FRC BSMAX-250
WIMAX BASE STATION

User Manual

Rev 1.0

Legal Rights

The material contained herein is proprietary, privileged, and confidential and owned by FRC Internet Products, LLC ("FRC"), its affiliates or its third party licensors. No disclosure thereof shall be made to third parties without the express written permission of FRC.

FRC reserves the right to alter the equipment specifications and descriptions in this publication without prior notice. No part of this publication shall be deemed to be part of any contract or warranty unless specifically incorporated by reference into such contract or warranty.

Trade Names

FRC®, The Blue Zone®, The BlueZone™, CPEMax™, BSMax™ and/or other products and/or services referenced herein are either registered trademarks or service marks of FRC Group.

All other names are or may be the trademarks of their respective owners. "WiMAX Forum" is a registered trademark of the WiMAX Forum. "WiMAX," the WiMAX Forum logo, "WiMAX Forum Certified," and the WiMAX Forum Certified logo are trademarks of the WiMAX Forum.

Statement of Conditions

The information contained in this manual is subject to change without notice.

FRC shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or equipment supplied with it.

Warranties and Disclaimers

All FRC products purchased from FRC or through any of FRC's authorized resellers are subject to the following warranty and product liability terms and conditions.

Exclusive Warranty

(a) FRC warrants that the Product hardware it supplies and the tangible media on which any software is installed, under normal use and conditions, will be free from significant defects in materials and workmanship for a period of twelve (12) months from the date of shipment of a given Product to Purchaser (the "Warranty Period"). FRC will, at its sole option and as Purchaser's sole remedy, repair or replace any defective Product in accordance with FRC' standard R&R procedure.

(b) With respect to the Firmware, FRC warrants the correct functionality according to the attached documentation, for a period of twelve (12) month from invoice date (the "Warranty Period")". During the Warranty Period, FRC may release to its Customers firmware updates, which include additional performance improvements and/or bug fixes, upon availability (the "Warranty"). Bug fixes, temporary patches and/or workarounds may be supplied as Firmware updates. Additional hardware, if required, to install or use Firmware updates must be purchased by the Customer. FRC will be obligated to support solely the two (2) most recent Software major releases.

FRC SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY PURCHASER'S OR ANY THIRD PERSON'S MISUSE, NEGLIGENCE, IMPROPER INSTALLATION OR IMPROPER TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING OR OTHER HAZARD.

Disclaimer

(a) The Software is sold on an "AS IS" basis. FRC, its affiliates or its licensors

MAKE NO WARRANTIES, WHATSOEVER, WHETHER EXPRESS OR IMPLIED, WITH RESPECT TO THE SOFTWARE AND THE ACCOMPANYING DOCUMENTATION FRC SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT WITH RESPECT TO THE SOFTWARE. UNITS OF PRODUCT (INCLUDING ALL THE SOFTWARE) DELIVERED TO PURCHASER HEREUNDER ARE NOT FAULT-TOLERANT AND ARE NOT DESIGNED, MANUFACTURED OR INTENDED FOR USE OR RESALE IN APPLICATIONS WHERE THE FAILURE, MALFUNCTION OR INACCURACY OF PRODUCTS CARRIES A RISK OF DEATH OR BODILY INJURY OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE ("HIGH RISK ACTIVITIES"). HIGH RISK ACTIVITIES MAY INCLUDE, BUT ARE NOT LIMITED TO, USE AS PART OF ON-LINE CONTROL SYSTEMS IN HAZARDOUS ENVIRONMENTS REQUIRING FAIL-SAFE PERFORMANCE, SUCH AS IN THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, AIR TRAFFIC CONTROL, LIFE SUPPORT MACHINES, WEAPONS SYSTEMS OR OTHER APPLICATIONS REPRESENTING A SIMILAR DEGREE OF POTENTIAL HAZARD. FRC SPECIFICALLY DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY OF FITNESS FOR HIGH RISK ACTIVITIES.

(b) PURCHASER'S SOLE REMEDY FOR BREACH OF THE EXPRESS WARRANTIES ABOVE SHALL BE REPLACEMENT OR REFUND OF THE PURCHASE PRICE AS SPECIFIED ABOVE, AT FRC'S OPTION. TO THE FULLEST EXTENT ALLOWED BY LAW, THE WARRANTIES AND REMEDIES SET FORTH IN THIS AGREEMENT ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING BUT NOT LIMITED TO WARRANTIES, TERMS OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, NON-INFRINGEMENT, AND ACCURACY OF INFORMATION GENERATED. ALL OF WHICH ARE EXPRESSLY DISCLAIMED. FRC' WARRANTIES HEREIN RUN ONLY TO PURCHASER, AND ARE NOT EXTENDED TO ANY THIRD PARTIES. FRC NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS.

Limitation of Liability

(a) FRC SHALL NOT BE LIABLE TO THE PURCHASER OR TO ANY THIRD PARTY, FOR ANY LOSS OF PROFITS, LOSS OF USE, INTERRUPTION OF BUSINESS OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES OF ANY KIND, WHETHER ARISING UNDER BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE AND WHETHER BASED ON THIS AGREEMENT OR OTHERWISE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

(b) TO THE EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE LIABILITY FOR DAMAGES HEREUNDER OF FRC OR ITS EMPLOYEES OR AGENTS EXCEED THE PURCHASE PRICE PAID FOR THE PRODUCT BY PURCHASER, NOR SHALL THE AGGREGATE LIABILITY FOR DAMAGES TO ALL PARTIES REGARDING ANY PRODUCT EXCEED THE PURCHASE PRICE PAID FOR THAT PRODUCT BY THAT PARTY (EXCEPT IN THE CASE OF A BREACH OF A PARTY'S CONFIDENTIALITY OBLIGATIONS).

Electronic Emission Notices

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC and to EN 301 489-1 rules. 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 of the following measures:

- Reorient or relocate the receiving antenna.

- Increase the separation between the equipment and 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/TV technician for help.

Operation is subject to the following two conditions:

1. This device may not cause harmful interference.

2. This device must accept any interference received, including interference that may cause undesired operation.

Radio Frequency Interference Statement

This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to part 15 of the FCC rules and to EN 301 489-1 rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential environment notwithstanding use in commercial, business and industrial environments. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

FCC Radiation Hazard Warning

To comply with FCC and ETSI RF exposure requirement, the antenna used for this equipment must be fixed-mounted on outdoor permanent structures with a separation distance of at least 100 centimeters from all persons.

R&TTE Compliance Statement

This equipment is confirmed to comply with the requirements set in the Council Directive of the Approximation of the laws of the Member States relating to R&TTE Directive (1999/5/EC) that include the Electromagnetic Compatibility Directive (2004/108/EC) and Low Voltage Directive (2006/95/EC).

Caution

To avoid electrical shock, do not perform any servicing unless you are qualified to do so.

Line Voltage

Before connecting this instrument to the power line, make sure that the voltage of the power source matches the requirements of the instrument. The unit must be connected to an earthed (grounded) outlet to comply with international safety standards.

Radio

The instrument transmits radio energy during normal operation. To avoid possible harmful exposure to this energy, do not stand or work for extended periods of time in front of its antenna. The long-term characteristics or the possible physiological effects of Radio Frequency Electromagnetic fields have not been yet fully investigated.

Outdoor Unit and Antenna Installation and Grounding

Ensure that outdoor units, antennas and supporting structures are properly installed to eliminate any physical hazard to either people or property. Make sure that the installation of the outdoor unit, antenna and cables is performed in accordance with all relevant national and local building and safety codes. Even where grounding is not mandatory according to applicable regulation and national codes, it is highly recommended to ensure that the outdoor unit and the antenna mast (when using external antenna) are grounded and suitable lightning protection devices are used so as to provide protection against voltage surges and static charges. In any event, FRC, The Supplier, is not liable for any injury, damage or regulation violations associated with or caused by installation, grounding or lightning protection.

