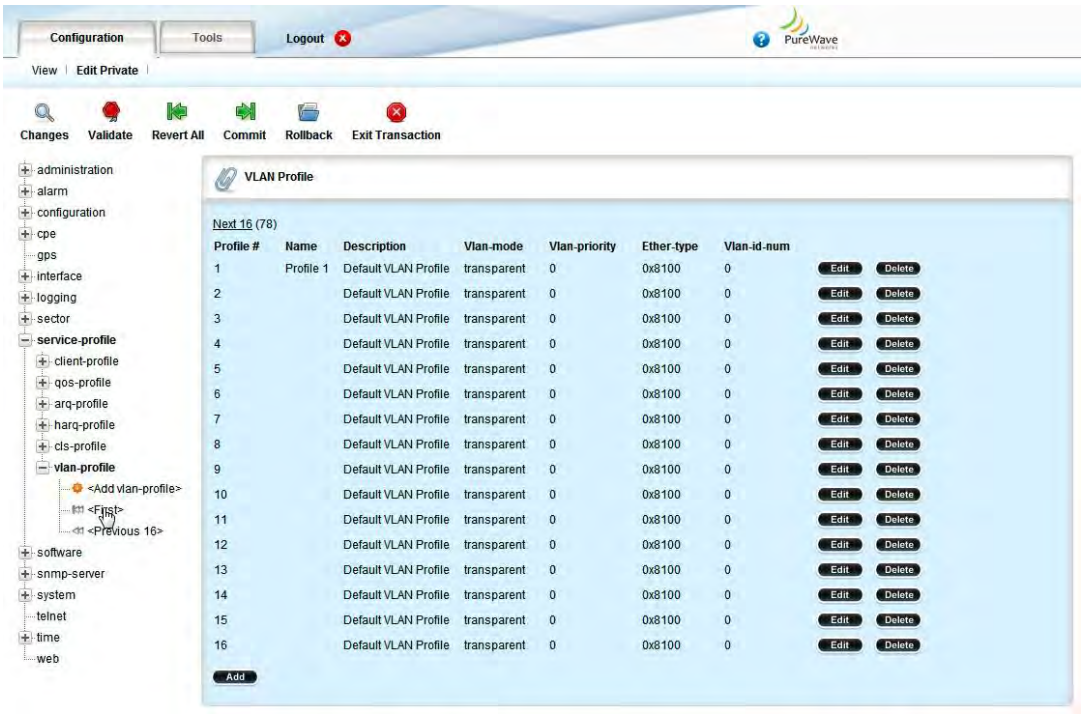


Figure 126 VLAN Profile Edit Mode

Figure 127 VLAN Profile Number

3. The User is now presented with a window that displays the following parameters. With the configuration below, it is assumed that the CPEs and Base Station have their VLAN tagging/untagging performed by other devices either behind the CPE or Base Station.
   - VLAN Profile Number. This parameter is a number between 1-94. It is recommended to leave Profile 1 unchanged.
   - Name/Description. Description for the VLAN Profile
   - VLAN Mode. Depending on your configuration, set this mode to *Transparent*, per-sf or per-mss
   - VLAN Priority. The priority bit (0-7) inside the VLAN Packet that will be sent out with (from the BST).
   - VLAN ID. The VLAN ID (0-4094) that the Packet will be sent out with (from the BST) and/or be expected to be received (from the Backhaul).
   - Ether Type. The Ethernet Type of the Packet that will be sent out with (from the BST) and/or expected to be received with). Valid Range is: 0x8100(802.1q), 0x9100/0x9200/0x9300/0x88a8 (QinQ).

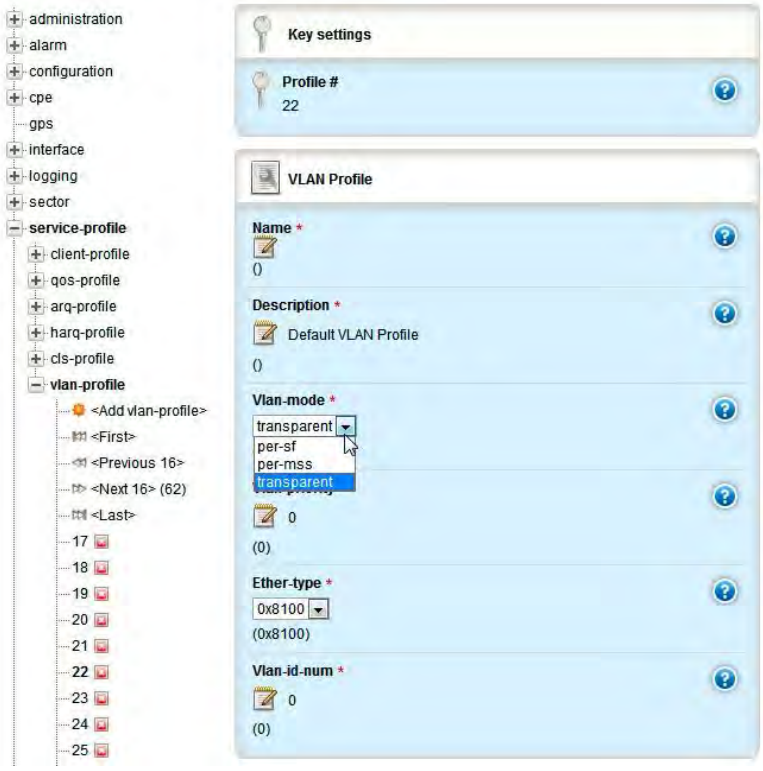


Figure 128 VLAN Profile Configuration

4. The User must ***Commit*** the changes (apply the configuration in run-time). To Commit, select the ***Commit*** option. A prompt screen will appear directing the User to confirm the pending configuration changes. To proceed the User must select ***Cancel*** or ***OK***.

The ***transparent*** mode configuration may also be used in combination with management VLAN where the system management interface VLAN is configured with a separate VLAN id. This will allow the management traffic to be isolated from data traffic.

In the ***Per CPE Basis*** (or per-mss) mode, the CPE will automatically have its traffic tagged with the configured VLAN ID for traffic leaving the base station. This configuration may also be used in combination with management VLAN where the system management interface VLAN is configured with a separate VLAN id. This will allow the management traffic to be isolated from data traffic. Additionally, a per Service Flow VLAN may be used in combination with this configuration providing that the VLAN classification rules are set correctly.

In the ***Per Service Flow Basis,*** the CPE will automatically have its traffic tagged with the configured VLAN ID for traffic leaving the base station. This configuration may also be used in combination with management VLAN and the per-CPE based configuration.

3.5.5.10 VLAN Classification

To configure the tagging options for per-CPE and per-SF basis, classification rules must be configured. The options for VLAN classification includes:

- CLS-priority (classifier priority)
- CLS-priority-used
- MAC-addr-option
- MAC-address-OUI

For further information on configuring a classifier for VLAN, please see section 3.5.5.1.

To apply a default VLAN profile to a CPE, please see section 3.5.4.

3.5.5.11 VLAN QinQ Configuration

QinQ (or double-tagging) allows multiple VLAN headers to be inserted into a single frame. This configuration allows the service provider to manage data traffic with their own ID and shield the VLAN ID of the user, so as to save the public network VLAN ID resource of the service provider. This configuration mode is used on the per CPE or per Service Flow basis.

To set QinQ configuration:

- **VLAN Profile Number**. This parameter is a number between 1-94.
- **Name/Description**. Description for the VLAN Profile
- **VLAN Mode**. Set this mode to *per-sf* or *per-mss* mode
- **VLAN Priority**. The priority bit (0-7) inside the VLAN Packet that will be sent out with (from the BST).
- **VLAN ID**. The VLAN ID (0-4094) that the Packet will be sent out with (from the BST) and/or be expected to be received (from the Backhaul).
- **Ether Type**. To configure QinQ set the Ether Type to 0x9100/0x9200/0x9300/0x88a8.

3.6 Base Station Software Upgrade

One of the Base Stations' key features is that it has been designed to support a "Software Defined Radio" (SDR) architecture. The distinct advantage is that a Base Station can be remotely upgraded with additional features and capabilities as these are developed. The Base Station maintains two software versions/images that may be selectively enabled, thus providing a fail-safe software upgrade procedure.

The software upgrade process may be performed from the CLI, the Web Interface, as well as from the PureView EMS. In this section, the software upgrade procedures using the Web Interface is detailed.

The first step in the process is to copy the software to a directory on the PC which is running the FTP server. Please ensure the Mercury directory structure is kept intact. Copy the software image, as provided by Mercury, to the assigned home directory of the FTP server (Figure 129).

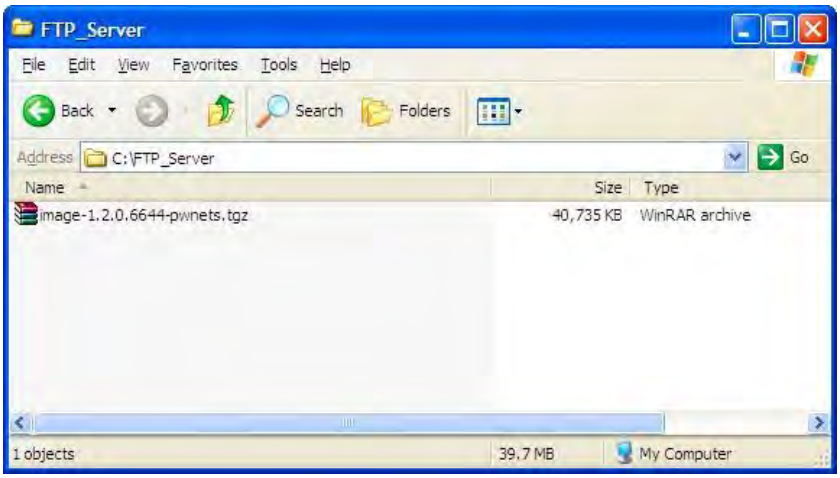


Figure 129 Software Components

The next step is to confirm and setup the FTP Server. There are several free commercially available FTP Servers that can be used (Figure 130) such as 3CDaemon. Ensure that the FTP Server is running.

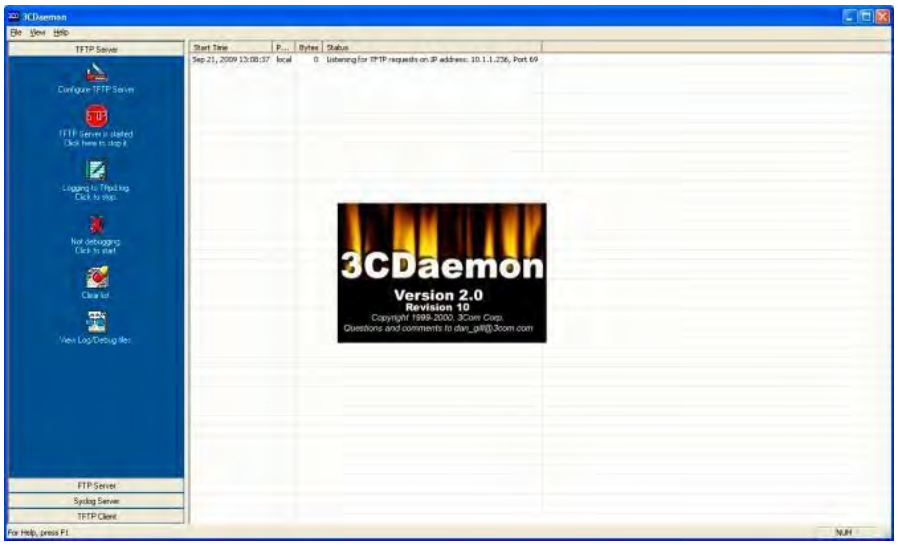


Figure 130 FTP Server Configuration

At the Main Web GUI Interface Screen select the ***Configuration*** Tab and then the ***software*** Main Menu Option. This will display the software Settings and the display is split into two main grouping sections. There are three further sub-element associated with this option. There are no User configurable options for the ***software*** Main Menu Option.

The Base Station flash contains two partitions which are both loaded with software. There is a Bank "A" and a Bank "B". The GUI will provide an indication as to current status of the software.

The two main grouping sections for this Menu Main Sub-Element are (Figure 131):

- ***Software Image Management***. This displays the details for each software image. The options are:
  - ***Current Boot Bank***. This indicates which bank provided the current running software load.
  - ***Next Boot Bank***. This indicates after the next reboot of the Base Station, which bank the software will be loaded from.
  - ***Boot Bank A***. This indicates the software revision that is currently loaded into bank A.
  - ***Boot Bank B***. This indicates the software revision that is currently loaded into bank B.
  - ***Sw Version Candidate***. This is not relevant for the current method of software upgrade. It will simply indicate "No Software candidate available".
- ***Software Image Status***. This provides an indication of the download status. The options are:
  - ***State Detail***. This will provide an indication of the current state of software upgrade detail.
  - ***Download Progress***. This is a percentage indicator of the state of download progress.

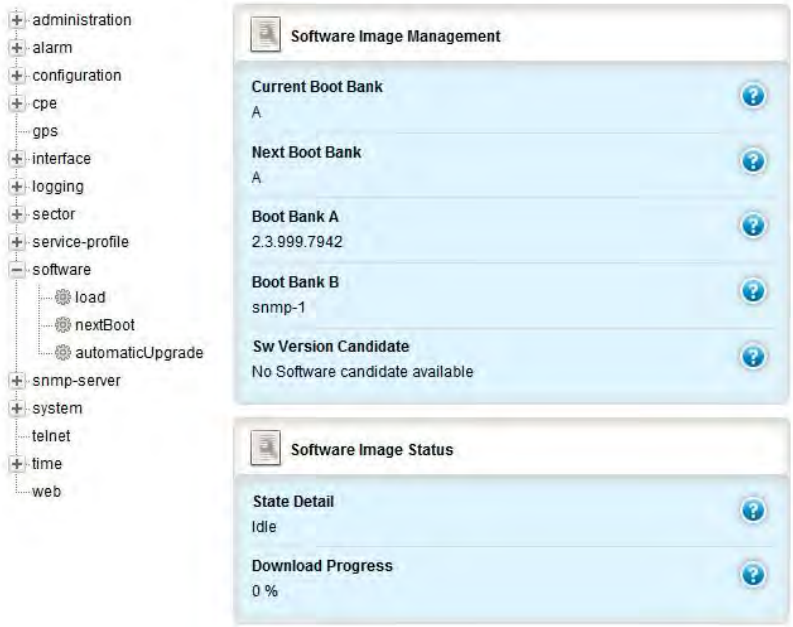


Figure 131 Software Image Management Dialog

3.6.1 Automatic Upgrade

The Base Station software upgrade process can be performed using a single automatic operation. This performs the following procedure while providing continual upgrade status to the User.

1. Loads the software image file from a user defined location using FTP, HTTP, or HTTPS.
2. Unpacks the downloaded software image, verifies the image integrity (CRC and MD5 checksum), and prepares for installation.
3. Performs operations to distribute the software image to the various components of the Base Station.
4. Selects the new software image installed as the partition to be used after the next Base Station reboot.
5. Reboots the Base Station.

To execute the Single-Step Software Upgrade Procedure, at the Main Web GUI Interface Screen the ***Configuration*** Tab, then the ***software*** Main Menu Option and then the ***automaticUpgrade*** Main Menu Sub-Element. The User will be presented with two main grouping sections (Figure 132).

In the ***Load selected image from server, set nextBoot bank*** and ***Reboot*** section, enter the URL of the new software image in the *SW Image URL* box. There are a variety of formats of the URL of remote source file is. These can be displayed if the User selects the "help" key. These URL formats are defined as:

- ftp://[user[:password]@]hostname[:port]/filepath
- http://hostname[:port]/filepath
- https://hostname[:port]/filepath

Where [ ] indicates optional items. Thus,

- user:password@ is optional, and the :password part can be omitted
- [:port] is also optional

Examples using ftp (you can substitute http or https):

- ftp://myhost.com/filename
- ftp://myhost.com/directory/filename
- ftp://myhost.com:2323/directory/filename
  ftp://myname@myhost.com:2323/directoryname/filename
  ftp://myname:password@myhost.com:2323/directoryname/filename

URL of remote source file; format is as follows:

- protocol://[user[:password]]@host[:port]/path protocol can be ftp, http, or https

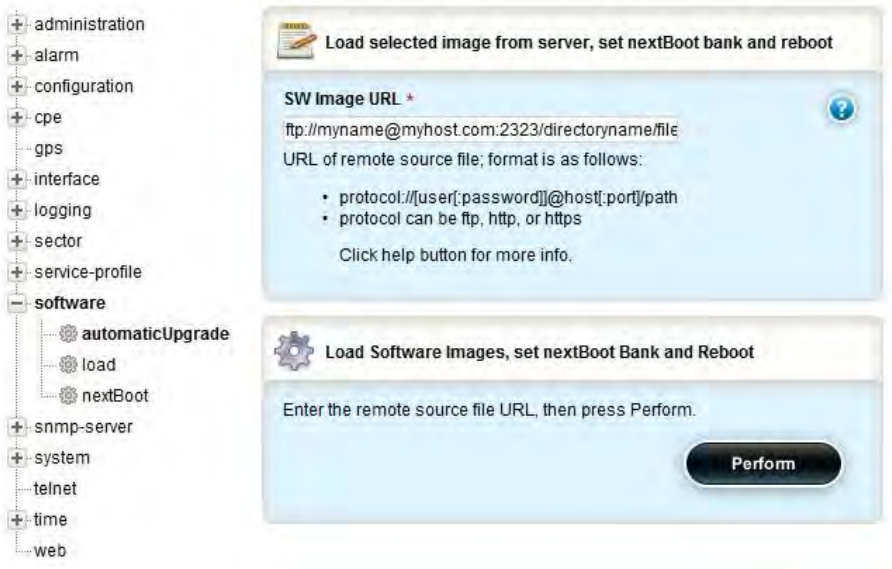


Figure 132 Single-Step Software Upgrade Dialog

Once the URL has been entered, the User must select the *Perform* Command Menu Option in the ***Load selected image from server, set nextBoot bank,*** and ***Reboot*** section to initiate the upgrade process. This action will upgrade the Base Station in one simple step.

3.6.2 Manual Software Upgrade

The Base Station software upgrade process can also be performed in two steps as an alternative to the automatic process. This will present the User with control over the various stages of the software upgrade process.

3.6.2.1 Loading Software

In this procedure the following steps are performed:

1. Loads the software image file from a user defined location using FTP, HTTP, or HTTPS.
2. Unpacks the downloaded software image, verifies the image integrity (CRC and MD5 checksum), and prepares for installation.
3. Performs operations to update the flash partition.

The first step is the software download and installation procedure. At the Main Web GUI Interface Screen select the ***Configuration*** Tab, then the ***software*** Main Menu Option and then the ***load*** Main Menu Sub-Element. The User will be presented with two main grouping sections (Figure 133).

In the ***Download*** and ***Install Software Images*** section, then enter the URL of the new software image in the ***SW Image URL*** box. Please see section 3.6.1 for syntax and examples of URLs that may be used.

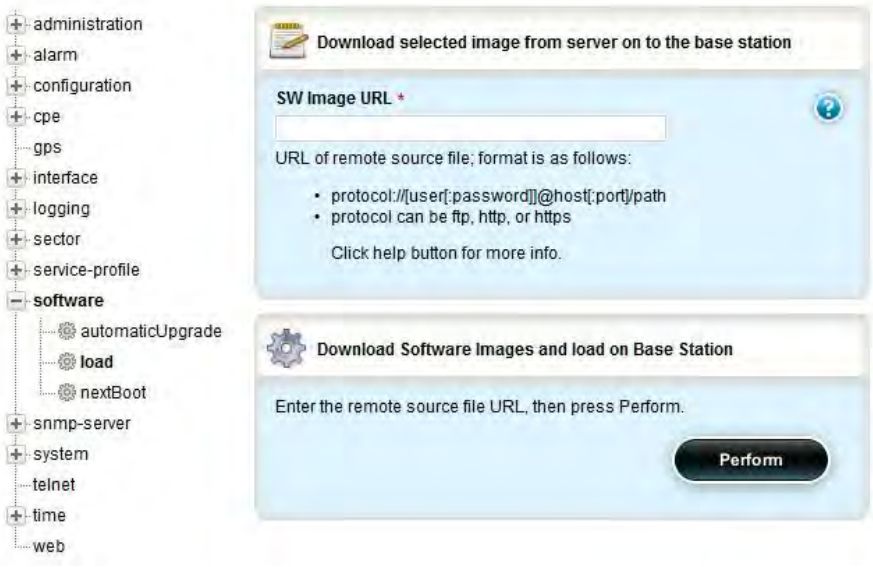


Figure 133 Software Load Menu Option

Once the URL has been entered, the User must select the ***Perform*** Command Menu Option in the ***Download Software Images from server on Base Station*** section to initiate the software load process.

3.6.2.2 NextBoot Image Bank Selection

The final step in the Multiple Step Software Upgrade process is the next boot partition selection and display procedure.