Disposal of Electronic and Electrical Waste

Pursuant to the WEEE EU Directive electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Important Notice

This user manual is delivered subject to the following conditions and restrictions:

- This manual contains proprietary information belonging to FRC. Such information is supplied solely for the purpose of assisting properly authorized users of the respective FRC products.

- No part of its contents may be used for any other purpose, disclosed to any person or firm or reproduced by any means, electronic and mechanical, without the express prior written permission of FRC.

- The text and graphics are for the purpose of illustration and reference only.

- The specifications on which they are based are subject to change without notice.

- The software described in this document is furnished under a license. The software may be used or copied only in accordance with the terms of that license.

- Information in this document is subject to change without notice.

- FRC reserves the right to alter the equipment specifications and descriptions in this publication without prior notice. No part of this publication shall be deemed to be part of any contract or warranty unless specifically incorporated by reference into such contract or warranty.

- The information contained herein is merely descriptive in nature, and does not constitute an offer for the sale of the product described herein.

- Any changes or modifications of equipment, including opening of the equipment not expressly approved by FRC will void equipment warranty and any repair thereafter shall be charged for. It could also void the user's authority to operate the equipment.

Some of the equipment provided by FRC and specified in this manual, is manufactured and warranted by third parties. All such equipment must be installed and handled in full compliance with the instructions provided by such manufacturers as attached to this manual or provided thereafter by FRC or the manufacturers. Non-compliance with such instructions may result in serious damage and/or bodily harm and/or void the user's authority to operate the equipment and/or revoke the warranty provided by such manufacturer.

GLOSSARY

This section defines or identifies technical terms, abbreviations, and acronyms used throughout this document.

100BASE-TX IEEE 802.3u specification for 100 Mbps Fast Ethernet over two pairs of Category 5 or better UTP cable.

10BASE-T IEEE 802.3 specification for 10 Mbps Ethernet over two pairs of Category 3 or better UTP cable.

Administrator An administrator performs the service of maintaining a network. In the case of this device, the person who sets up the device and makes changes to the settings.

Advanced Encryption Standard (AES) A strong encryption algorithm that implements symmetric key cryptography.

Authentication The process to verify the identity of a client requesting network access.

Auto-negotiation Signaling method allowing each node to select its optimum operational mode (speed and duplex mode) based on the capabilities of the node to which it is connected.

Base Station A WIMAX service provider's equipment that is installed at a fixed location to provide network connectivity for subscriber stations within a defined service area.

Client A computer on the network that uses the services of the Router, such as the automatic DHCP server and Firewall.

Customer Premise Equipment (CPE) Customer Premise Equipment: Communications equipment that resides on the customer's premises. In FRC Wimax system, this also referred to as **Subscriber station (SS) or Mobile station (MS).**

Demilitarized Zone (DMZ) A virtual zone in the router that is not protected by The Router's firewall. One computer can be placed in the DMZ.

Domain Name System (DNS) A system used for translating host names for network nodes into IP addresses. DNS allows Internet host computers to have a domain name (such as belkin.com) and one or more IP addresses (such as 192.34.45.8). A DNS server keeps a database of host computers and their respective domain names and IP addresses, so that when a domain name is requested (as in typing **easyDNS.com** into an Internet browser), the user is sent to the proper IP address. The DNS server address used by the computers on the home network is the location of the DNS server the ISP has assigned.

Dynamic Host Control Protocol (DHCP) Dynamic Host Configuration Protocol: Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

Dynamic IP An IP address that is automatically obtained from a DHCP server.

Ethernet A popular local area data communications network, which accepts transmission from computers and terminals. A standard for computer networks. Ethernet networks are connected by special cables and hubs, and move data around at up to 10 gigabits per second (Gbps).

Encryption Data passing between a base station and clients can use encryption to protect from interception and eves-dropping.

Extensible Authentication Protocol (EAP) An authentication protocol used to authenticate network clients. EAP is combined with IEEE 802.1X port authentication and a RADIUS authentication server to provide "mutual authentication" between a client, the access point, and the a RADIUS server

File Transfer Protocol (FTP) File Transfer Protocol: A TCP/IP protocol used for file transfer.

Firewall An electronic boundary that prevents unauthorized users from accessing certain files or computers on a network.

Firmware Software stored in memory. Essential programs that remain even when the system is turned off. Firmware is easier to change than hardware but more permanent than software stored on a disk.

Hypertext Transfer Protocol (HTTP) Hypertext Transfer Protocol: HTTP is a standard used to transmit and receive all data over the World Wide Web.

IEEE 802.16e A standard that provides mobile broadband wireless access using Scalable Orthogonal Frequency Division Multiple Access (SOFDMA).

IP Address IP stands for Internet Protocol. An IP address consists of a series of four numbers separated by periods, that identifies a single, unique Internet computer host. Example: 192.34.45.8.

ISP Internet Service Provider. An ISP is a business that provides connectivity to the Internet for individuals and other businesses or organizations.

ISP Gateway Address (see ISP for definition). The ISP Gateway Address is an IP address for the Internet router located at the IPS's office. This address is required when using a cable, DSL or wireless modem.

Local Area Network (LAN) A LAN is a group of computers and devices connected together in a relatively small area (such as a house or an office). A home network is considered a LAN.

MAC Media Access Control: The lower of the two sub-layers of the data link layer defined by the IEEE. The MAC sub-layer handles access to shared media, such as whether token passing or contention will be used.

MAC Address Standardized data link layer address that is required for every port or device that connects to a LAN. Other devices in the network use these addresses to locate specific ports in the network and to create and update routing tables and data structures. MAC addresses are six bytes long and are controlled by the IEEE.

Orthogonal Frequency Division Multiplexing (OFDM) Orthogonal Frequency Division Multiplexing: OFDM allows multiple users to transmit in an allocated band by dividing the bandwidth into many narrow bandwidth carriers.

Power over Ethernet (PoE) Power over Ethernet: A specification for providing both power and data to low-power network devices using a single Category 5 Ethernet cable. PoE provides greater flexibility in locating network devices, and significantly decreased installation costs.

MTU Maximum Transmission Unit. The largest unit of data that can be transmitted on any particular physical medium.

NAT Network Address Translation. This process allows all of the computers on the home network to use one IP address. Using the NAT capability of the Home-Connect home network gateway, access is available to the Internet from any computer on the home network without having to purchase more IP addresses from the ISP.

Port A logical channel that is identified by its unique port number. Applications listen on specific ports for information that may be related to it.

PPPoE Point-to-Point Protocol over Ethernet. Point-to-Point Protocol is a method of secure data transmission originally created for dial-up connections; PPPoE is for Ethernet connections.

PPTP Point-to-Point Tunneling Protocol. A version of PPP (Point-to-Point Protocol) that has the ability to encapsulate packets of data formatted for one network protocol in packets used by another protocol. This tunneling technique allows TCP/IP data to be transmitted over a non-TCP/IP network. PPTP can be used to join different physical networks using the Internet as an intermediary.

SNTP Simple Network Time Protocol. A communication standard that allows for the transmission of real time information over a network or the Internet.

SPI Stateful Packet Inspection. SPI is the type of corporate-grade Internet security provided by a HomeConnect home network gateway. Using SPI, the gateway acts as a firewall, protecting the network from computer hackers.

Static IP An IP address that is manually configured and never changes.

Subnet Mask A subnet mask, which may be a part of the TCP/IP information provided by the ISP, is a set of four numbers configured like an IP address. It is used to create IP address numbers used only within a particular network (as opposed to valid IP address numbers recognized by the Internet, which must assigned by Inter-NIC).

Subscriber Station A general term for a customer's WIMAX terminal equipment that provides connectivity with a base station.

TCP Transmission Control Protocol. The most common Internet transport layer protocol. TCP is connection-oriented and stream-oriented, and provides for reliable communication over packet-switched networks.

TCP / IP Transmission Control Protocol over Internet Protocol. This is the standard protocol for data transmission over the Internet.

Trivial File Transfer Protocol (TFTP) Trivial File Transfer Protocol: A TCP/IP protocol commonly used for software downloads.

UDP User Datagram Protocol. Communications protocol for the Internet Network layer, transport layer, and session layer, which makes it possible to send a datagram message from one computer to an application running in another computer. Unlike TCP, UDP is connectionless and does not guarantee reliable communication; the application itself must process any errors and check for reliable delivery.

UTP Unshielded twisted-pair cable.

WAN Wide Area Network. A network that connects computers located in Geographically separate areas, (i.e., different buildings, cities, countries). The Internet is a wide area network.

WAN IP Address The IP address assigned to the router by the ISP.

WLAN Wireless Local Area Network. A local area network that connects Computers close together via radio (such as 802.11b)

Contents

1. BASE STATION INTRODUCTION & INSTALLATION

1.1 GENERAL INTRODUCTION

The FRC Wimax Base station BSMax-250 is an all-outdoor micro-level WiMax base station that complies with WiMax standard IEEE 802.16e-2005 and operates in the frequency range of 2497.75~2688.25MHz. Below are pictures (front view and back view) of the base station set with antenna.

Figure 1: BSMax-250 and antenna, front view

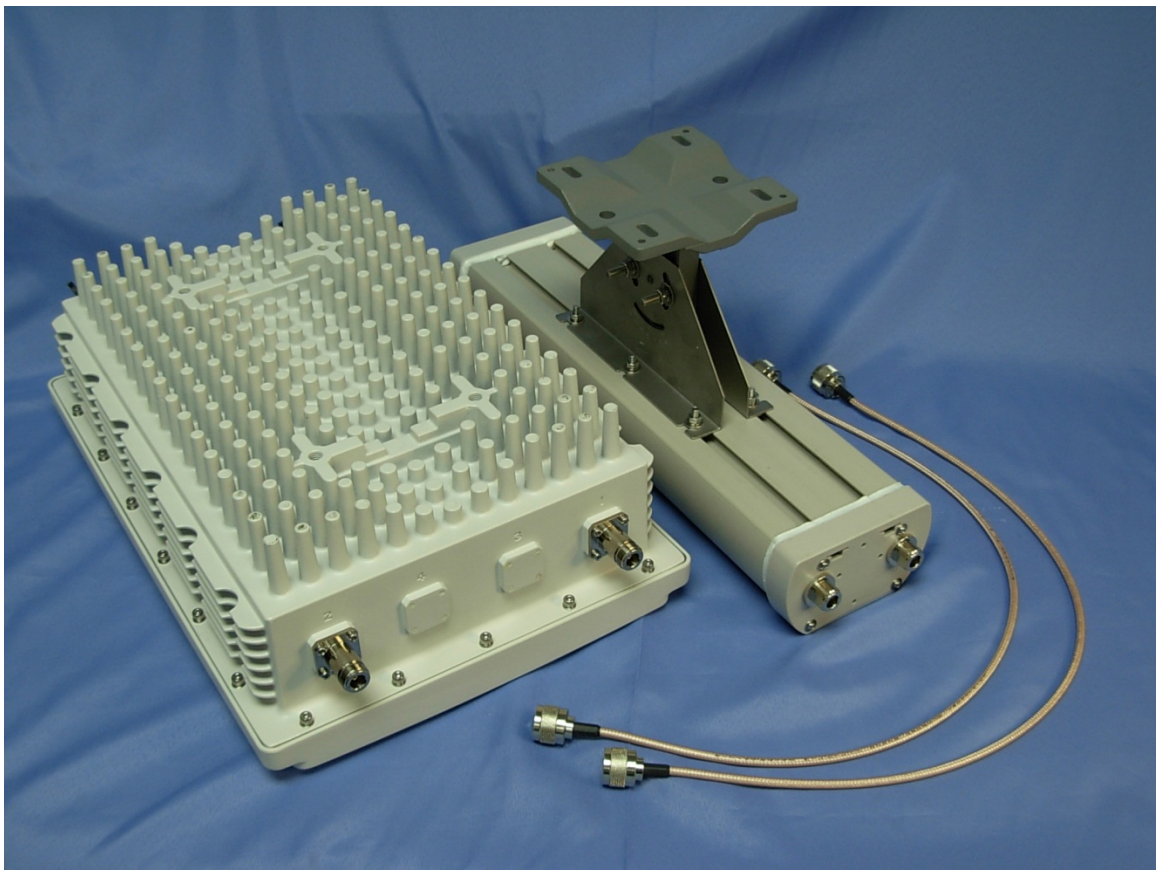


Figure 2: BSMax-250 and antenna, back view

1.2 PRODUCT SPECIFICATION

Table below is a list of hardware specifications of the base station.

System Standard	IEEE 802.16e
RF band	2497.75~2688.25MHz
Channel sizes	3.5, 5,7 and 10MHz (512 and 1024 FFT size for OFDMA signal)
Duplexing	TDD
Transmit power	Up to 32dbm
RF Dynamic range	Tx > 20db, Rx > 70db
Transmit power accuracy	Within +/- 1db
Frame length	5ms
MIMO support	2 Tx, 2Rx
Multiple antenna support	UL MRC, UL Matrix A, DL Matrix A/B
Certification compliance	*being applied*
Power surge protection	>4KV
Power supply	Via -48VDC Power-over-Ethernet or

	standalone -48VDC
Waterproof	IP 65
Operating temperature	-40 to +55 degree Celcius
Operating humidity	0 to 95% (non-condensing)

Table 1: Base station specification

1.3 CONNECTORS

There are 2 antenna connectors (N-type male) used to connect to antenna(s) on the top of the base station: Connector 1 to MIMO antenna 1 or SISO antenna; Connector 2 to MIMO antenna 2 or RF termination. The RF termination needs to have at least 2W RF power tolerance in the frequency range of operation (3400-3800MHz).

For the bottom of the base station, left to right, the connectors/indicators are (as shown in figure 1):

- Ethernet input (Power of Ethernet) with cover
- LED status indicator
- 1PPS signal input (TNC connector) with cover
- -48VDC input with cover

The label showing product model, serial number and MAC address is also placed on the bottom of the base station.

1.4 INSTALLING BASE STATION

The following steps are to be followed when installing the base station.

Step 1. Fasten base station unit on to the pole with mounting brackets and wing bolts(screws, washers and nuts), as shown in figure below.