At the Main Web GUI Interface Screen select the ***Configuration*** Tab, then the ***software*** Main Menu Option and then the *boot* Main Menu Sub-Element. The User will be presented with the option to select the ***next image bank to boot from*** (Figure 134):

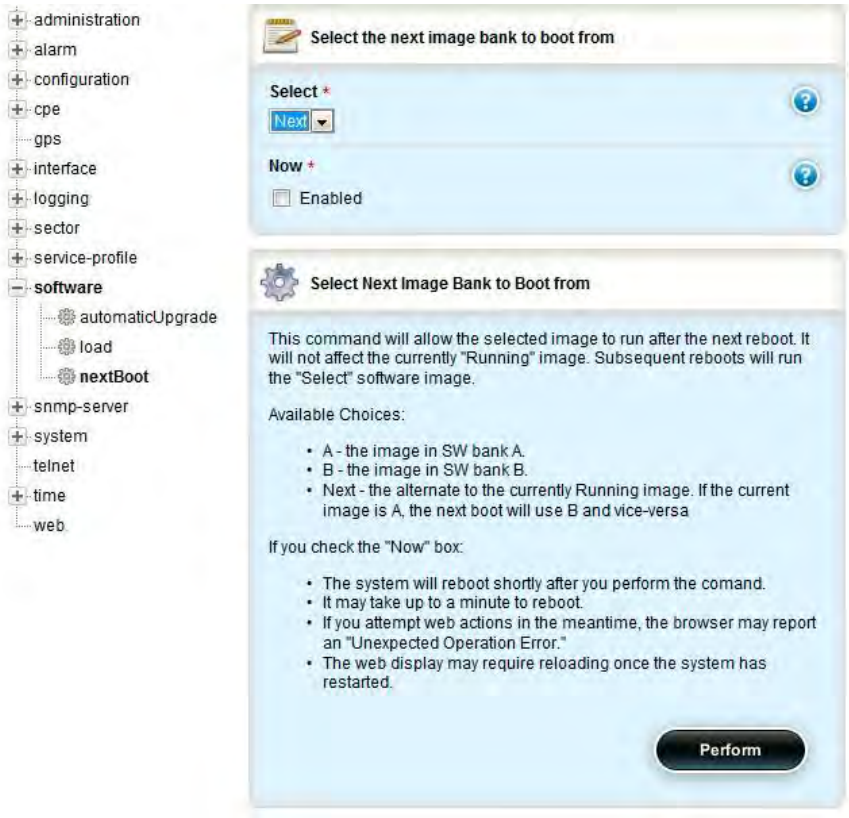


Figure 134 Software Image Bank Selection Display

The purpose of the ***Select Next image bank to boot from*** is to specify the selected image to run after the next reboot. It will not affect the currently "Running" image. Subsequent reboots will run the "Selected" software image (Figure 135). The available choices are:

- **A**: The image loaded in image bank A.
- **B**: The image loaded in image bank B.
- **Next**: The alternative to the currently "Running" image. If the current image is A, the next boot will use B and vice versa.
- ***Now***. This is a check box that must be enabled to perform automatic reset.

Figure 135 Software Image Partition Selection

3.6.3 Base Station Performance Monitoring

There are several monitoring parameters that can be checked to determine the overall performance of the Base Station and for any Subscribers that are connected to the Base Station. These parameters are contained within a variety of menu options.

The User's starting point is Web GUI Main Web GUI Interface Screen.

3.6.3.1 Interface

At Main Web GUI Interface Screen select the ***Configuration*** Tab and then the ***interface*** Main Menu Option this will display the key settings window. This window details enabled the configuration of the backhaul interfaces There are two Main Menu Sub-Elements to this window and the window is split into two main grouping sections (Figure 136).

Figure 136 Performance Monitoring Interface

The Main Menu Sub-Elements are:

- ***configure***. This configures the backhaul interfaces speed and mode of operation
- ***status***. This describes the configured settings and the current status of these interfaces.
- ***Backhaul learning***. Ethernet devices learned from backhaul
- ***Interface Settings and Status***. The configured settings and their current status that are displayed for the five interfaces are:
    - ***Admin State***. This is the admin state
    - ***Oper State***. This is the operational state
    - ***Link Speed***. This is the interface link speed
    - ***Duplex Type***. This is duplex status

- ***Autoneg***. This is autonegotiate setting
- ***Maximum MTU Length***. This is the maximum configured MTU Length
- ***MAC Address***. This is the MAC address of the interface

At the Main Web GUI Interface Screen select the ***Configuration*** Tab and then the ***interface*** Main Menu Option, then the ***status*** main Menu Sub-Element. The resulting window will be split into two main sections (Figure 137). These are:

- ***Key Settings.***
  - ***Name***. This will indicate which interface is being displayed
- ***Interface Statistics and Status***. The following settings and status are displayed. These are not editable parameters.
  - ***Admin State***. This is the admin state
  - ***Oper State***. This is the operational state
  - ***Link Speed***. This is the interface link speed
  - ***Duplex Type***. This is duplex setting
  - ***Maximum MTU Length***. This is the maximum configured MTU Length
  - ***MAC Address***. This is the MAC address of the interface

Figure 137 Interface Status Key Settings and Status

The same format is repeated for all interfaces and therefore only one will be outlined. To view the Interface Statistics of another interface then simply at the Main Web GUI Interface Screen select the ***Configuration*** Tab, then the ***interface*** Main Menu Option, then the ***status*** Main Menu Sub-Element and then relevant interface.

To view ***Backhaul Learning*** table, at the Main Web GUI Interface Screen select the ***Configuration*** Tab and then the ***interface*** Main Menu Option, then the ***backhaullearning*** main Menu Sub Element. The resulting window will be split into two main sections (Figure 138). These are:

- **MAC**. The MAC Address of the device learned.
- **Port**. The backhaul port where the device was learned from.
- **IP Address**. The IP address of the device. Applicable only in case of IP CS Stand Alone mode.
- **Ageing**. The time in seconds since the last packet was received from the device. There is 300 sec ageing.

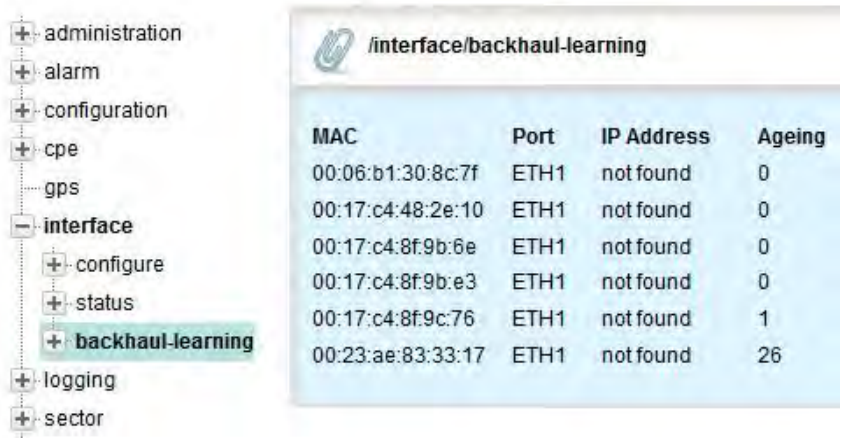


Figure 138 Backhaul Learning

To view an individual ***Backhaul Learning*** entry from the table, at the Main Web GUI Interface Screen select the ***Configuration*** Tab and then the ***interface*** Main Menu Option, then the ***backhaul-learning*** main Menu Sub-Element followed by the MAC address of the device (Figure 139).

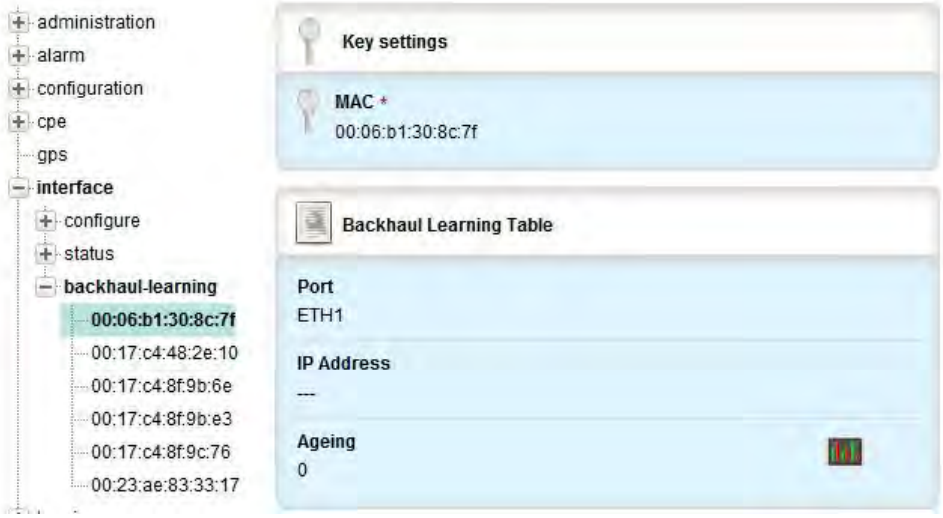


Figure 139 Backhaul Learning Table Entry

3.6.3.2 Sector Statistics

At the Main Web GUI Interface Screen select the ***Configuration*** Tab and then the ***sector*** Main Menu Option. This will display the Sector Settings window (Figure 140). There are no parameters to edit within the ***sector*** Main Menu Option.

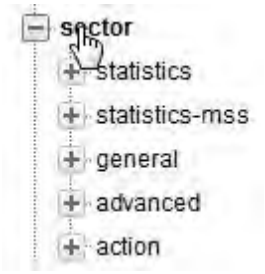


Figure 140 Sector Statistics

When you select, Statistics, the further sub-elements are:

- ***throughput-counters***. Sector throughput counters are displayed.
- ***startup-counters***. These are startup counters for a sector level.
- ***packer-error-rate-metrics***. This will display several key packet error rate counters.
- ***Sector Advanced Settings (configured)***
- ***Sector Provisioning (configured)***

Important sector statistics are contained within two options within the Sector Main Menu Option. The User now must navigate to the next level, therefore at the Main Web GUI Interface Screen select the ***sector*** main Menu option and then the ***statistics*** Main Menu Sub-Element. There are four further sub elements to this option and the window is split into four main grouping sections (Figure 141).

The main grouping sections provide a summary of the information that can be obtained by selecting and navigating down into the Menu Sub-Element level.

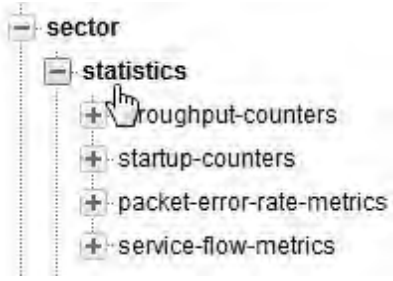


Figure 141 Sector Statistics Interface Key Settings

The further sub-elements are:

- ***service-flow-metrics***. Several key service flow metrics are provided at a sector level (i.e. a Base Station level).

To fully display all the available statistics the User now has to navigate to the next level, therefore at the Main Web GUI Interface Screen select the ***Configuration*** Tab and then the ***sector*** Main Menu Option then the ***statistics*** Main Menu Sub-Element, then ***service-flowmetrics*** and then ***1***. This will display the Metrics window. There are two distinct groups to this window (Figure 142).

- ***Key Settings***. This indicates the relevant sector, which as has been described in number 1. This is not a configurable parameter.
- ***Sector Service-Flow Metrics***. The following Metrics are displayed. These are displayed as a raw number but they can also be displayed in graphical form by selecting the "Graph" command button.
    - ***DSA Requests***
    - ***DSA Req Successes***
    - ***DSC Requests***
    - ***DSC Req Successes***
    - ***DSD Requests***
    - ***DSD Req Successes***
    - ***Max Active Svc Flows***
    - ***Max Active DL Svc Flows***
    - ***Max Active UL Svc Flows***

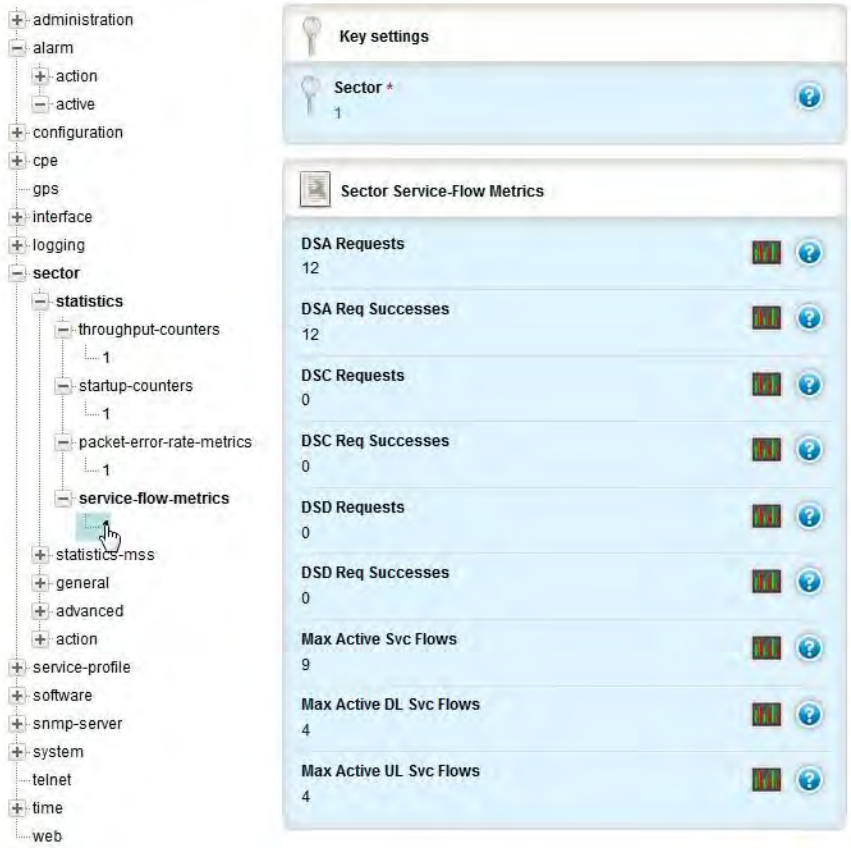


Figure 142 Sector Statistics Interface Key Settings

A similar format is repeated for the other sector, statistics sub elements. The Key Settings window indicates the relevant sector. The information that is presented for each sub element, ***packet-error-ratemetrics, startup-counters*** **and** ***throughput-counters*** is:

- For the ***packet-error-rate metrics*** menu option the following ***Sector Pkt Error-Rate Metrics*** are displayed (Figure 143)*:*
    - ***DL Packets Sent***
    - ***DL Packet Errors***
    - ***DL Pkt Error Rate***
    - ***UL Packets Sent***
    - ***UL Packet Errors***
    - ***UL Pkt Error Rate***
- For the *startup-counters* menu option, the following ***Sector Startup Counters*** are displayed (Figure 144):
    - ***Authentication Attempts***
    - ***Authentication Successes***
    - ***Ranging Attempts***
    - ***Ranging Successes***
    - ***Ranging Periodic***
    - ***Bandwidth Requests***
    - ***Handover Ranging***
- For the ***throughput-counters*** menu option, the following *Sector* ***Throughput Counters*** are displayed (Figure 145):
    - ***DL User Bytes***
    - ***UL User Bytes***
    - ***DL MAC Bytes***
    - ***UL MAC Bytes***
    - ***DL User Packets***
    - ***UL User Packets***
    - ***DL MAC Packets***
    - ***UL MAC Packets***
    - ***DL User Pkt Errors***
    - ***UL User Pkt Errors***
    - ***DL MAC Pkt Errors***
    - ***UL MAC Pkt Errors***

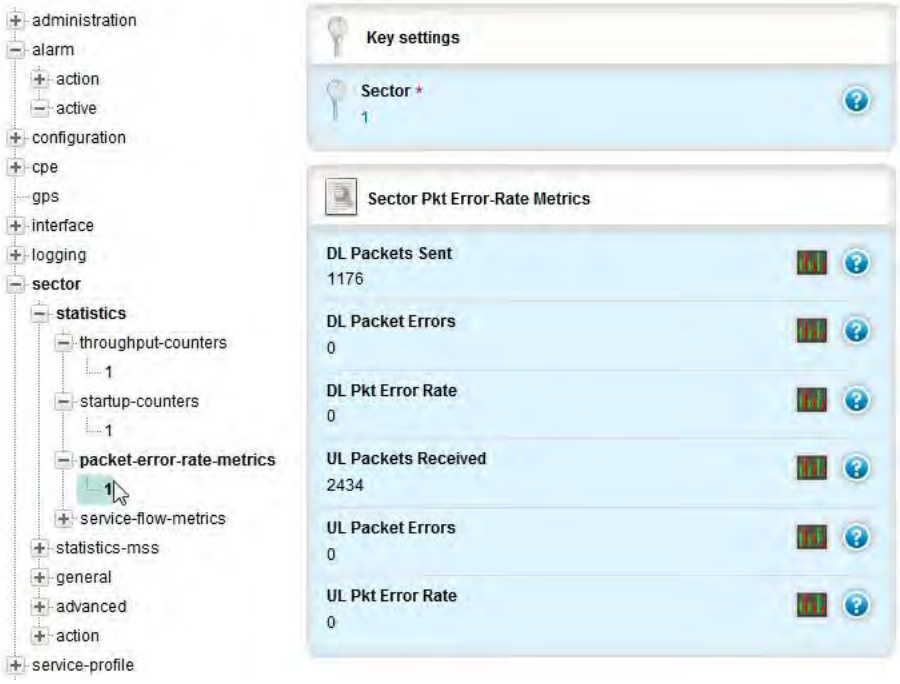


Figure 143 Sector Statistics Packet Error Rate Metrics

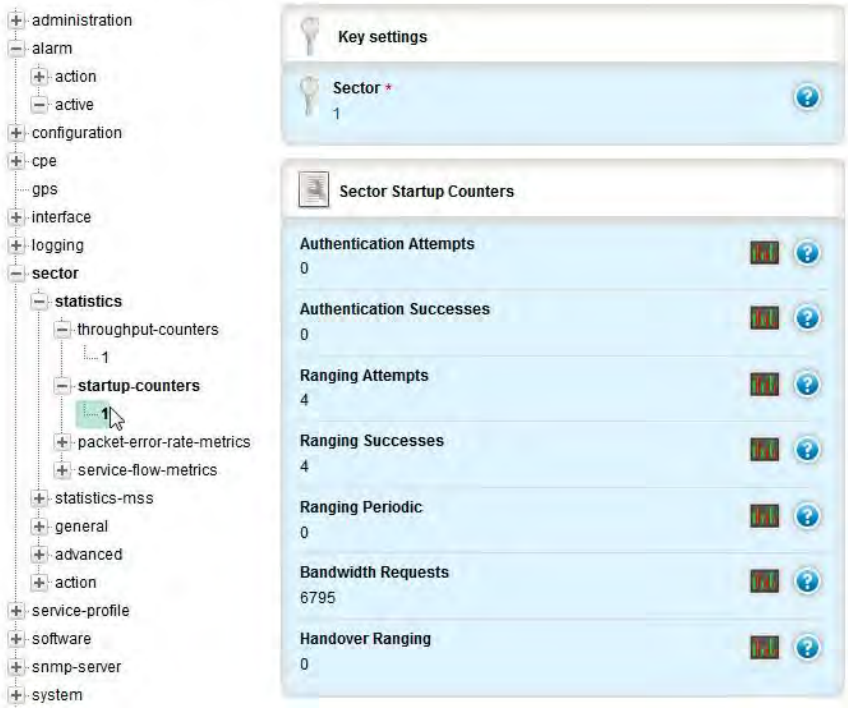


Figure 144 Sector Statistics Startup Counters

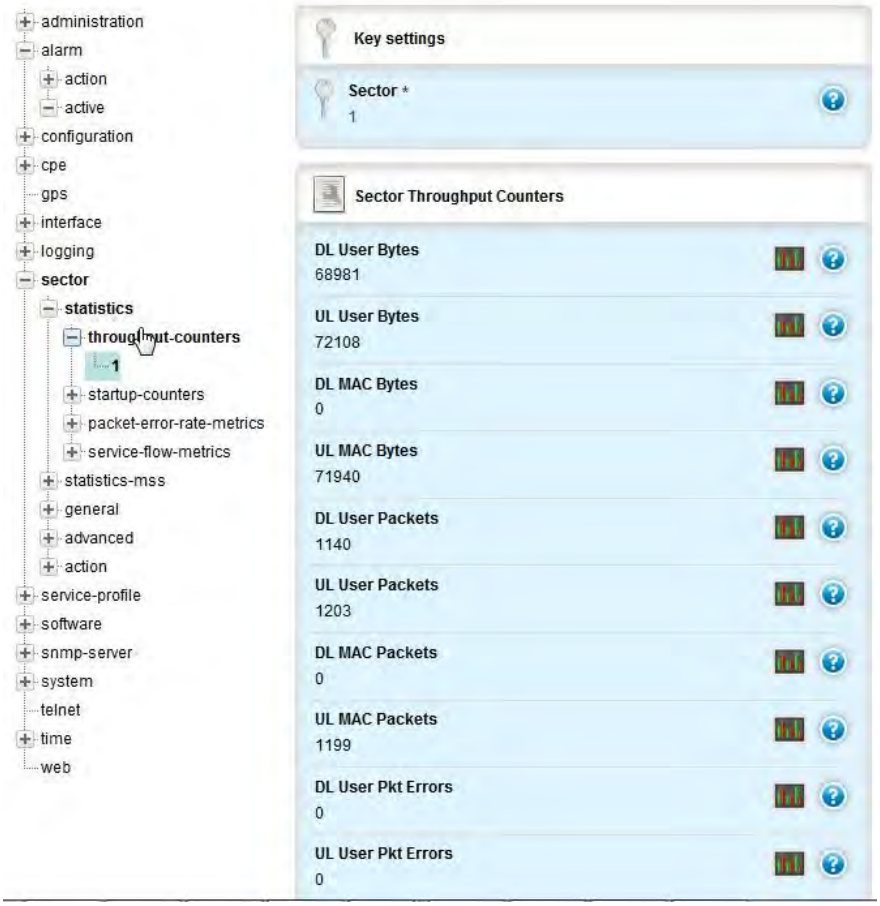


Figure 145 Sector Statistics Throughput Counters

Important Subscriber statistics are contained within the ***statistics-mss*** Main Menu Sub Element within the Sector Main Menu Option. The User now has to navigate to the next level, therefore at the Main Web GUI Interface Screen select the *sector* Main Menu Option and then the ***statistics-mss*** Main Menu Sub-Element. There are seven further sub elements to this option and the windows is split into the seven main grouping sections (Figure 146). The main grouping sections provide a summary of the information that can be obtained by selecting and drilling down into the sub-element level.