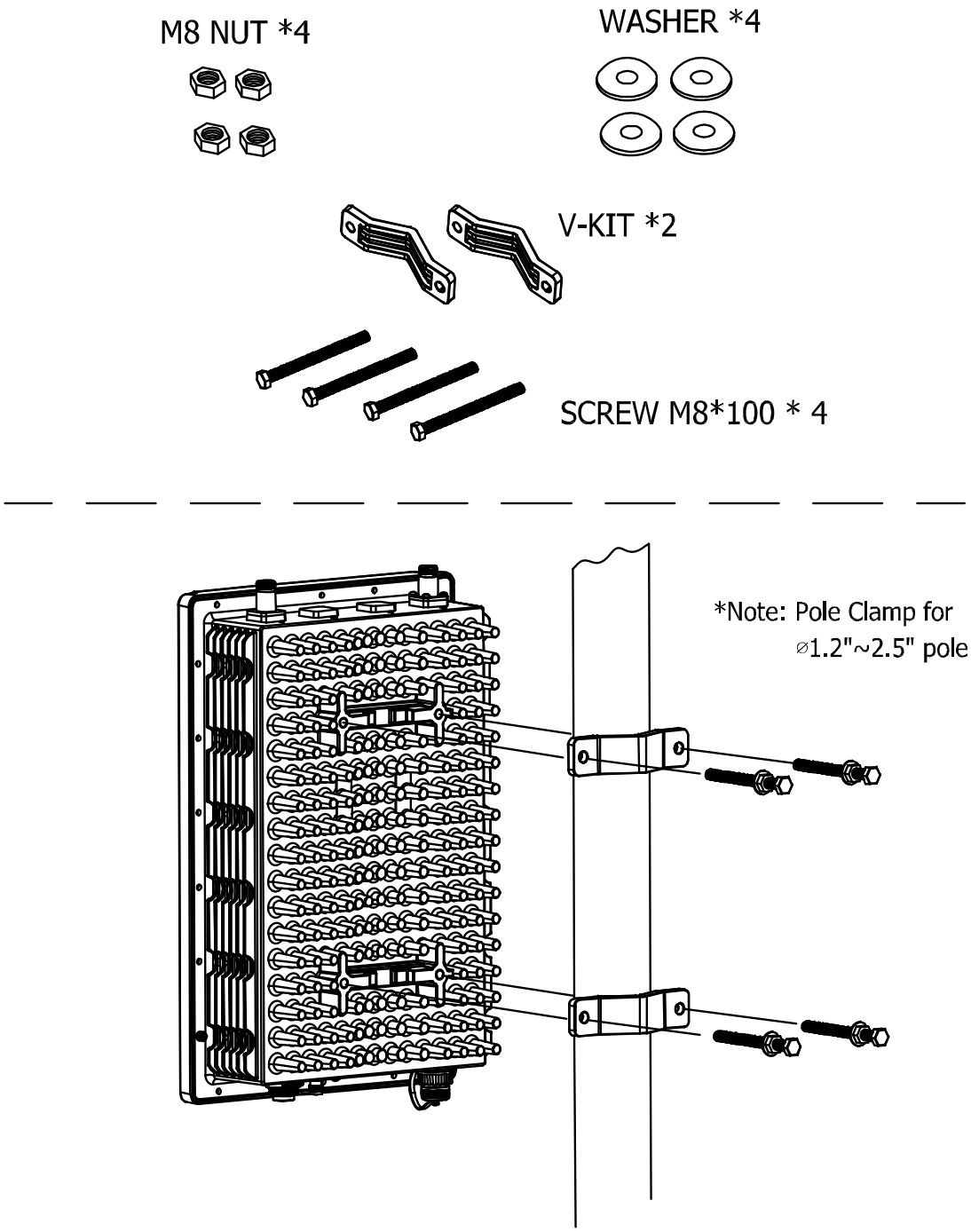


Figure 3: Install base station on pole

Step 2. Install antennas and connect RF coaxial cable to base station, as shown in figure below. The RF coaxial cable needs to be as short as possible to minimize loss.

Step 3. Install weather-proof CAT-5e cable to Ethernet port of base station, as shown in figure below.

Step 4. Install weather-proof TNC cable between GPS port of base station and GPS receiver (optional), as shown in figure below.

Step 5. Install grounding cable to “TO GND” port of base station, as shown in figure below.

Step 6. Install weather-proof power cable to “DC 48V IN” port of base station, as shown in figure below.

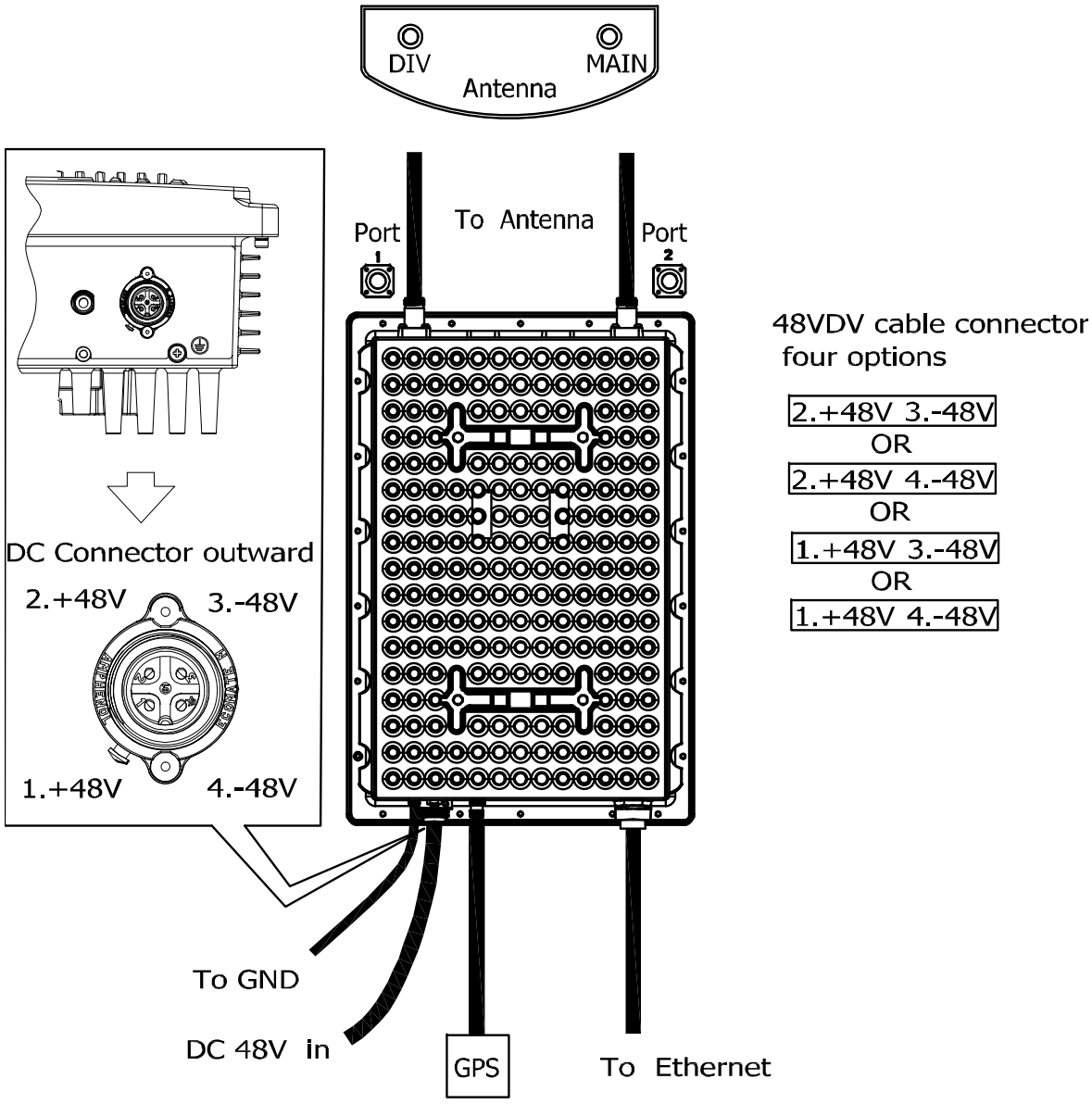


Figure 4: Connecting antennas

Step 7. Sealing connectors, wrapping RF ports of base station and antenna by rubber splicing tape, as shown in figure below.

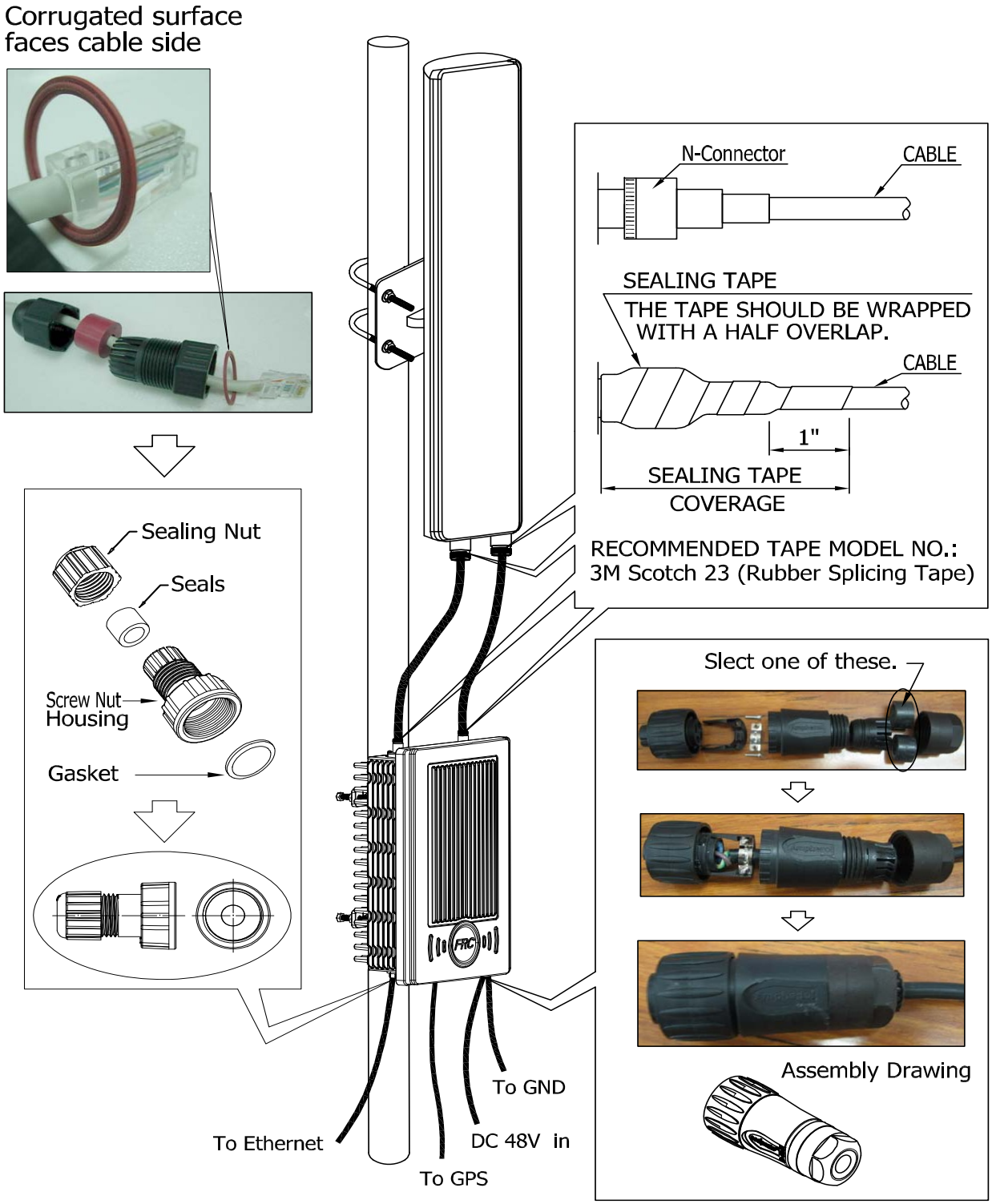
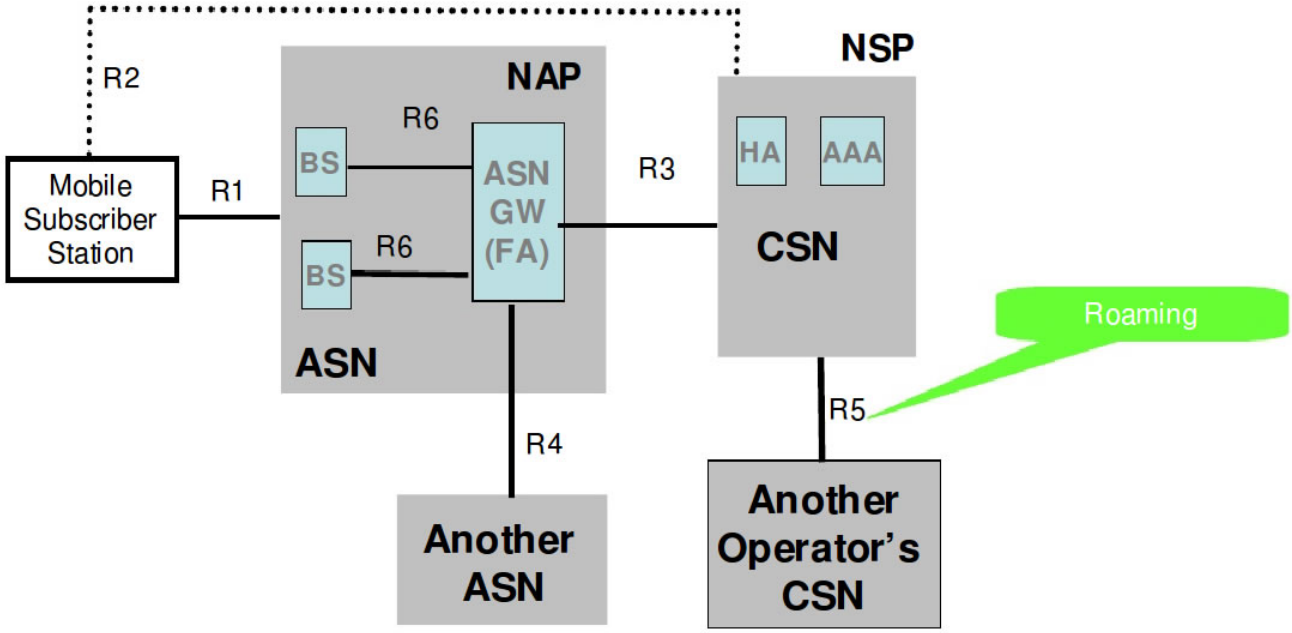


Figure 5: Sealing connectors and RF cables

1.5 NETWORK ARCHITECTURE

The WiMAX network structure involving base station can be explained in the figure below.



ASN – Access Services Network
CSN – Core Services Network
BS – Base Station
FA – Foreign Agent
NAP – Network Access Provider
NSP – Network Service Provider
HA – Home Agent
AAA – Authentication, Authorization, & Accounting

The reference points (R1-R6) as seen in figure are conceptual links that connects two functional entities. The reference points are:

R1: Reference point between SS and BS: implements IEEE 802.16e-2005.

R2: Reference point between MS and ASN-GW or CSN: logical interface used for authentication, authorization, IP host configuration and mobility management.

R3: Reference point between ASN and CSN: supports AAA, policy enforcement, and mobility –management capabilities. Implements tunnel between ASN and CSN.