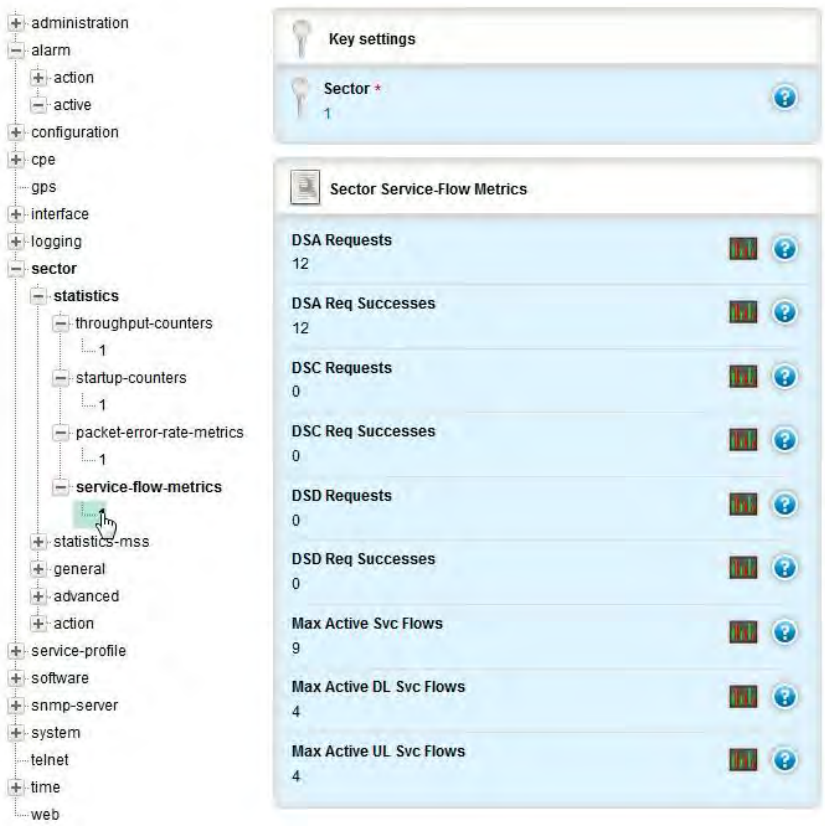


Figure 146 Sector MSS-Statistics Metrics

The further sub-elements are:

- ***mss-throughput-counters***. This is the throughput counters for the Subscribers that are communicating with the Base Station.
- ***sflow-throughput-counters***. These are the throughput counters per service flow.
- ***rssi-cinr-counters***. These are the RSSI and CINR metrics per Subscriber and per upstream/downstream direction.
- ***harq-counters***. These are the HARQ counters per Subscriber.
- ***modulation-code-rate***. These are the Modulation and Coding Scheme (MCS) per Subscriber.
- ***active-service-flows***. These are the active Service flows per Subscriber.
- ***registered-ss***. These are the registered Subscriber Station details.

The seven main grouping sections are the summary for the sub-elements on a per sector basis:

- ***Throughput Counters per MSS***
- ***Throughput Counters Per Service-Flow***
- ***RSSI and CINR Metrics Per MSS***
- ***HARQ Counters Per MSS***
- ***Modulation and Coding Scheme (MCS)***
- ***Active Service Flows***
- ***Registered Subscriber Station***

To fully display all the available statistics the User now has to navigate to the next level, therefore at the Main Web GUI Interface Screen select the ***Configuration*** Tab, then the ***sector*** Main Menu Option, then the ***statistics-mss*** Main Menu Sub-Element and then one of the seven further sub-elements. Under each tree Sub-element a list of all the connected Subscribers will be displayed. The Use has to select the relevant Subscriber and the information will be displayed for the particular Subscriber.

At the Main Web GUI Interface Screen select the ***Configuration*** Tab and then the ***sector*** Main Menu Option, then the ***statistics-mss*** Main Menu Sub-Element and then ***mssthroughput-counters***. There are two distinct groups to this window (Figure 147).

- ***Key Settings***. This indicates the relevant Subscriber. This is not a configurable parameter. The following information is presented:
  - ***Sector***
  - ***MAC Address***
- ***Throughput Counters Per MSS***. The following Metrics are displayed. These are displayed as a raw number but they can also be displayed in graphical form by selecting the "Graph" command button.
  - ***DL Bytes***
  - ***Ul Bytes***
  - ***DL Pkts***
  - ***UL Pkts***
  - ***DL Pkt Err***
  - ***UL Pkt Err***
  - ***Hcs-cnt***
  - ***Crc-cnt***

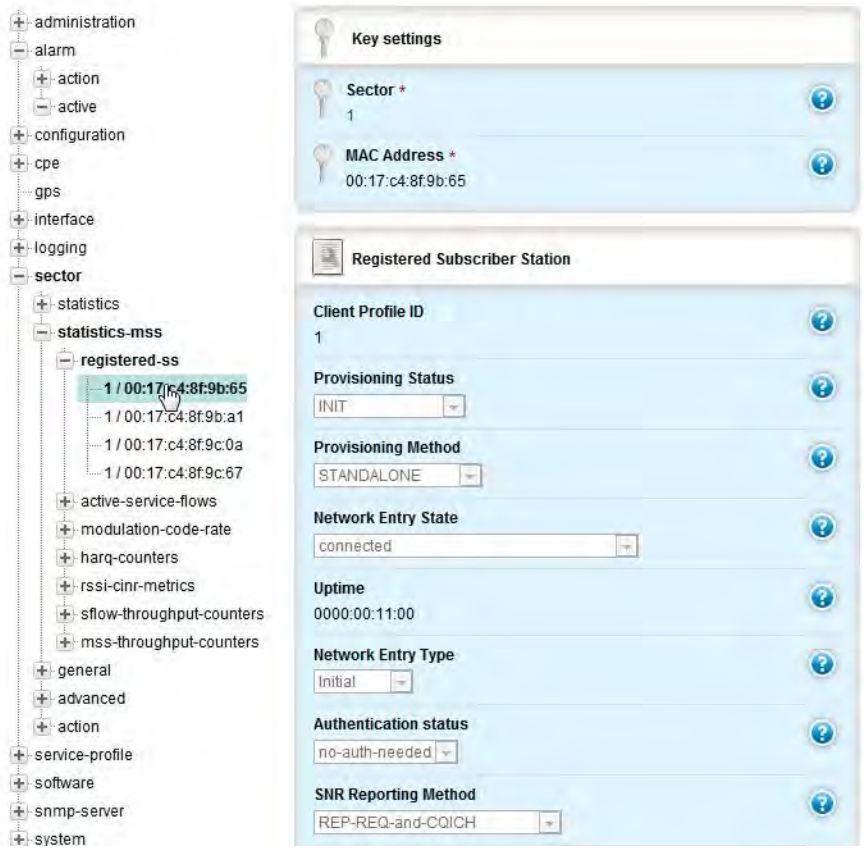


Figure 147 Registered Subscriber Station Throughput Counters

At the Main Web GUI Interface Screen select the ***Configuration*** Tab and then the *sector* Main Menu option, then the ***statistics-mss*** Main Menu Sub-Element and then ***sflowthroughput-counters***. The Service Flows that have been defined for each Subscriber will be displayed. For each Subscriber there will be at least two defined Service Flows, one for Upstream and another for Downstream. There are two distinct groups to this window (Figure 148).

- ***Key Settings***. This indicates the relevant Subscriber. This is not a configurable parameter. The following information is presented:
  - ***Sector***
  - ***MAC Address***
- ***SFID***. This is the Service Flow identifier.
- ***Throughput Counters Per Service-Flow***. The following Metrics are displayed. These are displayed as a raw number, but they can also be displayed in graphical form by selecting the "Graph" command button.
  - ***DL Bytes***
  - ***UL Bytes***
  - ***DL Pkts***
  - ***UL Pkts***

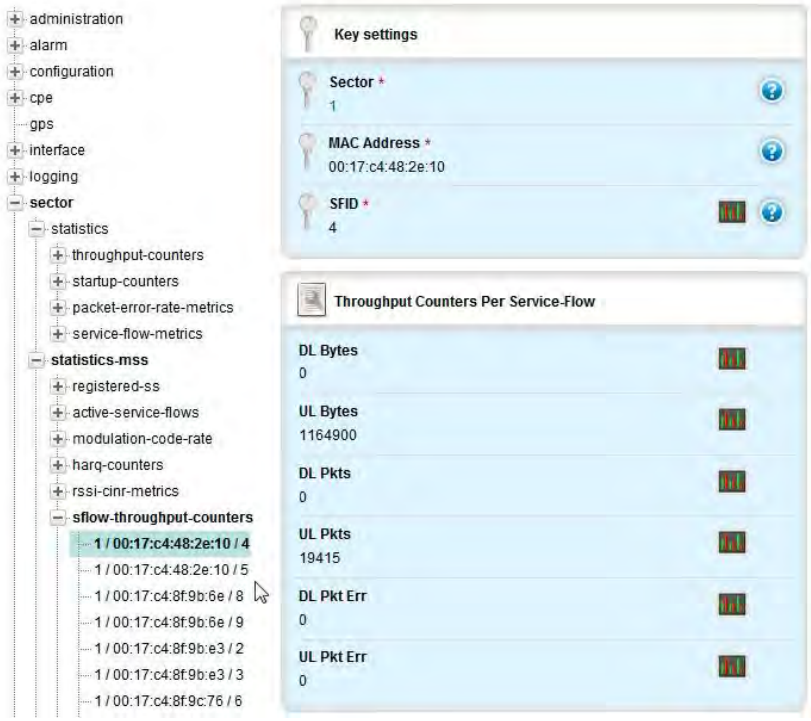


Figure 148 Sector Statistics Service Flow Throughput Counters

At the Main Web GUI Interface Screen select the ***Configuration*** Tab and then the *sector* Main Menu Option, then the ***statistics-mss*** Main Menu Sub-Element and then ***rssi-cinrmetrics.*** The downstream and upstream direction for each Subscriber will be displayed. There are two distinct groups to this window. ***Figure 149*** has the downstream RSSI parameters and ***Figure 150*** has the upstream metrics.

- ***Key Settings***. This indicates the relevant Subscriber. This is not a configurable parameter. The following information is presented:
  - ***Sector.***
  - ***MAC Address.***
  - ***Channel Dir****.* This indicates the respective direction that the Metrics are displayed.
- ***Downstream RSSI/CINR Metrics****.* The following Metrics are displayed. These are displayed as a raw number but they can also be displayed in graphical form by selecting the "Graph" command button. If the CLI is used to view metrics, the RSSI per antenna will be shown but will have the same value across all antennas.
  - ***CINR Mean***
  - ***CINR Std Dev***
  - ***RSSI Mean***
  - ***RSSI Std Dev***
- ***Upstream RSSI/CINR Metrics****. .* The following Metrics are displayed. These are displayed as a raw number but they can also be displayed in graphical form by selecting the "Graph" command button.
  - ***Mean CINR***
  - ***Std Dev CINR***
  - ***Maximum RSSI***

- ***Std Dev RSSI***
- ***Antenna 1 RSSI***
- ***Antenna 2 RSSI***
- ***Antenna 3 RSSI***
- ***Antenna 4 RSSI***
- ***Antenna 5 RSSI***

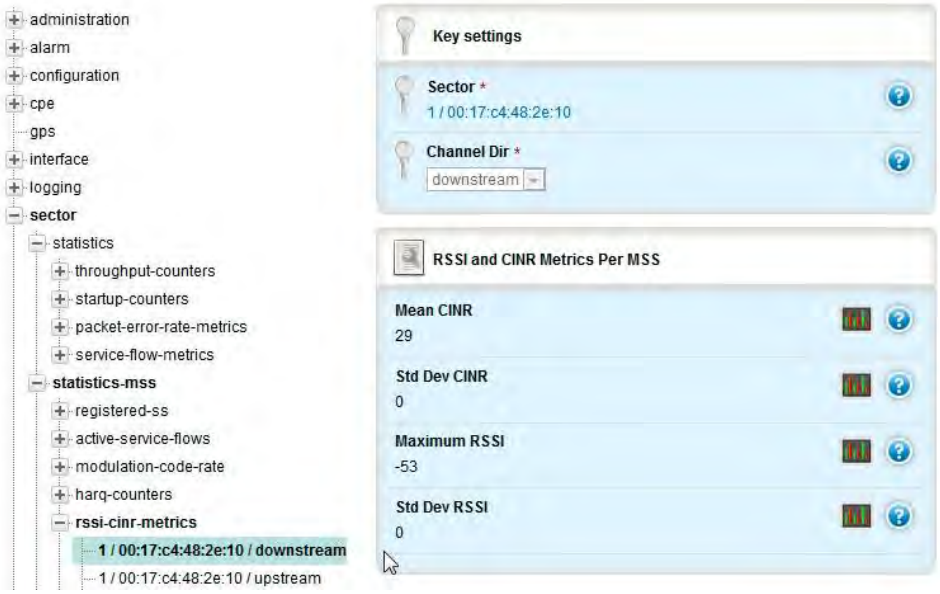


Figure 149 Sector Statistics Downlink RSSI CINR Metrics

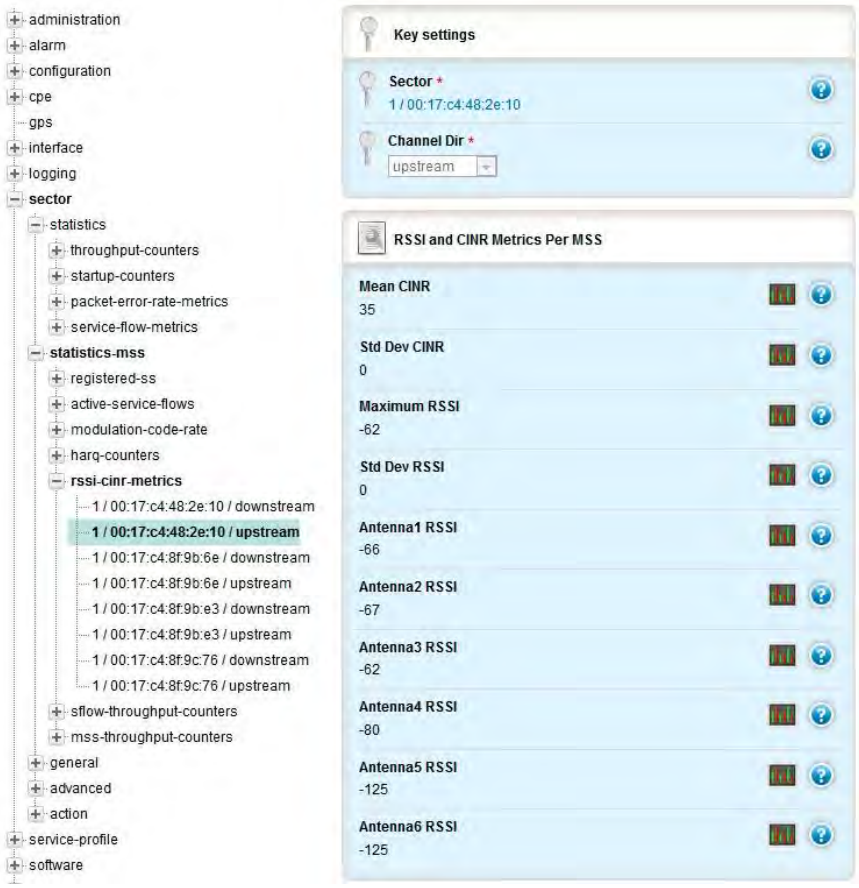


Figure 150 Sector Statistics Upstream RSSI CINR Metrics

At the Main Web GUI Interface Screen select the ***Configuration*** Tab and then the ***sector*** Main Menu Option, then the ***statistics-mss*** Main Menu Sub-Element and then ***harqcounters***. There will be three HARQ Service Flow identifiers displayed for each Subscriber. There are two distinct groups to this window (Figure 151).

- ***Key Settings***. This indicates the relevant Subscriber. This is not a configurable parameter. The following information is presented:
  - ***Sector.***
  - ***MAC Address.***
  - ***Svc Flow ID.***
- ***HARQ Counters Per MSS***. The following Metrics are displayed. These are displayed as a raw number, but they can also be displayed in graphical form by selecting the "Graph" command button. It is not possible to view all the metrics in one window and therefore the User must scroll down to view them all.
  - ***HARQ Enabled***. This indicates whether HARQ has been enabled. This is not however a configurable parameter.
  - ***HARQ DL Pkt Ack***
  - ***HARQ DL Pkt Neg Ack***
  - ***HARQ DL Pkt Trans***
  - ***HARQ DL Pkt Retrans***

- ***HARQ DL Pky Discards***
- ***HARQ DL Pkt 1st Neg Ack***
- ***HARQ UL Pkt Ack***
- ***HARQ UL Pkt Neg Ack***
- ***HARQ UL Pkt Trans***
- ***HARQ UL Pkt Retrans***
- ***HARQ UL Pky Discards***
- ***HARQ UL Pkt 1st Neg Ack***

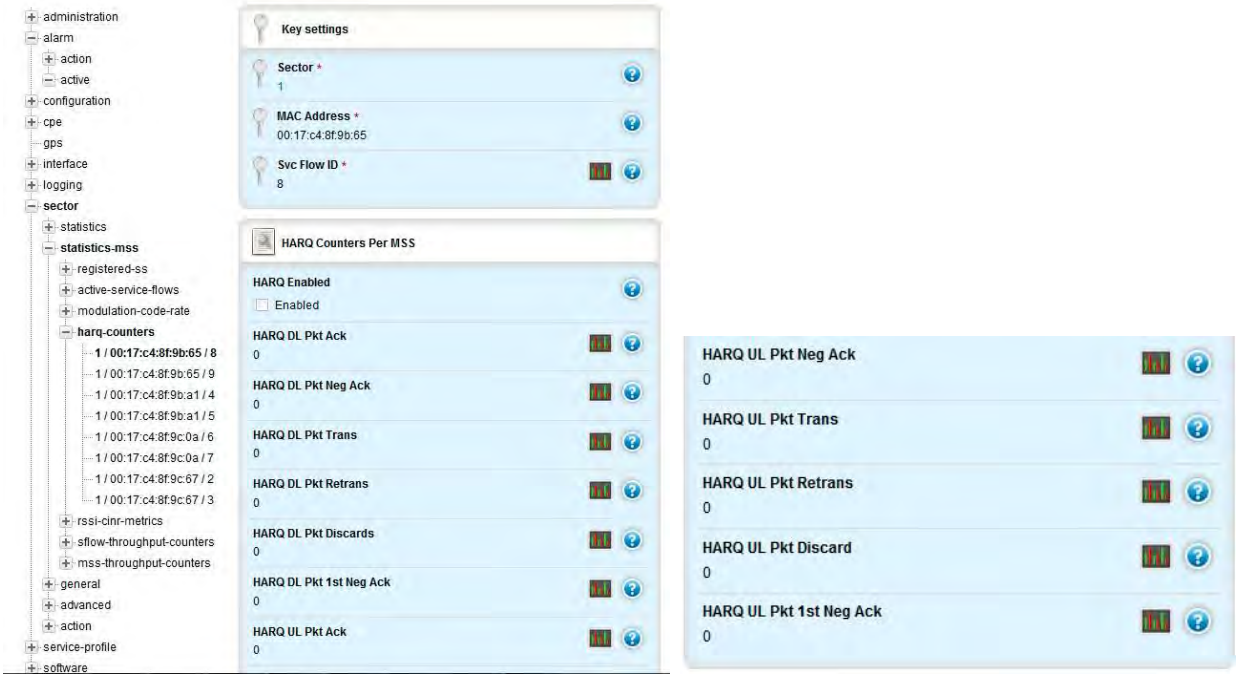


Figure 151 Sector Statistics HARQ Counters

At the Main Web GUI Interface Screen select the ***Configuration*** Tab and then the ***sector*** Main Menu option, then the ***statistics-mss*** Main Menu Sub-Element and then ***modulation-code-rate***. The information for each Subscriber is displayed. There are two distinct groups to this window (Figure 152).

- ***Key Settings***. This indicates the relevant Subscriber. This is not a configurable parameter. The following information is presented:
  - ***Sector***
  - ***MAC Address***
- ***Modulation and Coding Scheme (MCS)***. The following information is displayed.
  - ***DL MCS***. This indicates the current downlink MCS rate. The available options are:
    - QPSK 1/2
    - QPSK 3/4
    - QAM16 1/2
    - QAM16 3/4
    - QAM64 1/2
    - QAM64 2/3
    - QAM64 3/4

- QAM64 5/6
- o ***UL MCS.*** This indicates the current uplink MCS rate. The available options are the same as the downlink.
- o ***DL HARQ STATE.*** Indication if any of the downlink services flows have HARQ Enabled.
- o ***DL MCS HARQ.*** The current MCS Rate used for the downlink services flows that have HARQ.
- o ***UL HARQ STATE.*** Indication if any of the uplink services flows have HARQ Enabled.
- o ***UL MCS HARQ.*** The current MCS Rate used for the uplink services flows that have HARQ.