R4: Reference point between ASN and ASN: used for MS mobility across ASNs.

R5: Reference point between CSN and CSN: used for internetworking between home and visited network.

R6: Reference point between BS and ASN: implements intra-ASN tunnels and used for control plane signaling.

2. CONFIGURATION ACCESS

2.1 CONFIGURATION PARAMETERS

The basic configuration parameters, categorized into logical groups according to the system functionality are listed below.

FTP Parameters

This set of parameters is used when the system is trying to boot from the network upon failure to load from the primary and secondary images on flash as well as to perform software upgrades.

- FTP Host IP address: The IP address of the server which contains the firmware upgrades.
- User name: The user name by which the system can access the FTP server.
- Password: The password by which the user specified by the user name can access the FTP server.

SW Upgrade Parameters

This set of parameters is used to control the SUH operation.

- File path: The path on which the firmware upgrades exist.
- Filename: The name of the firmware package and its extension.
- Auto-upgrade time: The interval between auto-upgrades.
- Auto-upgrade enabled flag: Indicates whether the auto-upgrade feature is enabled or not.

Network Parameters

This set of parameters is used to configure the target network settings in order to be able to access the network.

- BS IP address: The IP address of the Ethernet interface through which the BS communicates with the network for FTP upgrades, TFTP configurations download and booting from network image upon failure.
- BS Subnet mask: The subnet mask associated with the IP address.
- BS Default Gateway: The gateway IP address through which the BS can communicate with external networks.
- System log IP server: The IP address of the log server to which the BS sends its logs.

- DHCP Server for SU: The IP address of the DHCP server which assigns the IP addresses to SUs associated with the BS.

Administration Parameters

This set of parameters is used for administrative purposes.

- Sector Name: The name of the sector represented by this instance of BS.
- Sector ID: The identifier of the sector
- Sector Location: A descriptive name of the location where the BS exists.
- Network Name: The name of the owner of the network to which this BS belongs.
- Cell Name: The name of the cell covered by this BS sector
- Admin system name: The name of the administrator of this BS
- Admin system contact: The contact information of the admin
- Admin system location: The location of the admin
- System log enabled flag: This indicates whether sending logs to the log server is enabled or not.

Credentials Parameters

This set of parameters is used to provide secure access to the system through the different interfaces supported by the system.

- CLI user name: The user name used to access the CLI remotely through telnet.
- CLI password: The password used by the CLI user name to remotely access the CLI through telnet.
- Web user name: The user name used to access the web interface.
- Web password: The password used by the web user to access the web interface.
- Read Community: The community string which allows network management systems to retrieve MIB values from the BS.
- Write Community: The community string which allows network management systems to set MIB values to the BS.

Operating Parameters

This set of parameters is used by the system to configure the MAC operating parameters.

- Uplink frequency: The frequency used in the uplink
- Downlink frequency: The frequency used in the downlink
- Uplink modulation: The modulation and FEC used for the first uplink burst profile. (UIUC-1)
- Downlink modulation: The modulation and FEC used for the first downlink burst profile (DIUC-1)
- TDD split: The time division duplexing ratio between the downlink and uplink.
- Bandwidth: The channel bandwidth.

2.2 Factory Default Parameter Values

For the parameters listed in the previous section, the factory default values are:

Id	Configuration Parameter name	Description	Value
1	*ftpHostIpAddr*	IP address of the server containing the SW version to be dowloaded	192.168.0.10
2	*userName*	User name required to access the server	frcwimax
3	*Passwd*	Password required to access the server	frcwimax
4	*filePath*	The complete path to the SW images	samba
5	*Filename*	Name of the SW image with the extension but without the version	FRC_WIMAX_BS_.Z
6	*isAutoUpgradeEnabled*	Set to TRUE to automatically upgrade the SW	TRUE
7	*autoUpgradeTime*	Periodicity of automatic upgrade (in seconds)	86400
8	*BsIpAddr*	IP address of the Base Station	192.168.0.20
9	*BsSubnetMask*	Subnet Mask of the Base Station	255.255.255.0
10	*BsDefaultGateway*	Default Gateway of the Base Station	192.168.0.1
11	*readCommunity*	The community string used for Get Requests	public
12	*writeCommunity*	The community string used for Set Requests	private
13	*sysLogIpAddress*	IP address of the system log server	192.168.0.10
14	*sectorName*	Descriptive name of the Sector	CBS_S1
15	*sectored*	A unique identifier of the sector ranging from 1~6	1
16	*sectorLocation*	Descriptive location	WiMAXCity
17	*dhcpServerForSu*	IP address of the DHCP server for SU	192.168.0.10
18	*AdminSysName*	Name of the administrator of the system	AB-FRC
19	*AdminSysContact*	Administrator Contact	frc@frccorp.com
20	*AdminSysLocation*	Location	WiMAXCity
21	*networkName*	Name of the network owner	FRC
22	*cellName*	Name of the cell	Cell-1
23	*cliUserName*	The user name used to access the CLI through telnet	frccli
24	*cliPassword*	The password used to access the CLI through telnet	frccli2009
25	*webUserName*	The user name used to access the web interface	frcweb
26	*webPassword*	The password used to access the web interface	frcweb2009
27	*isSysLogEnabled*	Enables and disables sending logs to the log server.	FALSE
28	*ulFrequency*	UL central frequency in Hz	255000

29	*dlFequency*	DL central frequency in Hz	255000
30	*ulModulation*	The first uplink burst profile (modulation and FEC scheme)	qam64-cc-3/4
31	*dlModulation*	The first downlink burst profile (modulation and FEC scheme)	qam64-cc-3/4
32	*Bandwidth*	The channel bandwidth	10
33	*tddSplit*	The time division duplexing split	75
34	*r6bsaddr2*	R6 BS address 2	192.168.0.20
35	*r6gwaddr=10.1.3.1*	R6 gateway address	10.1.3.1
36	*r6gwaddr2=10.1.3.1*	R6 gateway address 2	10.1.3.1
37	*r6bsport*	R6 BS port	2231
38	*r6gwport=2231*	R6 gateway port	2231
39	*r6dataportnexthopmacaddr*	R6 data port next hop MAC address	00:1c:ae:6f:3f:21
40	*NAI*	NAI	@thebluezone.com
41	*authmode*	Authentication mode	1
42	*suppworkaround*	Supplicant workaround	0

2.3 WEB ACCESS

The base station's software configuration can be accessed via web browser through HTTP protocol. The following options can be configured:

- Current settings and status query
- Configuring parameters of MAC and PHY layers
- Network setting changes
- Security setup
- Base station access credentials
- Configuration settings backup
- Default settings reset
- Firmware updates

To log in to the web interface:

- Set host computer (the computer that controls/configures the base station) connected to the base station via Ethernet (power over Ethernet) and host computer's IP address configured to an address within the same *BsSubnetMask* of *BsIpAddr*.

- Enter http://*192.168.0.20* in the web browser and the following log in page will be displayed:

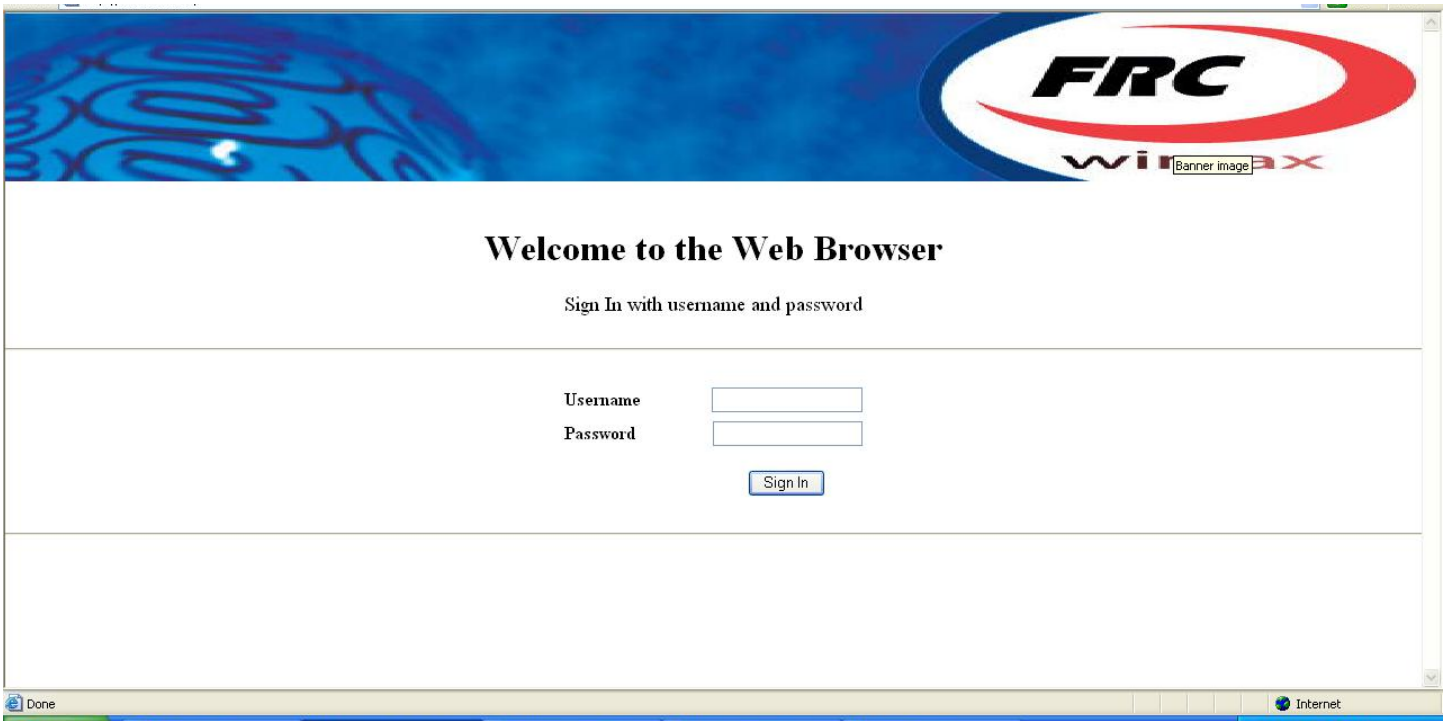


Figure 6: Web log in

In the username and password field, enter *frcweb* and *frcweb2009* respectively. Click on "sign in" button to log into the administration page, shown in figure below.

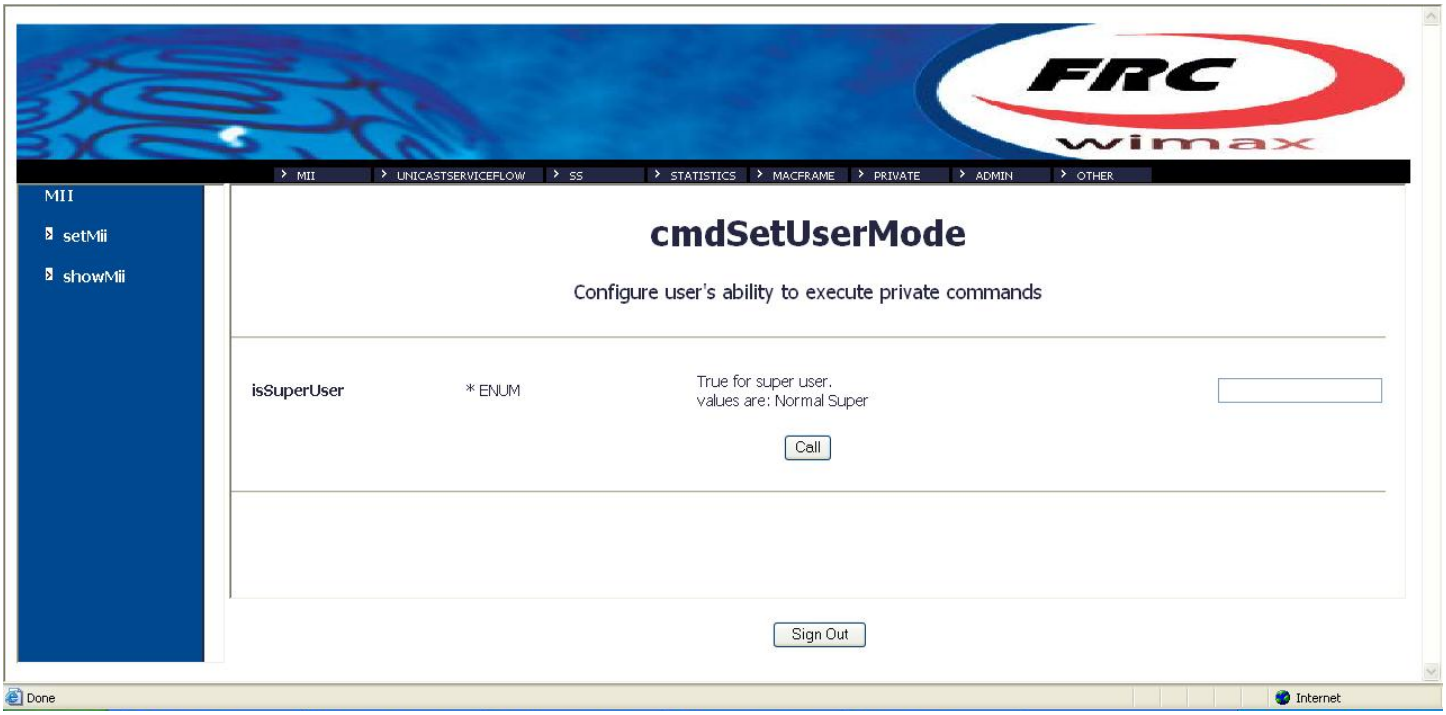


Figure 7: Web administration

The administration interface is categorized into 8 groups: MII, Unicast service flow, SS, Statistics, Mac frame, Private, Admin and other, listed on the top frame of the page. After clicking on a certain group, the commands available will be listed in the left frame of the page.

For each command, once clicked, the execution page including command name, description, argument name, argument type, and possible argument values will be displayed in the main frame of the page. To execute a certain command, fill in the arguments that need to be changed in the field to the right, then click on "call" button.

To log out from web interface, click on "sign out" button in the bottom frame.

The detailed information of each command can be found in chapter 3 of this document.

2.4 CLI ACCESS

Software configuration command prompt interface can be accessed through Telnet. To access:

- Set host computer connected to the base station via Ethernet and host computer's IP address configured to an address within the same *BsSubnetMask* of *BsIpAddr*.

- Telnet connection can be established to base station's default IP address: telnet *192.168.0.20*.

- Enter the log in credential: *frccli* and *frccli2009*.

Software configuration prompt is entered once telnet connection is established.