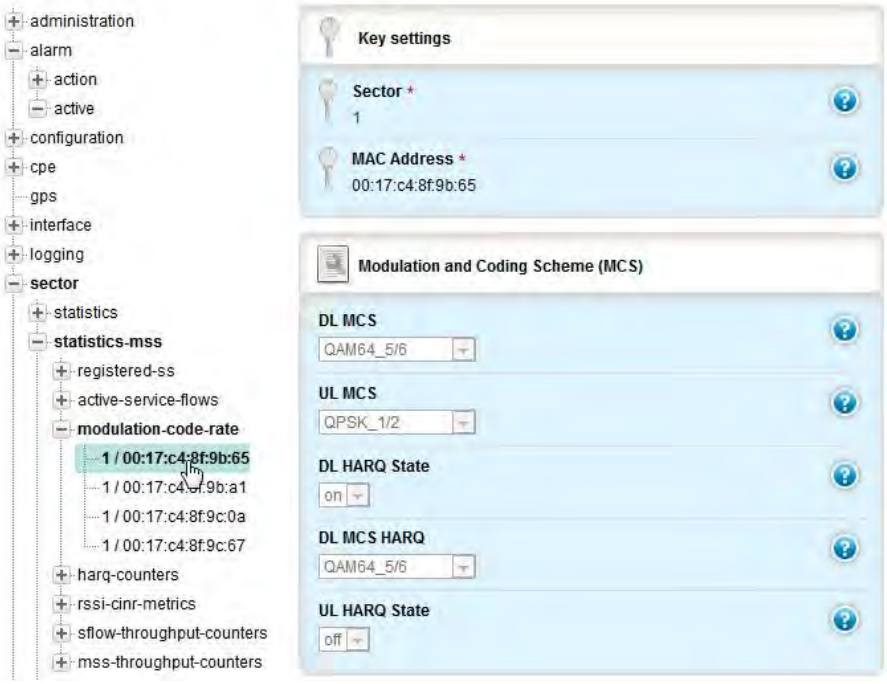


Figure 152 Sector Statistics Modulation Code Counters

At the Main Web GUI Interface Screen select the ***Configuration*** Tab and then the ***sector*** Main Menu Option, then the ***statistics-mss*** Main Menu Sub-Element and then ***activeservice-flows***. The Service Flows that are active for each Subscriber will be displayed. For each Subscriber there will be at least two active Service Flows, one for Upstream and another for Downstream. There are two distinct groups to this window (Figure 153).

- ***Key Settings***. This indicates the relevant Subscriber. This is not a configurable parameter. The following information is presented:
  - o ***Sector***
  - o ***MAC Address***
  - o ***Svc Flow ID.*** This is the Service Flow identifier.
- ***Active Service Flows.*** The following Metrics are displayed. These are displayed as a raw number, but they can also be displayed in graphical form by selecting the "Graph" command button.
  - o ***Svc Flow Dir.*** This provides an indication of the respective direction. The options are uplink or downlink.

- ***UL Bytes.*** This provides an indication of the Service Flow QoS (Quality of Service).
- ***Svc Flow CID***
- ***Svc Flow SAID***

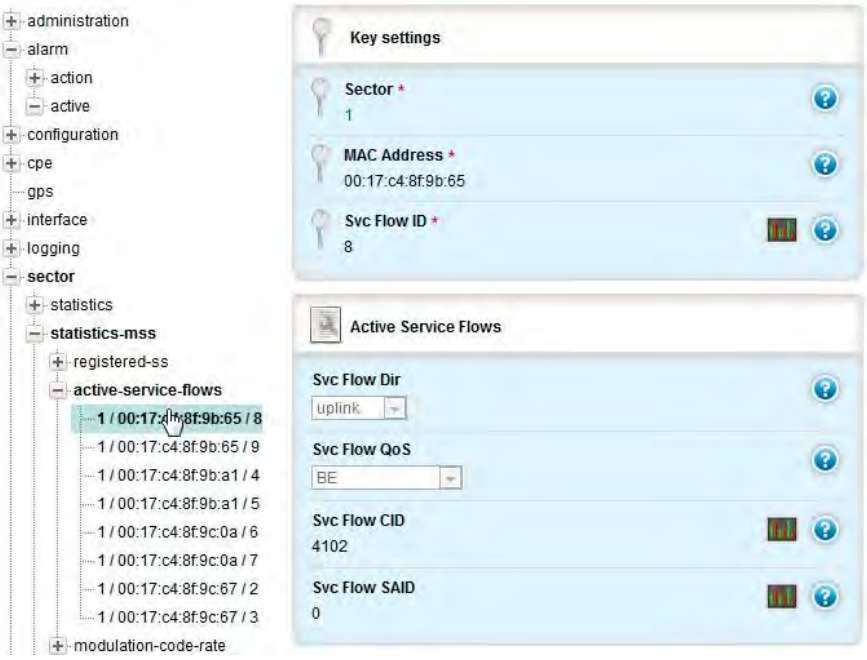


Figure 153 Sector Statistics Active Service Flows

At the Main Web GUI Interface Screen select the ***Configuration*** Tab and then the ***sector*** Main Menu Option, then the ***statistics-mss*** Main Menu Sub-Element and then ***registered-ss.*** The number of registered Subscribers will be displayed. There are two distinct groups to this window (Figure 154).

- ***Key Settings***. This indicates the relevant Subscriber. This is not a configurable parameter. The following information is presented:
  - ***Sector***
  - ***MAC Address.*** Subscriber Unit WIMAX MAC addresses.
- ***Registered Subscriber Station.*** The following information is displayed. These are not configurable parameters at this menu option.
  - ***Client Profile ID.***
  - ***Provisioning Status.*** One of the states below
    - **INIT**. Initializing – During Network Entry
    - **ACTIVE** – Service Flows are Provisioned and active
    - **DENY** – Provisioning Denied. Usually by the AAA server.
    - **TIMEOUT** – AAA Server timeout out.
    - **LOCAL TIMEOUT** – Local provisioning Timeout.
  - ***Provisioning Method.*** One of the methods below
    - **UKNOWN** – Usually during network entry.
    - **STANDALONE** – Uses local Base Station provisioning Database.
    - **STANDALONE DEF** – Uses Local Default Provisioning.
    - **AAA PROV** – Provisioned using AAA Server.
    - **ASN-GW PROV** – Provisioned using ASN Gateway.

- ***Network Entry State.*** This provides an indication as to the connected "state" of the Subscriber.
- ***Uptime***. This is the Subscriber connected time.
- ***Network Entry Type.*** This indicated the way the CPE connected to the Base station.
- ***Authentication status.*** The authentication mode of the CPE
- ***SNR Reporting Method***. The reporting method used by the CPE to report downlink channel status
- ***Basic CID***. Basic Connection ID
- ***Primary CID***. Primary Connection ID
- ***Vendor ID***. The part of the MAC Address used to determine the CPE vendor (OUI)
- ***MAC Version***. The WIMAX MAC version number

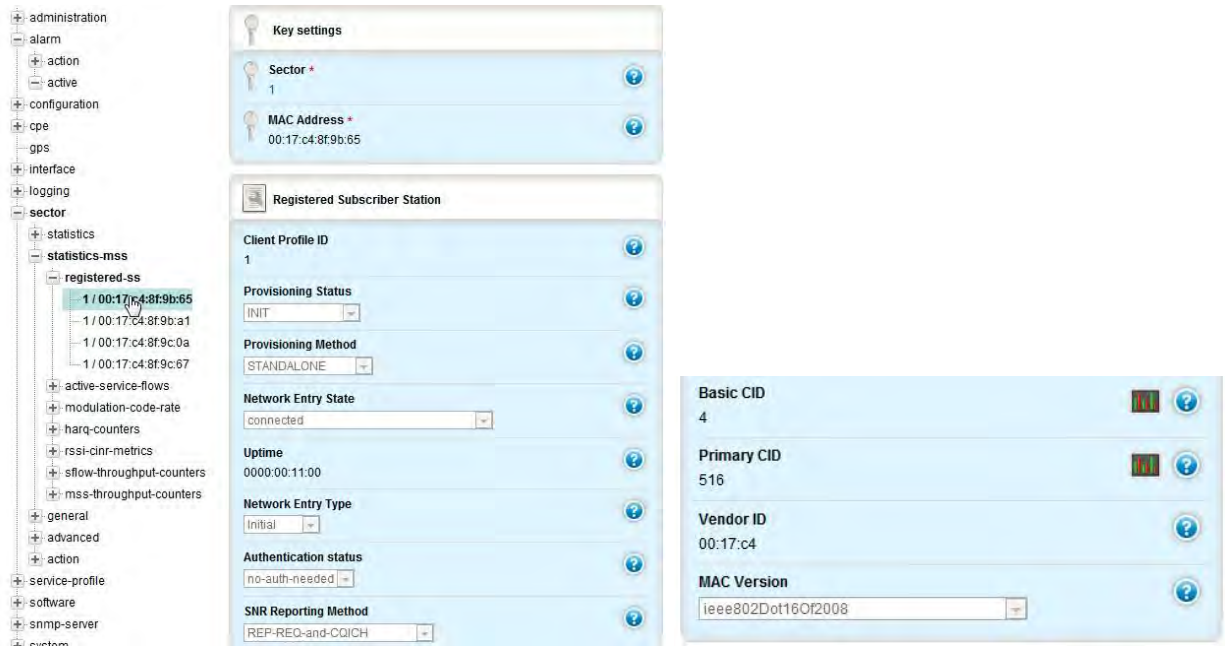


Figure 154 Sector Statistics Registered SS

3.6.3.3. Logging

The Base Station contains several internal system management logs. The Web GUI provides the User with complete flexibility on performing several key actions on these logs.

At the Main Web GUI Interface Screen select the ***Configuration*** Tab and then select the ***logging*** Main Menu Option. This will display all the system logs files (**Figure 155).**

Figure 155 Main Menu Logging Options

The logging Main Menu option contains four Main Menu Sub-Elements. These are:

- ***remote***. The User has the capability to define a remote server to forward a predefined log level.
- ***local***. The User has the capability to define the minimum severity level to log.
- ***file***. These are file actions that the User can perform.
- ***files***. This describes the system log files.

At the Main Web GUI Interface Screen select the ***Configuration*** Tab and then select the ***logging*** Main Menu Option and then the ***remote*** Main Menu Sub-Element. The User is now presented with a window that displays the remote Log Server Settings. There are two distinct groups to this window (Figure 156). The User is presented with a host Menu Sub-Element from the remote Main Menu Sub-Element level. If

the User navigates to this level, then it will display a list of all the log servers that have been configured. The User can select to view the relevant details.

- ***Default Remote Log Server Settings***. The User can view and hence configure the default minimum severity log level to forward to the remote server. This will apply to all remote servers which have a level of default. The User must be in Edit Mode to configure. In addition to the default level there are nine available options. These are:
  - ***none***
  - ***debug***
  - ***info***
  - ***notice***
  - ***warning***
  - ***error***
  - ***critical***
  - ***alert***
  - ***emergency***
- ***Remote Log Server Settings***. For log servers that have configured the following information is displayed. To configure the User must be in Edit Mode. Once in Edit Mode, the User can <***Add host***>, delete or change the Severity Level of an existing host.
  - *Hostname.* If the User wants to add a remote server then they must enter the syslog remote server IP address or domain name. The User cannot edit the hostname for a syslog server that has been configured, this syslog must be deleted and then it can be re-added. When in the Edit Mode, there is a red box beside each hostname. If the User navigates to the red icon, then this will present the User with the ability to delete the hostname.
  - *Security Level.* The User can configure or re-configure the syslog server to that of the default level or any of the nine available options.

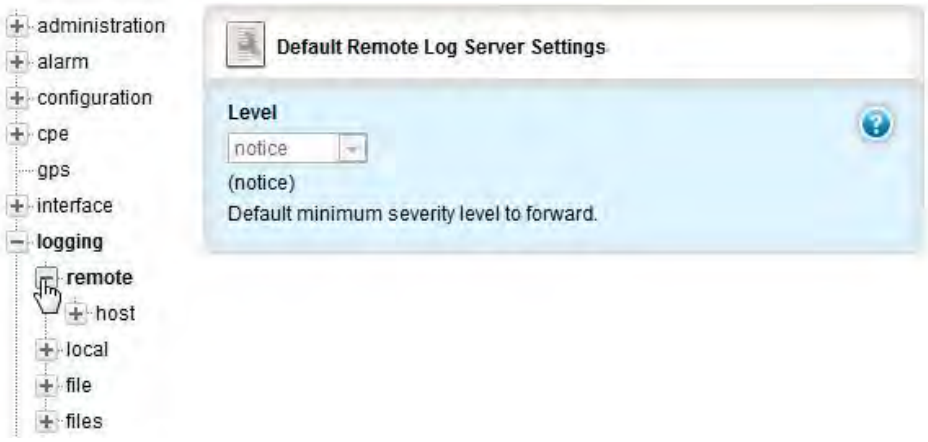


Figure 156 Logging Remote Host Information

At the Main Web GUI Interface Screen select the ***Configuration*** Tab and then select the ***logging*** Main Menu Option and then the ***local*** Main Menu Sub-Element. The User is now presented with a window that displays the local Log Server Settings. This only one distinct group to this window (Figure 157). The User can select to view the relevant details.

- ***Default Local Log Server Settings***. The User can view and hence configure the default minimum severity log level for the local internal log server. This will apply to all local servers except those which have been configured in the logging local override configuration. The User must be in Edit Mode to configure. To define the default level there are one of nine available options to select. These are:
  - ***none***
  - ***debug***
  - ***info***
  - ***notice***
  - ***warning***
  - ***error***
  - ***critical***
  - ***alert***
  - ***emergency***

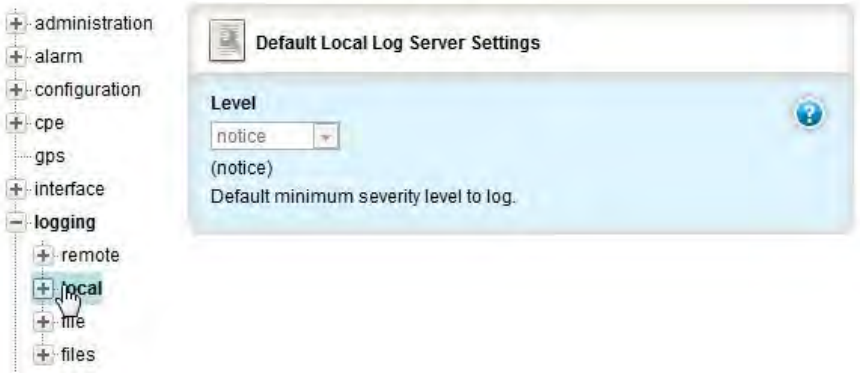


Figure 157 Logging Local Information

At the Main Web GUI Interface Screen select the ***Configuration*** Tab, then select the ***logging*** Main Menu option, then the ***local*** Main Menu Sub-Element and then ***override***. The User can now is now presented with an option to increase or decrease the internal sys log per daemon/application which are internal to the Base Station (Figure 158). The User must be in Edit mode to configure.

Figure 158 Logging Local Override

When in Edit mode only one distinct group to this window is displayed. The User must <***Add Source***> and define the relevant App Name. The configurable options are:

- ***Key Settings***
- ***App Name***
  - ***confd***
  - ***wmdlpcClientd***
  - ***r6mgrd***
  - ***sectord***
  - ***statsd***
  - ***genactiond***
  - ***snmpactiond***
  - ***gpsmgrsyncd***
  - ***swumgrd***
  - ***sysmgrd***

Once the ***App Name*** has been selected then the User is presented with an Application Log Settings menu where the *Severity Level* can be configured.

At the Main Web GUI Interface Screen select the ***Configuration*** Tab and then the ***logging*** Main Menu option and then the ***file*** Main Menu Sub-Element. The User is now presented with further Menu Sub-Elements (Figure 159). The User now has top select one of the Menu Sub-Elements to be presented with an action.

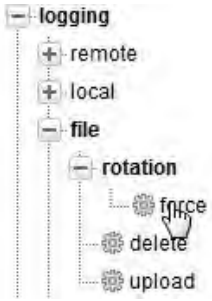


Figure 159 Logging File Information

At the Main Web GUI Interface Screen select the ***Configuration*** Tab, select the ***logging*** Main Menu Option, then the ***file*** Main Menu Sub-Element, then ***rotation*** and finally ***force***.

This will force a reboot of the Base Station and the log file to effectively rotate and begin logging again. The rotate feature forces the logging to the relevant file to stop, it then compresses the file, effectively renames it (generally by appending a .1 to the end of the filename) and then starts the logging to a new file. E.g. the current sys log file is messages but at the last rotate action this file was rotated into messages.1.gz and the then logging started again to messages. An automatic rotation will occur when the file size reaches 5MBytes. There are no parameters to edit and the User simply has to select the ***Perform*** Command Menu Option to initiate the log file rotation (Figure 160).

Figure 160 Logging File Rotation

At the Main Web GUI Interface Screen select the ***Configuration*** Tab, then the ***logging*** Main Menu Option, then the ***file*** Main Menu Sub-Element and then ***delete***. This option provides a means for the User to delete a log file (Figure 161). Two distinct window groups are presented to the User. These are:

- ***Delete Log File***. This simply provides a description of the actions.
- ***Delete Log File***. The User simply selects the log file that they would like to delete. The list of available files is presented via a drop-down menu. The User does not have to be in Edit mode to select the log file.

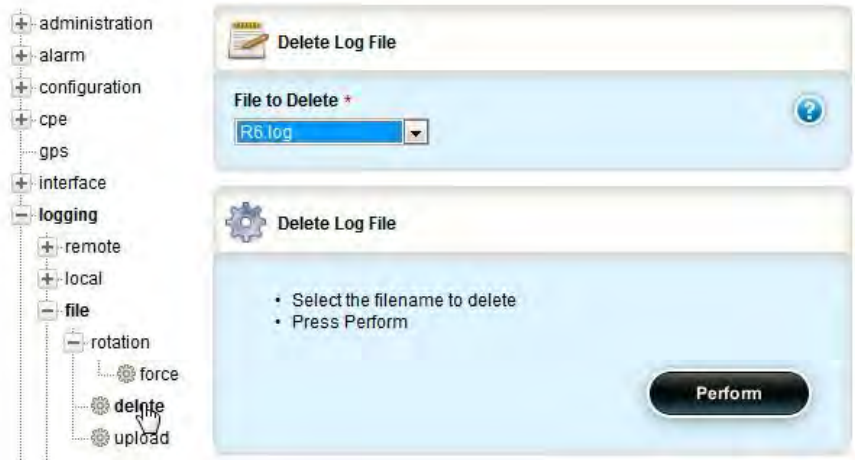


Figure 161 Logging File Delete

At the Main Web GUI Interface Screen select the ***Configuration*** Tab, then select the ***logging*** Main Menu Option, then the ***file*** Main Menu Sub-Element and then ***upload***. This option provides a means for the User to upload a log file to a server URL. Two distinct window groups are presented to the User. These are (Figure 162):

- ***Upload Log File to Remote Server***. This simply provides a description of the actions.
- ***Upload Log File***. The User does not have to be in Edit mode to perform these actions. Prior to uploading the file, the User must ensure that an FTP Server has been configured and is running. The User has to select the following information:
  - ***File to Upload***. The User selects the log file that they would like to upload. The list of available files is presented via a drop down menu.
  - ***Destination URL***. There are a variety of formats for the destination URL. These can be displayed if the User selects the "help" key. These URL formats are defined as:
  - ftp://[user[:password]@]hostname[:port]/filepath
  - http://hostname[:port]/filepath
  - https://hostname[:port]/filepath

Where [ ] indicates optional items. Thus, user:password@ is optional, and the :password part can be omitted

- [:port] is also optional
  Examples using ftp (you can substitute http or https):
- ftp://myhost.com/filename
- ftp://myhost.com/directory/filename
- ftp://myhost.com:2323/directory/filename
- ftp://myname@myhost.com:2323/directoryname/filename
  ftp://myname:password@myhost.com:2323/directoryname/filename

URL of remote source file; format is as follows:

- protocol://[user[:password]]@host[:port]/path
- protocol can be ftp, http, or https

Figure 162 Logging File Upload

At the Main Web GUI Interface Screen select the ***Configuration*** Tab, then select the ***logging*** Main Menu option, and then the ***files*** main Menu Sub-Element. This option provides a list of all the sys log files on the Base Station (Figure 163).

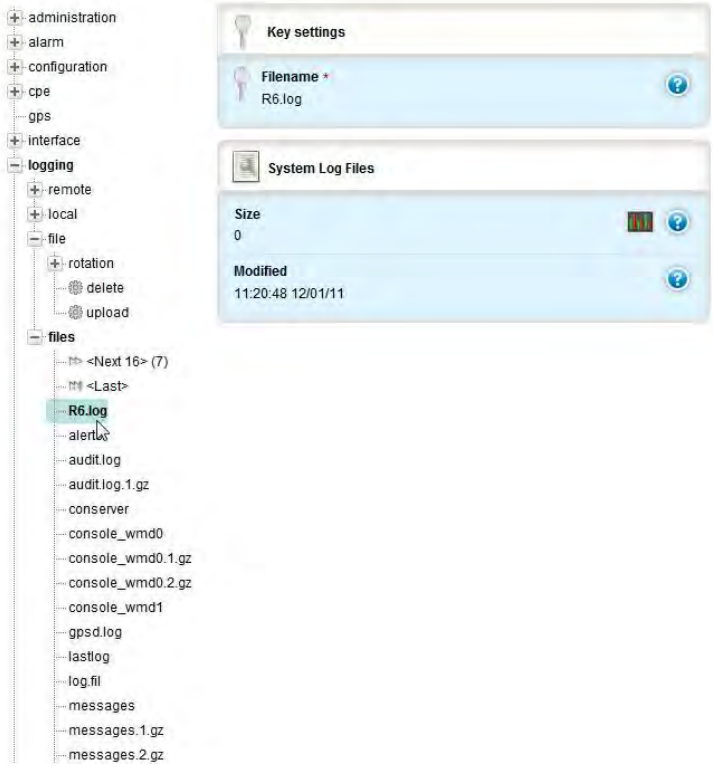


Figure 163 Logging File Filenames

If the User selects a relevant file, then the characteristics of the file are displayed. The following information will be displayed for each file:

- ***Key Settings***
  - ***Filename***
  - ***System Log Files***
  - ***Size***. This is the file size in bytes.
  - ***Modified***. This was the date that the file was last modified.

3.6.3.4 SNMP Server

Simple Network Management Protocol (SNMP) is an "Internet-standard protocol for managing devices on IP networks. The SNMP server exposes management data in the form of variables on the managed systems, which describe the system configuration (MIBs). These variables can then be queried and set by managing applications called Network Management Systems (NMS).

To configure the SNMP Server, select the ***Configuration*** Tab, ***Edit Private*** and then select the ***snmp-server*** *from* Main Menu Option (Figure 164).

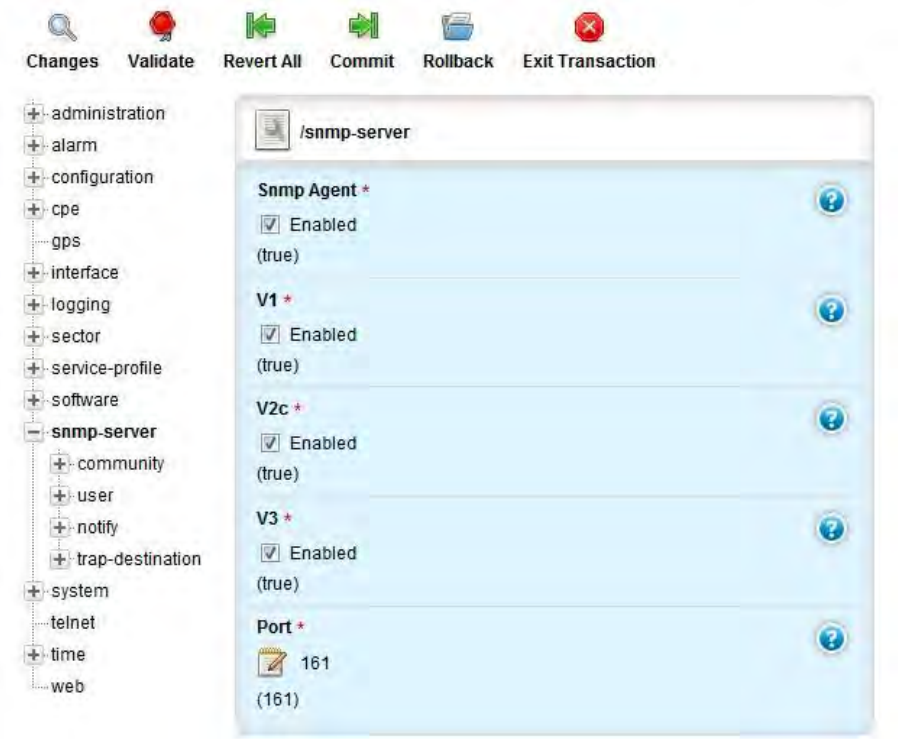


Figure 164 SNMP-Server Configuration

When in Edit mode, the configurable options are:

- ***SNMP Agent (enable/disable)***. Enables SNMP agent software on Base Station for connection to an NMS (Network management System).
- ***SNMP v1 (enable/disable)***. Enables SNMP version 1 (SNMPv1) is the initial implementation of the SNMP protocol and the de-facto network management protocol.

- ***SNMP v2c (enable/disable)***. Enables SNMP version 2 (SNMPv2) which is the implementation of the SNMP protocol and includes performance, security and confidentiality updates.
- ***SNMP v3 (enable/disable)***. Enables SNMP version 3 (SNMPv3) which includes encoded community strings for improved security.
- ***Port (default 161)***. The SNMP agent receives requests by default on UDP port 161.

The ***community*** sub-menu (Figure 165) allows the configuration of the community string (basic password) used for security for with SNMP. If the User wants to add or edit any of the existing community strings, then they must then select ***snmpCommunityTable*** and enter the Edit Mode (Edit Private or Edit Exclusive).

The following options will be available:

- <***Add snmpCommunityEntry***>. This allows addition of a new community string
- ***private***. SNMP access which allows read-write permissions.
- ***public***. SNMP access which allows read-only permissions.
- ***standard trap***. Read-only permissions for sending SNMP traps.

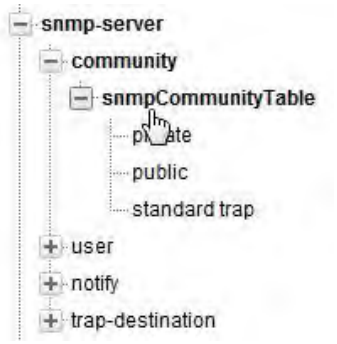


Figure 165 Community Sub-Menu

If the User wants to add or edit any of the existing community strings, then they must then select enter the Edit Mode (Edit Private or Edit Exclusive). The following options will be available for each entry (Figure 166):

- ***Key Settings***
  - ***SNMP Community Index***
- ***snmpCommunityEntry***
  - ***SNMP Community Name***. Name of the community string
  - ***SNMP Community Security Name***. Level of access including read-write and read-only
  - ***SNMP Community Context Engine ID.***
  - ***SNMP Community Context Name.***
  - ***SNMP Community Transport Tag.***
  - ***SNMP Community Storage Type***. Default value is permanent

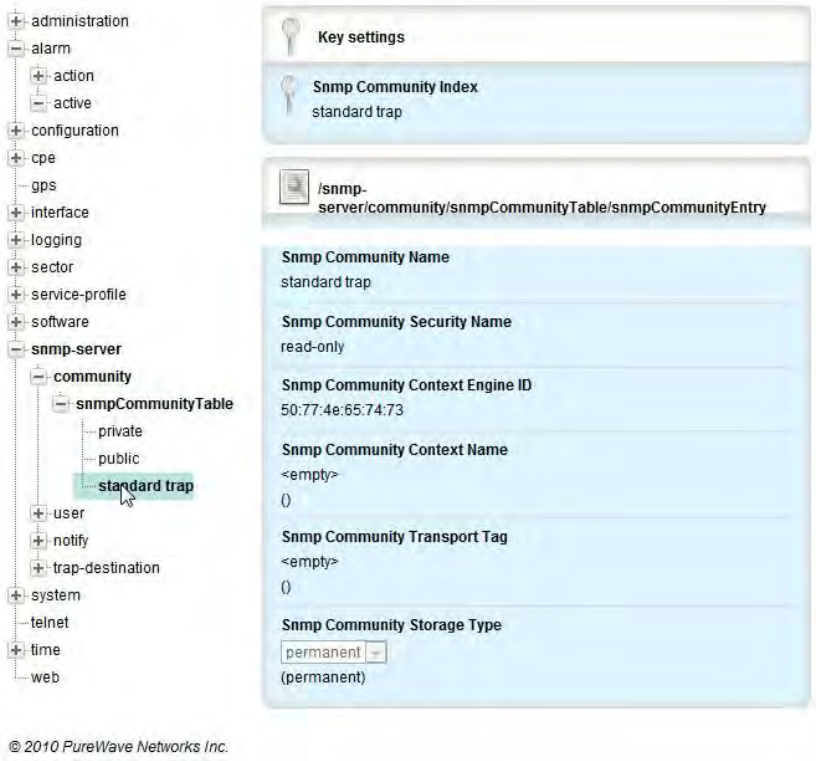


Figure 166 snmpCommunityEntry Table

The ***user*** sub-menu (Figure 167) allows the protection of SNMPv3 packets from the above threats by utilizing a concept of multiple users where each user provides secret keys for authentication and privacy. If the User wants to add or edit any of the existing user record, then they must then select ***user*** and enter the Edit Mode (Edit Private or Edit Exclusive).

The following options will be available:

- ***Key Settings***
  - ***Usm User Engine ID***
  - ***Usm User Name***
- ***usmUserEntry***
  - ***Usm User Security Name***
  - ***Usm User Clone From*.**
  - ***Usm User Auth Protocol*.**
  - ***Usm User Auth Key Change*.**
  - ***Usm User Own Auth Key Change*.**
  - **Usm User Priv Protocol.**
  - **Usm User Priv Key Change.**
  - **Usm User Own Priv Key Change.**
  - **Usm User Public.**
  - **Usm User Storage Type.** Default is nonVolatile
  - **Usm User Auth Key.**

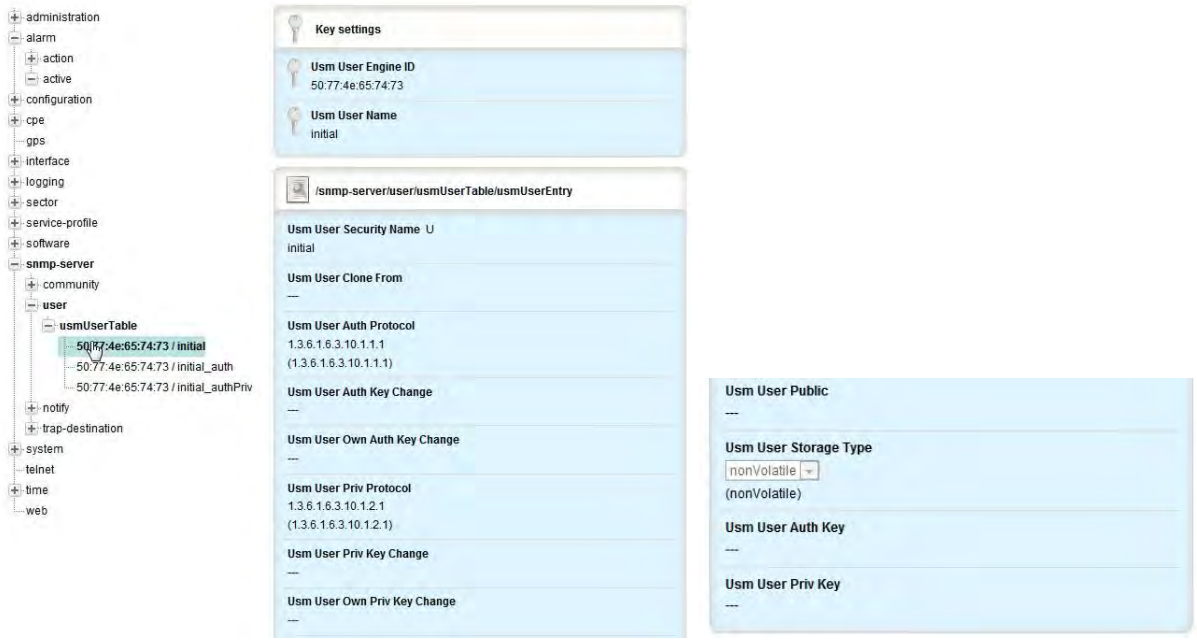


Figure 167 SNMP User Configuration

The ***notify*** sub-menu (Figure 168) configures the SNMP notification generation mechanism. If the User wants to add or edit any of the existing community strings, then they must then select ***snmpNotifyTable*** and enter the Edit Mode (Edit Private or Edit Exclusive).

The following options will be available:

- ***Key Settings***
  - ***SNMP Notify Name***
- ***snmpNotifyEntry*** *(Field entries are explained in Table 12 SNMP Notification Table)*
  - ***SNMP Notify Tag.***
  - ***SNMP Notify Type.***
  - ***SNMP Notify Storage Type.***

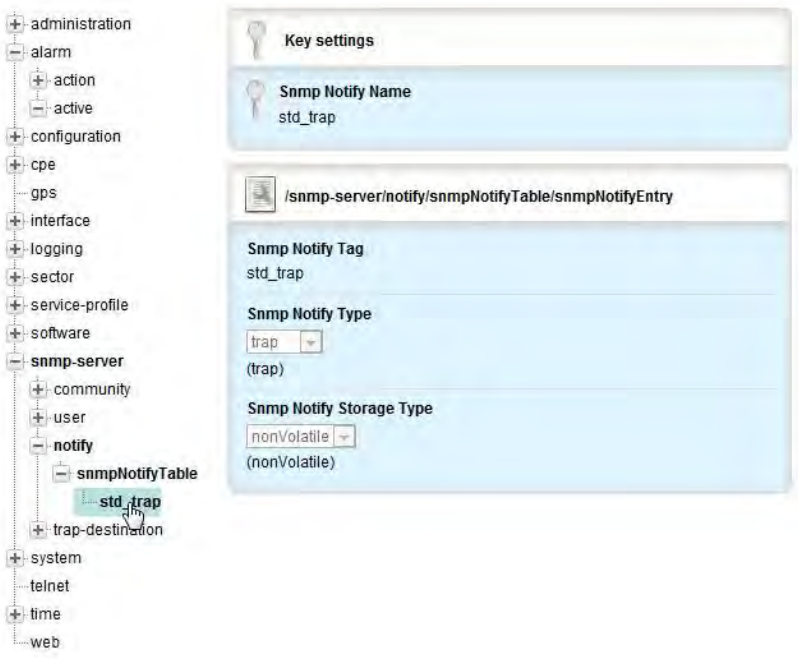


Figure 168 SNMP Notify Configuration

Name	Description	Field Example
SNMP Notify Name	A unique identifier used to index this table.	1-32 chars
SNMP Notify Tag	A tag value used to reference one or more entries in snmpTargetAddrTable.	Example: “std_trap”
SNMP Notify Type	Selects the type of notification to be generated for the entries in the snmpTargetAddrTable referenced by snmpNotifyTag: trap(1) - Generates an SNMPv2c Trap PDU inform(2) - Generates an InformRequest PDU	Example: trap
SNMP Notify Storage Type	String name assigned to the Base Station.	The default value is nonVolatile.

Table 12 SNMP Notification Table

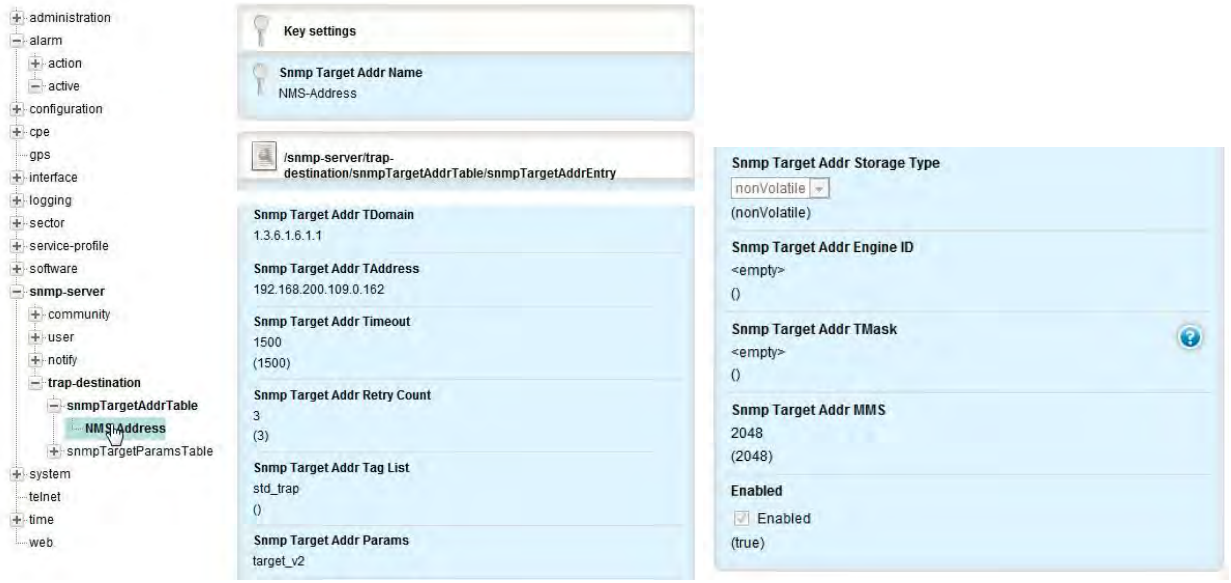


Figure 169 SNMP Trap Destination

The ***trap destination*** sub-menu (Figure 169) specifies the network and transport layer attributes of notification destinations. Each row in this table is used to send traps to a different NMS.

If the User wants to add or edit any of the existing trap destinations, then they must then select ***NMSAddress*** and enter the Edit Mode (Edit Private or Edit Exclusive). The following options will be available below:

- ***Key Settings***
  - ***NMS-Address***
- ***snmpNotifyEntry*** *(Field entries are explained in* Table 13 Table 12 SNMP Notification Table*)*
  - ***Snmp Target Addr TDomain.***
  - ***Snmp Target Addr TAddress.***
  - ***Snmp Target Addr Timeout.***
  - ***Snmp Target Addr TAddress.***
  - ***Snmp Target Addr Retry Count.***
  - ***Snmp Target Addr Tag List.***
  - ***Snmp Target Addr Params.***
  - ***Snmp Target Addr Storage Type.***
  - ***Snmp Target Addr Engine ID.***
  - ***Snmp Target Addr TMask.***
  - ***Enabled.***

Name	Description	Field Example
SNMPTargetAddName	Name of the target snmpTargetAddrTable.	1-32 chars
SNMPTargetAddrTDomain	This object indicates the transport type of the address contained in the snmpTargetAddrTAddress object.	“1.3.6.1.6.1.1” is the domain for UDP
SNMPTargetAddrTAddress	Specifies the target address, which consists of an IP address followed by a UDP port number.	Example: 127.0.0.1.0.162
SNMPTargetAddrTTimeout	Sets a timeout value (in ticks) for the transmission of InformRequest PDU or TCP connection. The agent will wait this amount of time for a response to an InformRequest PDU or TCP connection before attempting again.	Example: 1500 is 1.5 seconds
Name	**Description**	**Field Example**
SNMPTargetAddrRetryCou nt	Sets the number of times that the agent will resend an InformRequest PDU or attempt to establish a TCP connection before abandoning further attempts and logging an error in the agent log file.	Example: 3
SNMPTargetAddrTagList	A list that provides the correlation between snmpTargetAddrTable and snmpNotifyTable. When generating a notification, the agent searches this list for the value contained in snmpNotifyTag. If the list contains this value, then the agent uses the information in this row to create a destination for the notification.	For example: “std_trap”
SNMPTargetAddrParams	Indexes the row in snmpTargetParamsTable that describes the security parameters to be used when sending the notification. If the row specified does not exist, the notification will not be sent.	For example: “target_v2”
SNMPTargetAddrStorageT ype	Specifies how the row should be stored.	The default value is nonVolatile.
SNMPTargetAddrEngineID	Internal use only, leave blank.	“”

SNMPTargetAddrTMask	Internal use only, leave blank.	""
SNMPTargetAddrStorageT ype	Internal use only (Maximum message size) default 2048.	2048
Enabled	This field allows trap sending to a given NMS to be paused.	true/false

Table 13 SNMP Target Address Table

3.6.3.5 Alarm Management

The Quantum Base Station has advanced alarm and fault management capabilities. When a fault or event occurs, an alarm condition will be raised. An alarm is a persistent indication of a fault that clears only when the triggering condition has been resolved.

To configure Alarm Management, select the ***Configuration*** Tab and then select the ***alarm*** Main Menu Option (Figure 170).

When in View or Edit mode, the options are:

- ***action****. Allows acknowledgement, clearing and un-acknowledgment of alarms*
- ***active****. View a list of the active alarms*

Figure 170 Alarm Management

To acknowledge, clear or un-acknowledge an alarm, select the ***action*** sub-Element (Figure 171). The User is now presented with a window that displays an operation to be performed on the following alarm-names.

- ***Voltage****. Allows acknowledgement, clearing and un-acknowledgment of alarms*
- ***Sector-Comm-Loss****. Indicates if Sector is Up or Down.*
- ***Temperature****. Low, Hi or Normal Operating Temperature*
- ***Sector-Down****. View the active alarms*
- ***GPS-Synch-Holdoff****. Indicates if GPS is reliable or unreliable.*
- ***GPS-Synch-Loss****. Indicates if GPS is reliable or unreliable.*

Select the alarm type and click Perform to apply the action

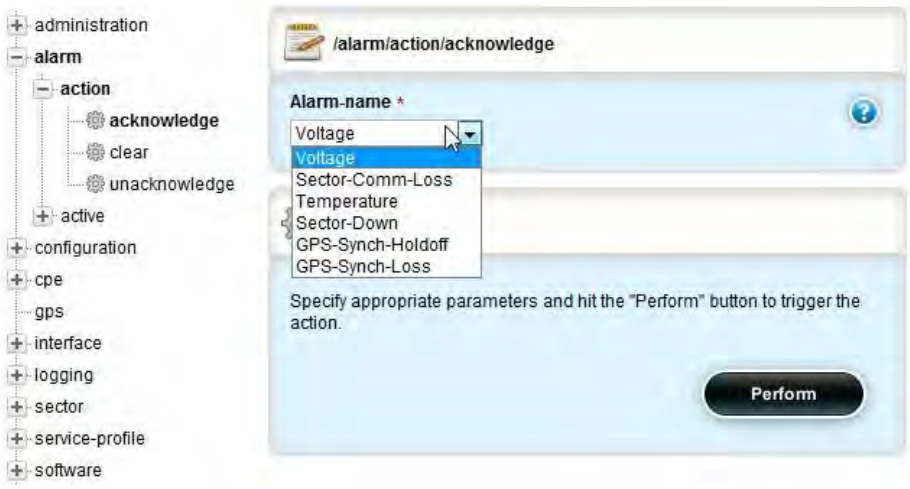


Figure 171 Alarm Action

4 Citizens Broadband Radio Service Operations (47 C.F.R. Part 96)

All information provided herein including, but not limited to, feature content, releases, functionality, estimated dates, and timelines, has been prepared by Mercury Networks, LLC. for general information and documentation purposes only and is subject to change at any time. Including, without limitation, because of specific field conditions. Mercury Networks, LLC. is under no obligation and is making no commitments with regards to any of the information contained in the following section (4. Citizens Broadband Radio Service Operations). Mercury Networks, LLC. has made all reasonable effort to ensure that the information contained in the following section is adequate and free of material errors. Subject to applicable law, in no event will Mercury Networks, LLC. be liable for errors in this documentation, or for any damages including but not limited to direct, in-direct, incidental, or consequential, or any losses that may arise from use of this documentation or the information in it.

For operations under FCC Part 96, Citizens Broadband Radio Service, the Quantum 6636 can me modified for use with the additional spectrum available in the CBRS band (3550-3700) through the combination of a firmware upgrade and use of a proprietary Domain Proxy application. For access to the necessary firmware and domain proxy applications, operators must contact Mercury Networks for assistance. The following sections outline Quantum 6636 operations under Part 96, the necessary configuration, and use of the domain proxy application.

4.1 Citizens Broadband Radio Service (CBRS) Overview

Citizens Broadband Radio Service (**CBRS**) is a 150 MHz wide broadcast band of the 3.5 GHz band (3550 MHz to 3700 MHz) in the United States. In 2017, the US Federal Communications Commission (FCC) completed a process which began in 2012 to establish rules for commercial use of this band, while reserving parts of the band for the US Federal Government to limit interference with US Navy radar systems and aircraft communications (otherwise known as 47 CFR Part 96).

On January 27, 2020, the FCC authorized full use of the CBRS band for wireless service provider commercialization without the restrictions to prevent interference with military use of the spectrum. Under the new rules, wireless carriers using CBRS might be able to deploy 5G mobile networks without having to acquire spectrum licenses.

Existing 3.65 GHz licenses possessed by various operators will begin their transition from Part 90 to Part 96 in October of 2020. Unless the license being used is covered by a Part 90(z) Grandfathered Protection Zone registration, which may extend the use of the license temporarily beyond the anticipated October 2020 transition date, will be required to transition to CBRS for continued use of the Quantum 6636 product inside the US (see 47 CFR Subpart Z – Wireless Broadband Services in the 3650-3700 MHz band for up-to-date information regarding the latest federal regulations).

4.1.2 CBRS Operations

The Citizens Broadband Radio Service is governed by a three-tiered spectrum authorization framework to accommodate a variety of commercial uses on a shared basis with incumbent federal and non-federal users of the band in the US. Access and operations will be managed by a dynamic spectrum access system, conceptually similar to the databases used to manage Television White Spaces devices. The three tiers are: *Incumbent Access*, *Priority Access*, and *General Authorized Access*.

- ***Incumbent Access*** users include authorized federal and grandfathered fixed satellite service users currently operating in the 3.5 GHz Band. Under the rules promulgated by the FCC, these users, particularly including US Navy radar operators, will be protected from harmful interference from Priority Access and General Authorized Access users. Existing 3650–3700 MHz band operations "are grandfathered for up to 5 years", with the FCC's Wireless Telecommunications Bureau and Office of Engineering and Technology charged with soliciting public comment on "the appropriate methodology for defining the grandfathered wireless protection zone contours".
- The ***Priority Access*** tier consists of Priority Access Licenses (PALs) that will be assigned using competitive bidding within the 3550-3650 MHz portion of the band. Each PAL is defined as a non-renewable authorization to use a 10-megahertz channel in a single census tract for three-years. Up to seven total PALs may be assigned in any given census tract with up to four PALs going to any single applicant. Applicants may acquire up to two-consecutive PAL terms in any given license area during the first auction.
- The ***General Authorized Access*** tier is licensed-by-rule to permit open, flexible access to the band for the widest possible group of potential users. General Authorized Access users are permitted to use any portion of the 3550-3700 MHz band not assigned to a higher tier user and may also operate opportunistically on unused Priority Access channels.

A Spectrum Access System (SAS) is used as an automated frequency coordinator that can manage spectrum sharing on a dynamic, as-needed bases across the three tiers of access. The Quantum 6636 can engage communications with and accept commands from a SAS utilizing the Mercury Networks Domain Proxy. A Domain Proxy (DP) is an entity engaging in communications with the SAS on behalf of multiple individual CBSDs or networks of CBSDs. The Domain Proxy can also provide a translational capability to interface legacy radio equipment in the 3650-3700 MHz band with a SAS to ensure compliance with Part 96 rules.

More information regarding FCC and Winnforum standards can be found here: https://cbrs.wirelessinnovation.org/. ***We highly encourage any operator who wishes to utilize the Quantum 6636 for deployment in a CBRS environment carefully review the standards available on the WinnForum site as they may change periodically.***

4.1.3 Requirements for the Quantum 6636 to Operate in CBRS

Whether you plan to operate with an Incumbent Access license, a Priority Access license, or a General Authorized Access license, the Quantum6636 can utilize the full 150 MHz available in CBRS (3550-3700 MHz), provided a few preparations have been made first:

1. The Quantum 6636 Base Station will need the latest CBRS compatible software build. You can learn more about upgrading the Base Station software in **section 3.6** of this guide.
    a. The software will be issued by an authorized Mercury Networks support technician. To learn more about this process contact support@mercurynets.com.
2. Basic Base Station parameters will need to be configured prior to connecting the Quantum 6636 with the Mercury Networks Domain Proxy. This is covered in detail in **section 4.2.**
3. The Quantum 6636 Base Station will require the Mercury Networks Domain Proxy for use with an authorized SAS provider. To learn more about the Mercury Networks Domain Proxy, see **section 4.3** of this guide.

4. All Quantum 6636 installations will need to be signed by a Certified Professional Installer (CPI) with a valid certificate loaded into the Mercury Networks Domain Proxy. To learn more about the Mercury Networks Domain Proxy, see **section 4.3** of this guide.

4.2 Base Station Configuration for use with CBRS and the Mercury Networks Domain Proxy

The following section will outline the basic configuration parameters that need to be established with the Quantum 6636 product prior to use with the Mercury Networks Domain Proxy. There are two methods for managing/configuring a Base Station:

1. Command Line Interface (CLI)
2. Graphical User Interface (GUI) Web Interface

All configuration parameters are available through CLI. ***The CLI is recommended for configuring a Base Station for use in the CBRS band and with the Mercury Networks Domain Proxy.*** The CLI is accessible via the Base Station Console Interface using an appropriate terminal emulator, or via a Base Station ETH-1 port using either SSH or Telnet ***(Telnet is disabled by default).*** Refer to **section 3 – Quick Start Guide** for additional information regarding initial configuration, and a full list of configurable parameters.

The following commands assume you have read through **section 3** and are prepared to use the CLI for issuing configuration commands to the Base Station. Items you will need to know prior to configuration are:

- System IP address
- Sector IP address
- Management VLAN
- Antenna gain
- Antenna beadwidth
- Antenna downtilt
- Cable loss
- Host Name
- BSID
- Time Zone
- NTP Server

Enter configuration mode and issue the following commands via CLI to configure the Quantum 6636:

1. ***configure***
2. Connect to the Base Station via ETH-1.
    a. Default Base Station Management IP address (Host Name): 192.168.1.10
    b. Default credentials are:
        admin
        admin123
3. Gather the needed files for the software upgrade (contact support@mercurynets.com)
4. Perform the necessary software upgrade to both banks A and B
5. Run commands

   a. ***system interface ip address <new device ip> netmask <new device subnet mask> default-gateway <new device gateway>***
   b. ***system interface mgmt-vlan vlan-enabled true vlan-id <new vlan>***
      This will change the IP address and VLAN immediately. It is recommended to make this change via the Console connection, so you don't lose access to the device.
   c. write memory
6. Once changes have been committed you will have to change your Ethernet adapter information and SSH to the new Management IP address and VLAN (if applicable) you just entered.
7. Enter configuration mode ***configure***
8. Type "***sector advanced 1***" to begin sector configuration then type the below commands
   a. ***wimax max-uplink-rate QAM64_5/6***
   b. ***wimax max-downlink-rate QAM64_5/6***
   c. ***wimax antenna-tx-mode MIMO-AB***
   d. ***wimax auto-power-control open-loop***
   e. ***wimax channel-bw 10MHz***
   f. ***wimax dl-ul-frame-ratio 26:21***
      i. ***Options: 26:21, 29:18, 32:15, 35:12***
   g. ***Radio antenna-gain <applicable antenna gain>***
   h. ***Radio cable loss <applicable cable loss>***
9. ***sector general 1 system ip address <IP address> netmask <netmask> gateway <gateway>***
10. ***ctrl c***
11. ***write memory***

The Quantum 6636 should now be configured for management access on your network. This will be required for the device to communicate with the Domain Proxy. Refer to **section 3.6** of this guide for additional configuration options.

4.3 External Antennas

For operations under Part 96, the Quantum 6636 can only be used in conjunction with the Mercury Networks 3.5GHz 2-Port Antenna (098-00459-0035) in a sectorized and cross-polarized configuration, or the Mercury Networks 3.5GHz 6-port Panel Antenna (099-00455-003).

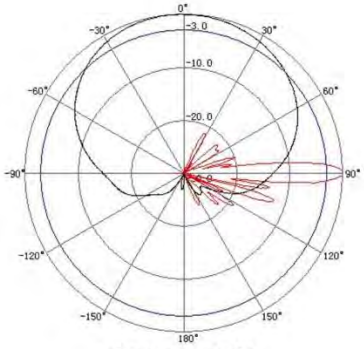
The following sections provide additional guidance for permissible antenna types and configurations for operations under Part 96. Be advised the conducted transmit power of the Quantum 6636 may need to be reduced to ensure the regulatory limit on transmitter EIRP is not exceeded. The installer must understand how to compute the effective antenna gain from the actual antenna gain and the feeder cable losses.

The range of permissible values for maximum antenna gain and feeder cable losses are taken into consideration with the domain proxy, and calculations are performed to ensure that it is not possible for the installation to exceed the EIRP limit, when the appropriate values for antenna gain and cable feeder loss are entered into the domain proxy GUI. The Quantum 6600 platform adheres to all applicable EIRP limits for transmit power when operating in MIMO mode.

4.3.1 Mercury Networks 3.3-3.8GHz 2-Port Antenna (098-00459-035)

The Mercury Networks 3.5GHz 2-Port Antenna (098-00459-0035) allows for a sectorized, cross polarized deployment. For operations under Part 96 that involve a single Quantum 6636 deployment, or "OmniWave" deployment, the following antenna array and configuration should be used to prevent overlap and interference. Antenna specifications can be found on the following table:

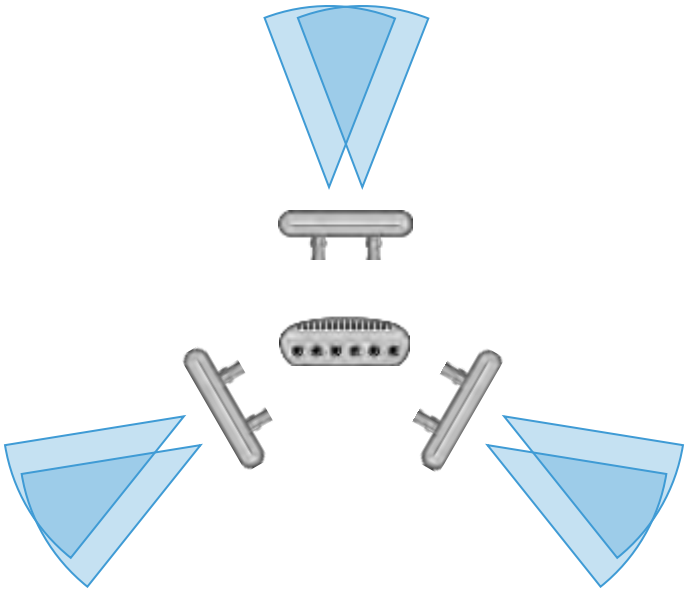
Electrical Specifications	
Frequency Bands	3300-3800 MHz
Polarization	± 45°
Horizontal -3dB Beamwidth	90°
Vertical -3dB Beamwidth	7.5°
Gain	17dBi
Impedence	50Ω
VSWR	≤ 1.5:1
Upper Side Lobe Suppression	≥ 16dB
Front-to-Back Ratio	≥ 23dB
Port-to-Port Isolation	≥ 30dB
Cross-Polar Discrimination	≥ 15dB
IM3 (20W carrier)	≤-150dBc
Input Power	200W
Lightning Protection	DC Ground
Connectors	2 x N-Type
Mechanical Characteristics	
Dimensions (L x W x D)	800 x 128 x 56mm (31.5 x 5.0 x 2.2 in)
Weight (without Mounting Brackets)	3kg (6.6lbs)
Temperature	-40° to 60°C
Survival Wind Speed	>216km/hr (>134mph)
Pole Diameter for Mounting Bracket	35-75mm (1.4-3.0in)



3300-3800MHz

	2-port antenna installation should be sectorized, cross polarized, and arranged so that the 3dB band does not overlap each other.

The recommended azimuth for a standard OmniWave deployment arranges the antennas in a manner that separation between the antennas will prevent overlap and interference. Antennas must be arranged in the following deployment.



- Sector 1 Azimuth: 0° (true north)
- Sector 2 Azimuth: 120°
- Sector 3 Azimuth: 240°

3dB Beamwidth

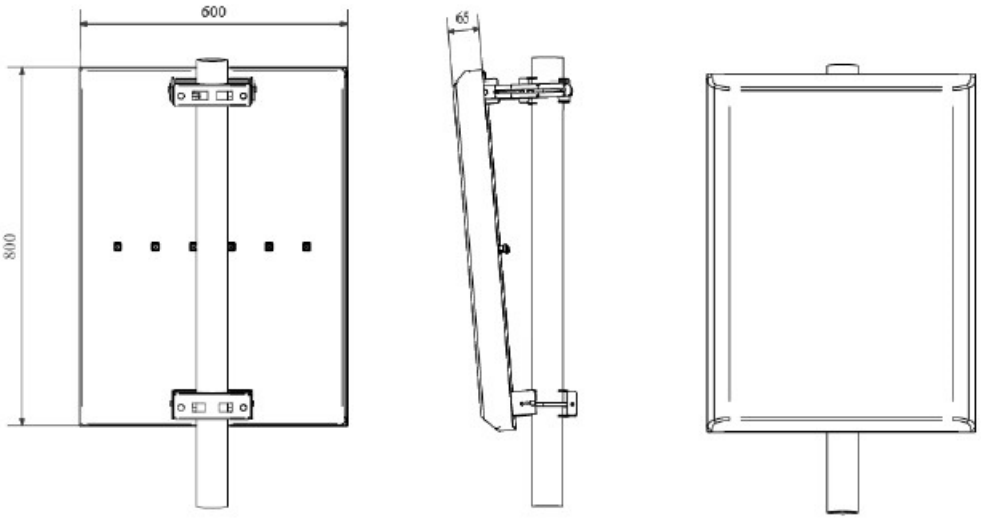
The azimuthal beamwidth between 3dB down angles shall be 90 degrees nominal. The elevation beamwidth between 3dB down angles is 8 degrees minimum

Polarization

Each array is +/-45 degree dual slant

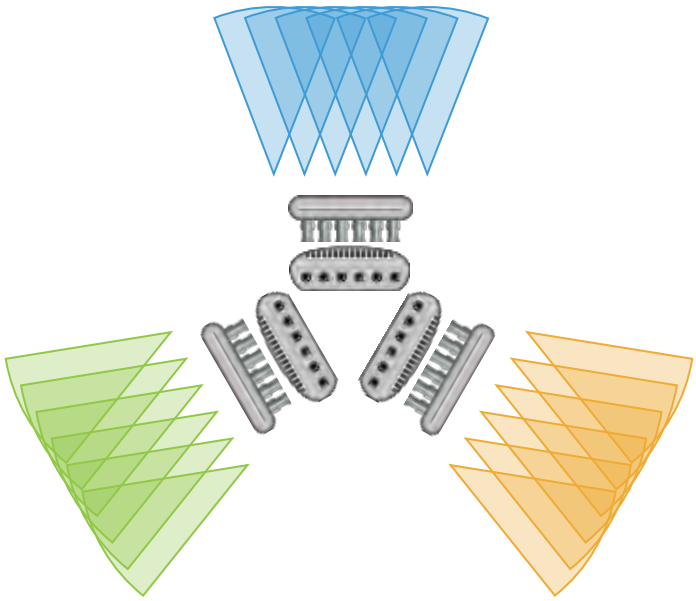
4.3.2 Mercury Networks 3.3-3.8GHz 6-Port Antenna (098-00455-003)

The Mercury Networks 3.5GHz 6-Port Antenna (099-00455-003) allows for a directional deployment of a Quantum 6636. Antenna specifications are found in the following table:



Specifications:	
Electrical	
Frequency range	3.3-3.8 GHz
GAIN, min.	15 dBi
VSWR, max.	1.8 : 1
Polarization	Dual Slant, ±45°
3 dB Beam-Width, H-Plane, typ.	90°
3 dB Beam-Width, E-Plane, min.	8°
Side Lobes, min. Elevation plane:	-12 dB
Azimuth plane:	-20 dB
Cross Polarization Discrimination, typ.	-20 dB
Port to Port Isolation, min.	20 dB
Front-to-Back Ratio, min.	30 dB
Array Element Spacing	136 mm (1.5λ on 3.3 GHz)
Input power	5 Watts average, 50 Watts peak
Input Impedance	50 Ohm
Lightning Protection	DC Grounded
Mechanical	
Dimensions (HxWxD)	800 x 600 x 41 mm
Weight	6.5 Kg.
Connector	6 x N-Type Female
Back Plane	Aluminum protected through chemical passivation
Radome	UV Protected, Plastic
Mount	MNT - 25
Environmental	
Operating Temperature Range	- 40°C to + 65°C
Vibration	According to IEC 60721-3-4
Wind Load	200 km/h (survival)
Flammability	UL94
Water Proofing	IP-65
Humidity	ETS 300 019-1-4, EN 302 085 (annex A.1.1)
Salt Fog	According to IEC 68-2-11
Ice and Snow	25mm radial (survival)

The recommended azimuth for a standard three Quantum 6636 deployment arranges the antennas in a manner that separation between the antennas will prevent overlap and interference. Antennas must be arranged in the following deployment.



- Sector 1 Azimuth: 0° (true north)
- Sector 2 Azimuth: 120°
- Sector 3 Azimuth: 240°

3dB Beamwidth
The azimuthal beamwidth between 3dB down angles shall be 90 degrees nominal. The elevation beamwidth between 3dB down angles is 8 degrees minimum

Polarization
Each array is +/-45 degree dual slant, cross-polarized with no phase-shifting

Alternative arrangements are possible, so long as each antenna has 120 degrees of separation from each azimuth measurement.

4.4 The Mercury Networks Domain Proxy

The information contained in this section will instruct you on how to connect your Quantum 6636 to the Mercury Networks Domain Proxy as a CBSD for use in the Citizens Broadband Radio Service (47 C.F.R. Part 96) band. This section is assuming the steps in **section 4.2** have been completed, as well as a review of **section 3.6.**

	You ***MUST*** have a GPS antenna connected and functional, and the Quantum 6636 ***MUST*** be obtaining GPS synchronization for the SAS to issue commands to the Base Station.

	A Certified Professional Installer (CPI) is required for activation of any CBSD for use with a SAS. The Quantum 6636, as with any CBSD, will not transmit until all necessary configuration parameters have been input into the Domain Proxy, and a CPI has signed off on the physical installation of the CBSD.

The Mercury Networks Domain Proxy is designed to act as a management platform for the Quantum 6636 product line, as well as a bridge for multiple Base Stations to communicate with a SAS. It possesses an intuitive, web-based GUI that will assist with commands issued by the SAS.

4.3.1 Accessing the Mercury Networks Domain Proxy

The Mercury Networks Domain Proxy can be accessed through a web browser by pointing your browser at the URL established for the Domain Proxy by the Mercury Networks support team. Once the page loads the User is presented with a login screen. Enter your E-mail Address and Password to get started (Figure 172).

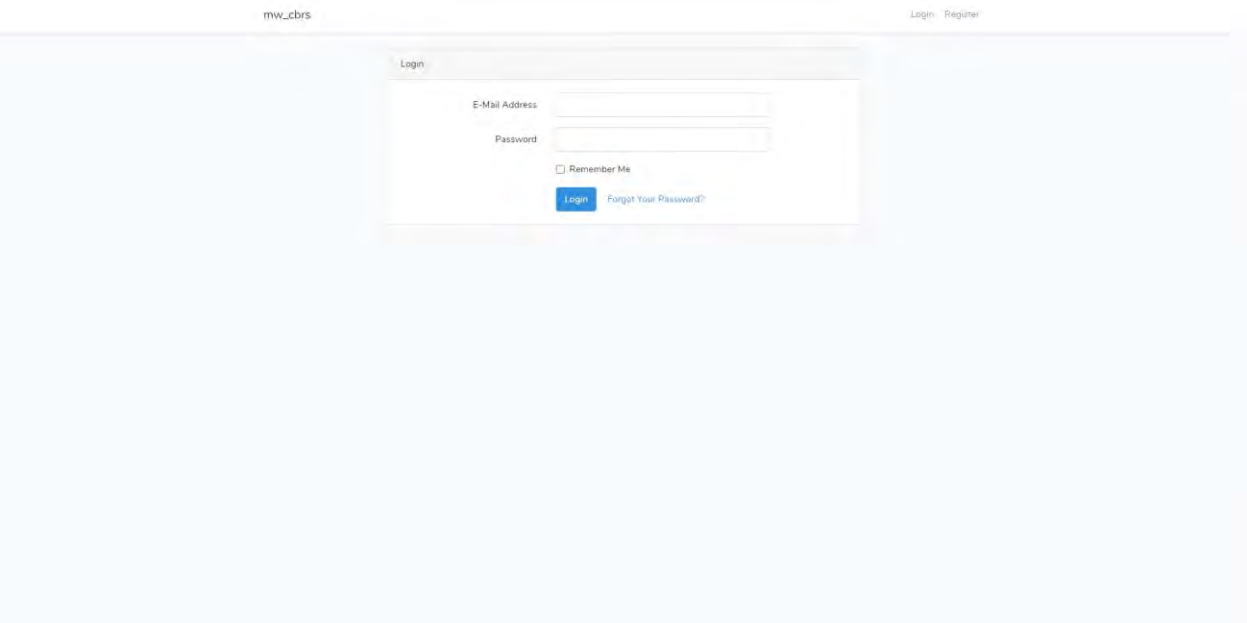


Figure 172 Domain Proxy Login

Once login credentials are successfully entered, the User is presented with a welcome screen, and tabs across the top of the screen for navigation (Figure 173).

The navigation tabs include:

- Devices – Displays a list of all CBSDs entered into the Domain Proxy
- CPIs – Displays a list of all Certified Professional Installers capable of signing-off on a CBSD installation. (Note: certificates for CPIs can be managed in the Domain Proxy, this will be covered later in this section).

- Logs – Displays operational logs for the Domain Proxy to provide information on CBSD and Domain Proxy communication with the SAS.
- Logout – Logs the User out of the Domain Proxy.

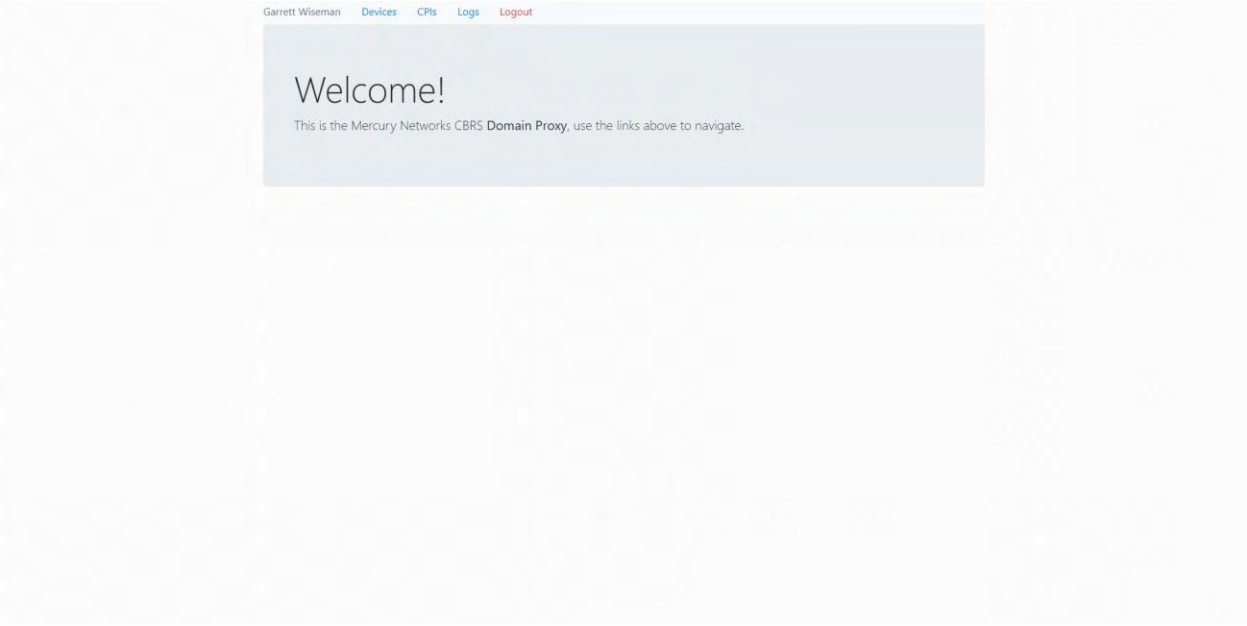


Figure 173 Welcome Screen

4.3.2 Domain Proxy – Devices

CBSDs can be managed through the domain proxy. When the Devices tab is selected the User will be presented with a list of all unregistered and registered CBSDs that have been added to the Domain Proxy for management. There are 3 navigation options in the Devices menu:

- Map – Represented by a green globe. Displays a map with locations for all registered CBSDs based on GPS coordinates.
- Add Device – Represented by a blue "+". Add a new CBSD to the Domain Proxy
- Device ID – Provides additional information for existing registered devices including configuration parameters, SAS Status, CBSD SAS ID, SAS Vendor, and the date of last update.

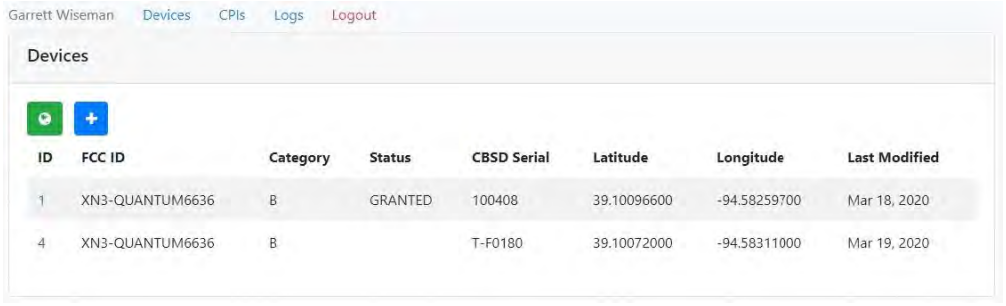


Figure 174 Devices Sub-menu

4.3.2.1 Map View

The Map View shows Users the geographic location for all CBSDs. A pin drop, which represents the CBSDs location, can be clicked on for additional information including the Device ID, Device Status, and SAS ID.

4.3.2.2 Device ID View

The Device ID View shows specific information for each CBSD managed by the Domain Proxy. This information includes a summary of the device's status with the SAS, FCC & CBSD information, installation parameters, antenna information, measurement capabilities, air interface information, CBSD hardware & software information, and a map view specific to the CBSD selected (Figures 176 and 177).

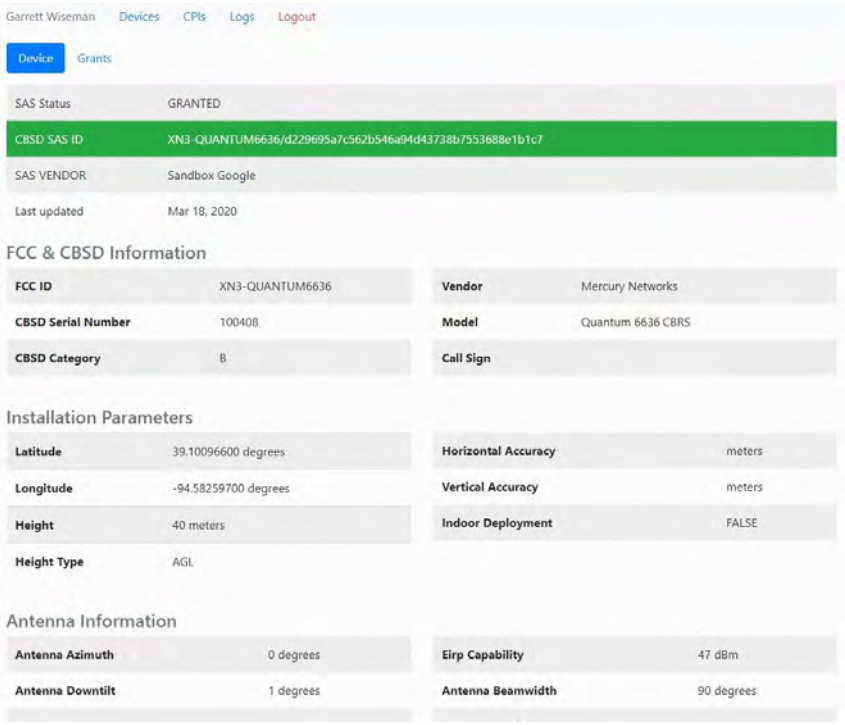


Figure 175 Device ID View

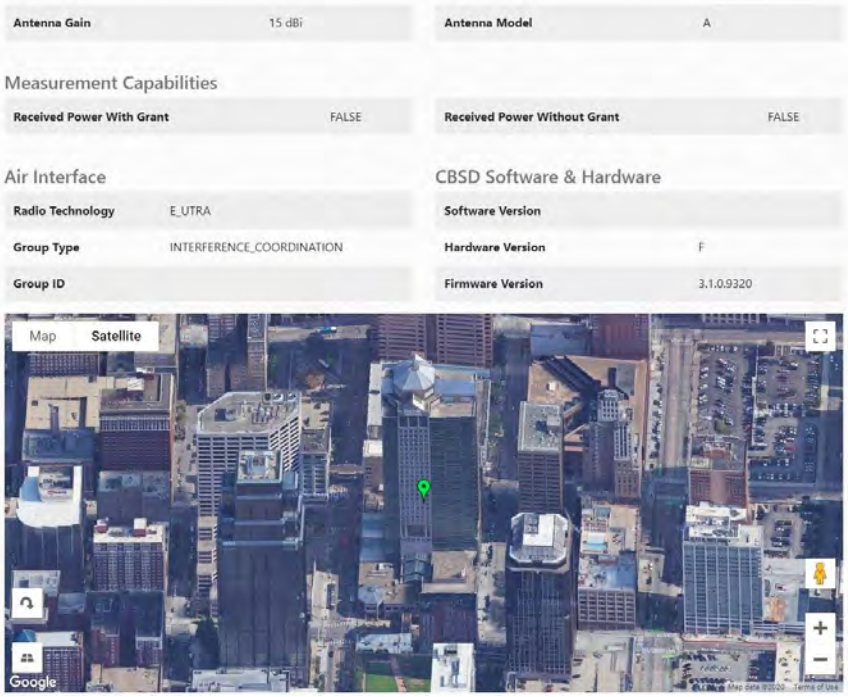


Figure 176 Device ID View Continued

4.3.2.3 Adding a Device

Clicking the blue "+" button on the devices sub-menu opens the New Device screen (Figure 178). The Quantum 6636 will need to have a management IP configured before you can add the device to the Domain Proxy. Once the management IP address is known, add it under the IP field, followed by the SNMP Community (by default this is ***private*** for most Quantum 6636 Base Stations). Once the IP and the SNMP community have been entered, select ***Query.***

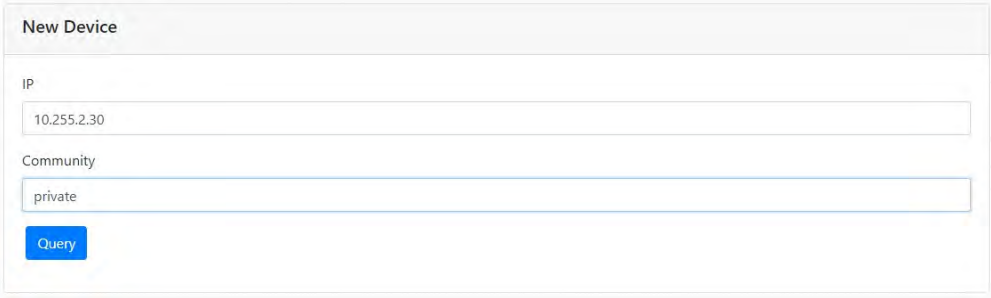


Figure 177 New Device

The User will be presented with a summary screen displaying all parameters automatically imported to the Domain Proxy (Figure 179 and 180). The following remaining parameters will need to be provided before the Quantum 6636 can be successfully added and registered to the Domain Proxy:

- Height (meters) – Height Above Average Terrain – The FCC currently provides a HAAT calculator to assist users with obtaining and entering this data (https://www.fcc.gov/media/radio/haat-calculator).

- Antenna Azimuth – The directional heading for the Quantum 6636 antenna. 0-360 degrees where 0 degrees would be used for an omniwave deployment.
- Antenna Downtilt – the mechanical downtilt of the Quantum 6636 antenna.
- Antenna Beamwidth – the degrees for the antennas horizontal plane coverage.

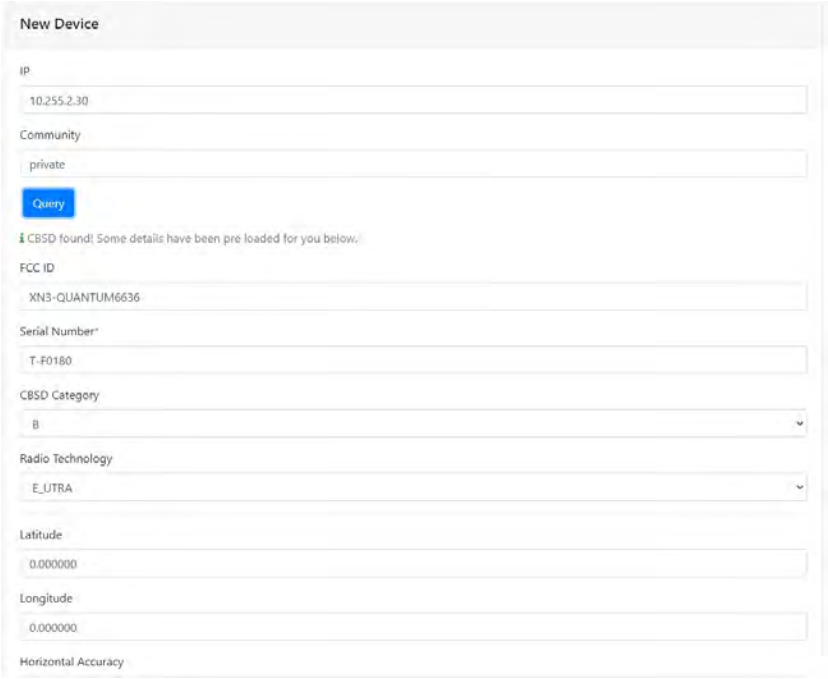


Figure 178 New Device Parameters

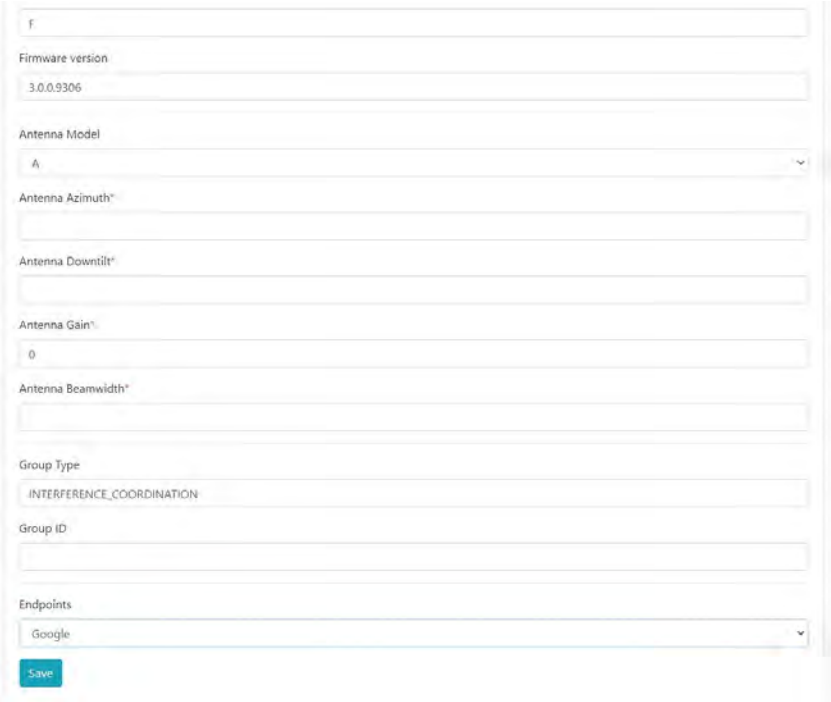


Figure 179 New Device Parameters Continued

Once all remaining parameters have been keyed, select an Endpoint (SAS) for registration and then select ‘Save’.

The User will then be presented with a summary screen where they can edit existing parameters, remove the device if it was keyed in error, or Sign & Register the device to the Domain Proxy (Figure 181).

	Note: If the User signed into the Domain Proxy is not a CPI, they will only have the ability to register the device. A CPI will still need to sign the device for communication with the SAS.

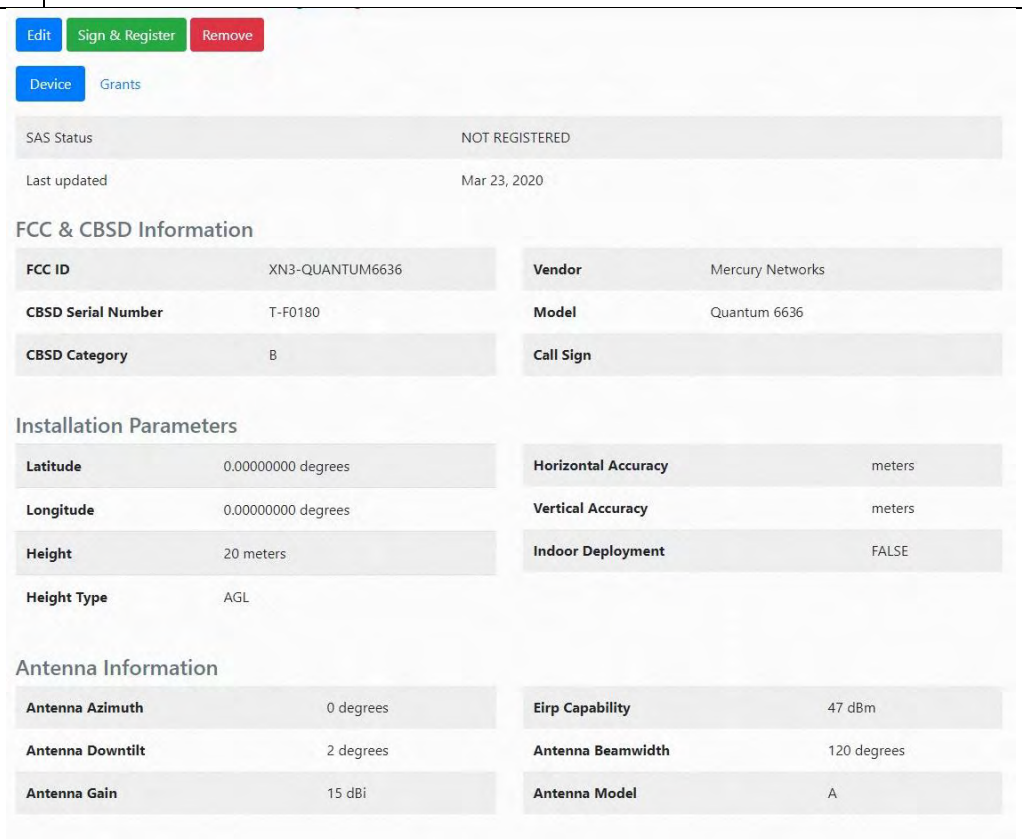


Figure 180 Device Summary

Once the Quantum 6636 has been signed and registered, it is ready to query the SAS for a grant to transmit. This can be done by selecting ‘Grants’ next to the ‘Device’ button in the summary screen.

4.3.2.4 Obtaining a Grant from the SAS

In the ‘Grants’ tab, select ‘New’ to begin the spectrum inquiry process (Figure 182). Using the drop-down menu select the frequency to perform the spectrum inquiry and then select ‘save’.

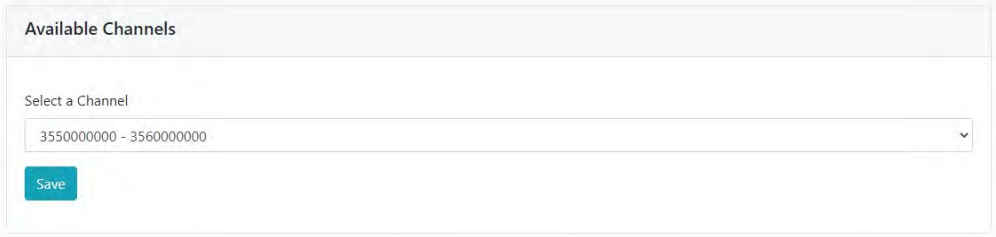


Figure 181 Spectrum Inquiry Screen

Once a grant has been received an updated SAS status will be displayed (Figure 183). The Quantum 6636 should now receive instructions from the Domain Proxy for transmit. If the requested frequency is not available an error will be displayed.

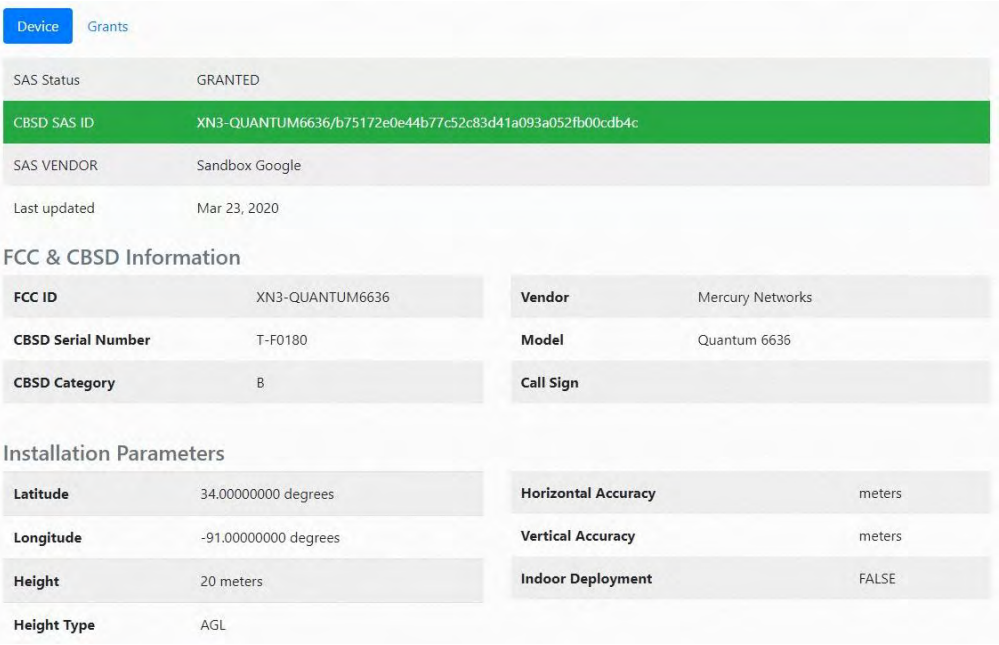


Figure 182 SAS Status Update

4.3.3 CPIs (Certified Professional Installers)

The CBRS band provides for a sophisticated multi-tier shared spectrum with protected incumbents. Pursuant to the FCC, the majority of CBRS radio transceivers or Citizen's Broadband Service Devices (CBSDs) must be installed by a CPI in order to lawfully operate within the designated spectrum of CBRS.

In order to meet the FCC Part 96 rules, CPIs must be trained and currently certified. The WInnForum's the CPI Accreditation Standard provides a working outline of how training programs for CPI will be achieved as well as what CBSDs need certification, CPI responsibilities, and more. CPIs using the Mercury Networks Domain Proxy can be managed through the CPIs menu.

4.3.3.1 Adding a New CPI

In the CPIs menu, a new CPI can be added by selecting 'Create' in the upper right-hand corner (Figure 184).

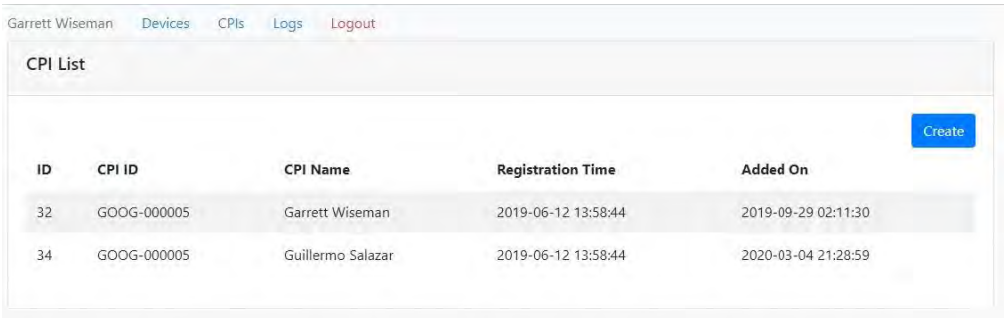


Figure 183 CPI List

A new CPI will need the unique CPI name, CPI ID, CPI password, and P12 certificate issued by the accrediting body. Certificates only need to be uploaded once and can be centrally managed by the Domain Proxy until they expire. Once the appropriate credentials have been added, select 'Save' to add the CPI (Figure 185).

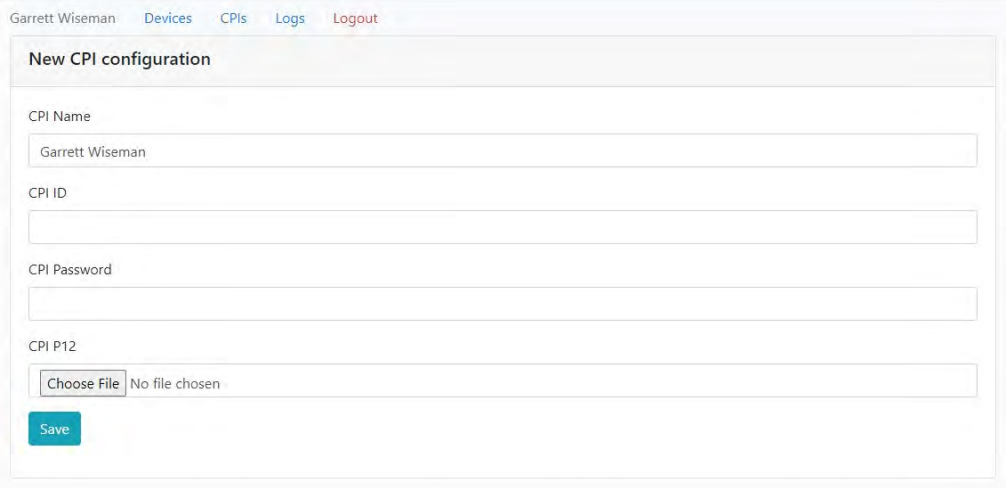


Figure 184 New CPI

4.3.4 Logs

Logs can be used to trouble-shoot and validate communication with the SAS. Output for all SAS communication is displayed under the Logs menu in the Domain Proxy (Figure 186).

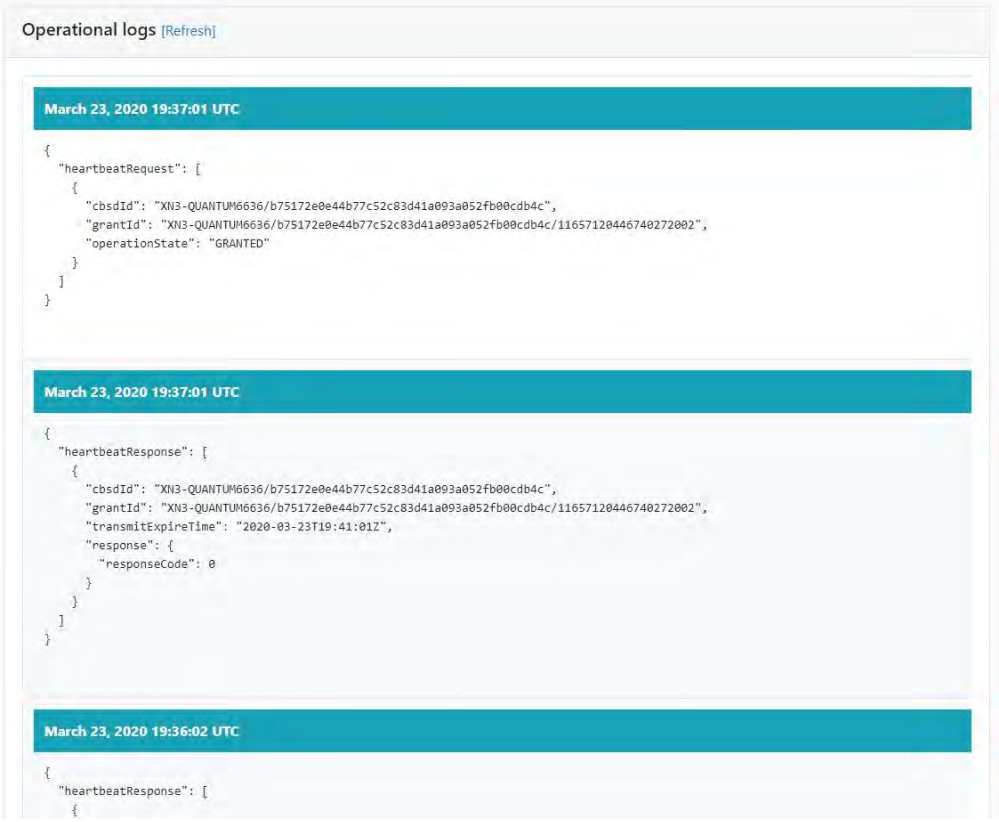


Figure 185 Operational Logs

Appendix A Capacity Tables

We present here a set of tables specifying the raw (MAC-layer) throughput of a Mercury Quantum Family base Station for 5, 7 and 10MHz, under ideal conditions, corresponding to the maximum achievable performance that can be achieved using IEEE 802.16e per channel bandwidth and TDD configuration ratio.

All results assume PUSC, a MAP size of 4 symbols, and 1 preamble symbol. The numbers represent the maximum MAC layer performance using all sub-channels and exclude Ethernet Layer 2 or higher layer overheads. Values are in units of Mbps.

Note that these results are specific to the stated configuration under ideal conditions and should be considered indicative of expected results. Actual results will vary depending upon the actual configuration, error rate, environment, and numerous other factors.

MCS Rate	10MHz			5MHz		
	Downlink	Uplink	Bi-Dir	Downlink	Uplink	Bi-Dir
64QAM-5/6	21.60	5.04	25.44	10.8	2.45	13.25
64QAM-3/4	19.44	4.54	22.90	9.72	2.2	11.92
64QAM-2/3	17.28	4.03	20.35	8.64	1.96	10.6
64QAM-1/2	12.96	3.02	15.26	6.48	1.47	7.95
16QAM-3/4	12.96	3.02	15.26	6.48	1.47	7.95
16QAM-1/2	8.64	2.02	10.18	4.32	0.98	5.3
QPSK-3/4	6.48	1.51	7.63	3.24	0.73	3.97
QPSK-1/2	4.32	1.01	5.09	2.16	0.49	2.65

Table 14 Max Throughput 35:12 - 74%:26%

MCS Rate	10MHz			5MHz		
	Downlink	Uplink	Bi-Dir	Downlink	Uplink	Bi-Dir
64QAM-5/6	18.72	6.72	25.44	9.36	3.26	12.62
64QAM-3/4	16.85	6.05	22.90	8.42	2.94	11.36
64QAM-2/3	14.98	5.38	20.35	7.49	2.61	10.10
64QAM-1/2	11.23	4.03	15.26	5.62	1.96	7.57
16QAM-3/4	11.23	4.03	15.26	5.62	1.96	7.57
16QAM-1/2	7.49	2.69	10.18	3.74	1.31	5.05
QPSK-3/4	5.62	2.02	7.63	2.81	0.98	3.79
QPSK-1/2	3.74	1.34	5.09	1.87	0.65	2.52

Table 15 Max Throughput - 32:15 - 68%:32%

MCS Rate	10MHz			5MHz		
	Downlink	Uplink	Bi-Dir	Downlink	Uplink	Bi-Dir
64QAM-5/6	17.28	8.40	25.68	8.64	4.08	12.72
64QAM-3/4	15.55	7.56	23.11	7.78	3.67	11.45
64QAM-2/3	13.82	6.72	20.54	6.91	3.26	10.18
64QAM-1/2	10.37	5.04	15.41	5.18	2.45	7.63
16QAM-3/4	10.37	5.04	15.41	5.18	2.45	7.63
16QAM-1/2	6.91	3.36	10.27	3.46	1.63	5.09
QPSK-3/4	5.18	2.52	7.70	2.59	1.22	3.82
QPSK-1/2	3.46	1.68	5.14	1.73	0.82	2.54

Table 16 Max Throughput - 29:18 - 62%:38%

MCS Rate	10MHz			5MHz		
	Downlink	Uplink	Bi-Dir	Downlink	Uplink	Bi-Dir
64QAM-5/6	14.40	10.08	24.48	7.20	4.90	12.10
64QAM-3/4	12.96	9.07	22.03	6.48	4.41	10.89
64QAM-2/3	11.52	8.06	19.58	5.76	3.92	9.68
64QAM-1/2	8.64	6.05	14.69	4.32	2.94	7.26
16QAM-3/4	8.64	6.05	14.69	4.32	2.94	7.26
16QAM-1/2	5.76	4.03	9.79	2.88	1.96	4.84
QPSK-3/4	4.32	3.02	7.34	2.16	1.47	3.63
QPSK-1/2	2.88	2.02	4.90	1.44	0.98	2.42

Table 17 Max Throughput - 26:21 - 55%:45%

MCS Rate	7MHz		
	Downlink	Uplink	Bi-Dir
64QAM-5/6	11.5	5.0	16.6
64QAM-3/4	10.4	4.5	14.9
64QAM-2/3	9.2	4.0	13.2
16QAM-3/4	6.9	3.0	9.9
16QAM-1/2	4.6	2.0	6.6
QPSK-3/4	3.5	1.5	5.0
QPSK-1/2	2.3	1.0	3.3

Table 18 Max Throughput - 21:12 - 64%:36%

MCS Rate	7MHz		
	Downlink	Uplink	Bi-Dir
64QAM-5/6	13.0	3.4	16.3
64QAM-3/4	11.7	3.0	14.7
64QAM-2/3	10.4	2.7	13.1
16QAM-3/4	7.8	2.0	9.8
16QAM-1/2	5.2	1.3	6.5
QPSK-3/4	3.9	1.0	4.9
QPSK-1/2	2.6	0.7	3.3

Table 19 Max Throughput - 23:9 - 72%:28%

MCS Rate	7MHz		
	Downlink	Uplink	Bi-Dir
64QAM-5/6	8.6	6.7	15.4
64QAM-3/4	7.8	6.0	13.8
64QAM-2/3	6.9	5.4	12.3
16QAM-3/4	5.2	4.0	9.2
16QAM-1/2	3.5	2.7	6.1
QPSK-3/4	2.6	2.0	4.6
QPSK-1/2	1.7	1.3	3.1

Table 20 Max Throughput - 17:15 - 53%:47%

Appendix B Changes Requiring a Reboot

- gps enabled
- sector general 1
    - system bs-id
    - system cell-id
    - system cs-type
    - system ip address
    - system ip netmask
    - system ip gateway
    - system mode
    - system downlink-broadcast-rate
    - system block-dhcp-downlink-broadcasts
    - system cpe-to-cpe-relay-enabled
    - system cpe-to-cpe-brodcast-relay-enabled
- sector advanced 1
    - wimax auto-power-control
    - wimax dl-ul-frame-ratio
    - wimax max-distance
    - wimax large-map-enabled
    - security ak-lifetime
    - security enabled
    - security tek-lifetime
- system interface mgmt-vlan vlan-enabled
- system interface mgmt-vlan vlan-id
- system interface mgmt-vlan vlan-priority
- system base-station asn-gateway ip-address
- system base-station asn-gateway port-number
- system base-station radius ip-address
- system base-station radius port-number
- system base-station radius secret
- system base-station mode

Appendix C Limited Warranty Statements

Hardware

Mercury, Inc. (“Mercury” or the “Company”) warrants to the original end-user (“Customer”) that this hardware product will conform in all material respects to the specifications provided with the hardware and will be free from defects in workmanship and materials, under normal use and service, for a period of 365 days from the date of original shipment by Mercury.

Mercury's sole obligation under this limited warranty shall be, at Mercury's option, to repair the defective product or part, deliver to Customer an equivalent product or part to replace the defective item, or if neither of the two foregoing options is reasonably possible, refund to Customer the purchase price paid for the defective product. All products that are replaced will become the property of Mercury. Replacement products may be new or reconditioned. Mercury's obligations hereunder are conditioned upon the returned of affected articles in accordance with Mercury's Return Material Authorization (RMA) procedures.

The above warranty will also apply to any replaced or repaired product for 90 days from the date of shipment from Mercury of the replaced or repaired product, or the remainder of the initial warranty period, whichever is longer.

Software

Mercury warrants to the Customer that for a period of ninety (90) days from your receipt of the Product as demonstrated by written records (the “Warranty Period”) the Software will perform substantially in accordance with the Documentation.

If the Software fails to comply with the warranty set forth above, your exclusive remedy will be, at the option of Mercury (i) a reasonable effort by Mercury to make the Software perform substantially in accordance with the Documentation, or (ii) return of the purchase price. This limited warranty applies only if you return all copies of the Product, together with proof of purchase, to Mercury during the Warranty Period.

This limited warranty is VOID if failure of the Software is due to modification of the Software not made by Mercury, or the abuse or misapplication of the Software.

MERCURY DOES NOT WARRANT THAT THE SOFTWARE IS ERROR FREE, THAT THE CUSTOMER WILL BE ABLE TO OPERATE THE SOFTWARE WITHOUT PROBLEMS OR INTERRUPTIONS OR THAT THE SOFTWARE OR ANY EQUIPMENT, SYSTEM OR NETWORK ON WHICH THE SOFTWARE IS USED WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK.

Additional Conditions

Notwithstanding anything else herein or otherwise, Mercury reserves the right to establish amendments to its RMA Policy from time to time. Further, Mercury Technical Support may prefer to troubleshoot the wireless link with an onsite Customer technician while the Products are in their original non-conforming state. This process might assist Customer in understanding and troubleshooting the issue. If Mercury was not afforded the opportunity to troubleshoot an allegedly non-conforming Product in original non-conforming state, Mercury may approve or reject an RMA request in its sole discretion.

No Fault Found

Notwithstanding sections above, if Mercury cannot duplicate any alleged non-conformity, the Product will be returned to the Customer as "No Fault Found." Mercury reserves the right to charge a testing fee in connection with a returned product that Mercury determines as “No Fault Found,” and any such payment must be received by Mercury prior to return shipment of the applicable Product to Customer.

Warranty Limitations

Mercury’s warranties do not apply to any product (hardware or software) which has (a) been subjected to abuse, misuse, neglect, accident, or mishandling, (b) been opened, repaired, modified, or altered by anyone other than Mercury, (c) been used for or subjected to applications, environments, or physical or electrical stress or conditions other than as intended and recommended by Mercury, (d) been improperly stored, transported, installed, or used, or (e) had its serial number or other identification markings altered or removed.

Warranty Disclaimer

PURWAVE’S SPECIFIC WARRANTIES SUMMARIZED ABOVE ARE THE ONLY WARRANTIES GIVEN BY MERCURY WITH RESPECT TO ITS PRODUCTS (HARDWARE AND SOFTWARE) AND ARE GIVEN IN LIEU OF ANY AND ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR ARISING BY CUSTOM, TRADE USAGE, OR COURSE OF DEALING, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, AND MERCURY DISCLAIMS ANY AND ALL OTHER WARRANTIES TO THE MAXIMUM EXTENT PERMITTED BY LAW. Without limiting the generality of the foregoing sentence, Mercury makes no warranty or representation, either expressed or implied, as to, and disclaims all liability and responsibility for, (a) the operation, compliance, labeling, or packaging of any of its products under the laws of any jurisdiction outside of the United States of America and (b) the regulatory compliance of any products in any jurisdiction in which it has not specifically identified compliance or the use of any product in any jurisdiction in any manner other than as contemplated in the regulatory certifications and approvals for that product in that jurisdiction. To the extent an implied warranty cannot be excluded, such warranty is limited in duration to the warranty period. The disclaimer and exclusion apply even if the express warranty fails of its essential purpose.

Obtaining Warranty Service

Customer must contact the Company, by sending an e-mail to support@mercurynets.com to obtain warranty service authorization. When contacting Mercury for support, please be prepared to provide the product description and serial number and a description of the problem. The Customer will be expected to complete a “Return Material Authorization (RMA)” form to initiate the request. Full instructions as to how to complete and where to send the form are provided on the form. Date of proof of purchase from Mercury will be required.

Products returned to Mercury Inc. must be pre-authorized by Mercury with a Return Material Authorization (RMA) number and sent prepaid and packaged appropriately for safe shipment. The Customer requesting the RMA will be the exporter. The exporter is responsible to ship RMA equipment

to Mercury's address and has to bear the cost and risk involved in bringing the goods to Mercury's location.

Risk of loss in return shipment will be borne by Customer, and it is recommended that returned goods be insured and/or sent by a method that provides for tracking of the package. Responsibility for loss or damage does not transfer to Mercury until the returned item is received by Mercury. Provided that Mercury determines that the item is actually defective, the repaired or replaced item will be shipped to Customer, at Mercury's expense, (1) not later than thirty (30) days after Mercury receives the defective product or (2) to the terms of a separate written agreement with Mercury.

If the allegedly non-conforming Product is not received by Mercury within thirty (30) days of Customer initiating the RMA request, the RMA process for that Product will be deemed cancelled.

You may also obtain the status of their RMA request(s) by sending an e-mail to support@mercurynets.com referencing their assigned RMA Number(s).

No product will be accepted for repair or replacement by Mercury without a RMA number. The product must be returned to Mercury, properly packaged to prevent damage, shipping and handling charges prepaid, with the ***RMA number prominently displayed on the outside of the container***. If Mercury determines that a returned product is not defective or is not covered by the terms of the warranty, the Customer will be charged a service charge and return shipping charges.

RMA Related Issue	Under Warranty
Repair and return	No charge, Mercury Networks pays
Shipment of unit to Mercury Networks	Customer pays
Regular shipment to customer	No charge, Mercury Networks pays
Expedited shipment to customer	Customer pays the additional cost of the expedited shipping
No fault found	Mercury Networks reserves the right to levy a charge
Warranty for repaired and/or replaced product	Remainder of the original warranty or 90 days

Table 21 Summary of Mercury RMA Conditions and Changes

Assistance

For assistance, contact your nearest Mercury Networks Sales and Service office. Additional information is available on the Mercury Networks website at http://www.mercurynets.com.

For Customer Service call: +1-888-909-6717, or Email: support@mercurynets.com.