The following table lists the basic commands of the base station command prompt; the syntax will follow VxWorks 6.6 (the operating system of the base station):

Command name	function
cd "<dir>"	Change active directory to *<dir>*. E.g. *cd "host:"* enters the root directory of the FTP server; *cd "/tffs/"* enters the root directory of the on board flash
ls "<dir>" or *ll "<dir>"*	List the content of *<dir>*
cbe "<command>"	Execute *<command>.* Some commands do not require arguments, whereas some commands may require arguments to be input. To understand what arguments are supported in a configuration type command, *use cbe "help <command_name>"*. For the commands with arguments, the format to use will be *cbe "<command> <argument1>=<value1> <argument2>=<value2> … ".*
pwd	Show the current working directory
< <script_path_name>	Execute script *<script_path_name>*
cp "<source_path_file>" "<destination_path_file>"	Copy file
rm "<path_file>"	remove file
ping "<address>"	ICMP ping *<address>*
reboot	reboots the base station

Table 2: CLI command syntax

cbe commands have the same functionality of the commands of web interface described in previous section. For detailed explanation of the commands, please refer to Chapter 3 of this document.

3. CONFIGURATION COMMANDS

The details of the configuration commands mentioned in web and CLI access are explained in this chapter.

3.1 ADMIN COMMANDS

loadImage

loadImage		
Arguments	image	Represents which image will be loaded. Possible values are: **primary** : loads the primary image **secondary**: loads the secondary image **network**: loads image from network
Description	Load the base station software image.	

Output	Loading primary image... OR Loading secondary image... OR Loading image from network...
Output Description	The messages indicate which image is being loaded.
Example	loadImage primary loadImage secondary loadImage network
Error Messages	Mandatory Field is missing Invalid Image type. Possible values : primary, secondary, network

showSwVersions

showSwVersions		
Arguments	image	Represents which image will be loaded. Possible values are: **primary** : loads the primary image **secondary**: loads the secondary image
Description	Get the version of specified primary, secondary or both images software.	
Output	Primary image version is: <version> OR Secondary image version is: <version> OR The two messages together if user didn't specify image type	
Output Description	The messages indicate the specified image version and if user didn't specify image type it will indicates the primary and secondary images versions.	
Example	showSwVersions showSwVersions primary showSwVersions secondary	
Error Messages	Invalid Image type. Possible values : primary, secondary Failed to get primary image version Failed to get secondary image version primary image version is corrupted the default will be used secondary image version is corrupted the default will be used	

setOperatingParameters

setOperatingParameters		
Arguments	ulFrequency	The uplink frequency.
	dlFrequency	The downlink frequency
	bandwidth	The BS bandwidth. Possible values for bandwidth are: **3MHz 3.5MHz 4.375MHz 5MHz 6MHz 7MHz 8.75MHz 10MHz**
	ulModulation	The uplink modulation type. Possible values for modulation: **qpsk-cc-1/2 qpsk-cc-3/4 qam16-cc-1/2 qam16-cc-3/4 qam64-cc-1/2 qam64-cc-2/3 qam64-cc-3/4 qpsk-ctc-1/2 qpsk-ctc-3/4 qam16-ctc-1/2 qam16-ctc-3/4 qam64-ctc-1/2 qam64-ctc-2/3 qam64-ctc-3/4 qam64-ctc-5/6 none**

	dlModulation	The downlink modulation type.
	tddsplit	Time division duplexing split
	operatingImage	Represents which image will be loaded. Possible values are : **primary**, **secondary**, **network**
	save	Save operating parameters to configuration file
Description	Set one or more of the operating parameters and also give the option to save them to flash	
Output	**If user specifies save as 1:** Operating Parameters has been saved successfully The changes you have made will take effect after reboot. You can use loadImage command to reboot. **If user didn't specify save or specifies it as 0:** Operating Parameters has been updated successfully The changes you have made will take effect after saving and reboot You can use this command to save and loadImage command to reboot	
Output Description	None	
Example	setOperatingParameters ulModulation=qam64-ctc-3/4 tddsplit=15 dlFrequency=250000 save=1 setOperatingParameters bandwidth=3MHz If all the configuration values are to be specified then no need to write the parameter name but they must be entered in order.	
Error Messages	Please enter at least one value Invalid UL Frequency value value. UL Frequency should have value in range <Min value> -> <Max value> only. Invalid UL Frequency value value. UL Frequency should have value in range <Min value> -> <Max value> only. Invalid bandwidth value. Possible Values: 3MHz, 3.5MHz, 4.375MHz, 5MHz, 6MHz, 7MHz, 8.75MHz, 10MHz. Invalid TDDSPLIT value. TDDSPLIT should have values 53->75 only. Invalid UL Modulation value. Possible Values: qpsk-cc-1/2 qpsk-cc-3/4 qam16-cc-1/2 qam16-cc-3/4 qam64-cc-1/2 qam64-cc-2/3 qam64-cc-3/4 qpsk-ctc-1/2 qpsk-ctc-3/4 qam16-ctc-1/2 qam16-ctc-3/4 qam64-ctc-1/2 qam64-ctc-2/3 qam64-ctc-3/4 qam64-ctc-5/6 none Invalid UL Modulation value. Possible Values: qpsk-cc-1/2 qpsk-cc-3/4 qam16-cc-1/2 qam16-cc-3/4 qam64-cc-1/2 qam64-cc-2/3 qam64-cc-3/4 qpsk-ctc-1/2 qpsk-ctc-3/4 qam16-ctc-1/2 qam16-ctc-3/4 qam64-ctc-1/2 qam64-ctc-2/3 qam64-ctc-3/4 qam64-ctc-5/6 none The type of operating image. Possible Values: primary, secondary, network Failed to save operating parameters values to flash	

setTFTPAddress

setTFTPAddress		
Arguments	ipAddress	Represents the IP address of the TFTP server
	configFilePath	Represents the configuration file full path
	removeAndReboot	Represents whether to remove the existing configuration file and reboot the system to get it

		again from TFTP server or not.
Description	Set the TFTP IP address and Configuration file path and also give the option to remove the existing file and reboot the system.	
Output	TFTP Host IP Address has been set successfully Configuration File Path has been set successfully The System will now remove the configuration file and reboot	
Output Description	The message indicates the status of set operation of specified parameters and if system will reboot.	
Example	setTFTPAddress ipAddress=192.168.0.10 removeAndReboot=1 setTFTPAddress configFilePath= 00_26_19/2E/bsconfig.conf	
Error Messages	Invalid TFTP IP address format. IPv4 format is x.x.x.x Please enter at least one argument.	

upgradeSw

upgradeSw		
Arguments	image	Represents which image will be upgraded. Possible values are: **primary:** upgrades the primary image **secondary :** upgrades the secondary image
	version	String representing the version which is used in the upgrade. The version consists of the major.minor.revision Ex: v1.0.7
	hostIP	The IP address of the FTP server on which upgraded software is placed. If hostIP is not specified, the default host IP configured in the BS is used.
	path	The full path to the software image on the FTP server. If path is not specified, the default path configured in the BS is used.
	username	The user name to login to the FTP server to get the software image. If the user name is not specified the username configured in the BS is used.
	password	The password to login to the FTP server to get the software image. If the user name is not specified the password configured in the BS is used.
	reboot	Specify whether to make reboot for system or not.
Description	Upgrade the SW on the BS.	
Output	Performing software upgrade to Version = x.x.x **If user didn't specify reboot option or specified it as 0** "Software upgrade succeeded. The updates will take effect after reboot. You can use loadImage command to reboot" message will be displayed. **If user specified reboot option as 1** " Software upgrade succeeded. System	

	will reboot now" message will be displayed.
Output Description	System indicates that upgrade is being performed with the specified version.
Example	upgradeSw primary v1.0.15 upgradeSw secondary v2.171.0 169.15.171.1 upgrades/rev1
Error Messages	Version is a mandatory field Invalid IP address format. IPv4 format is x.x.x.x No Software Upgrade can be performed now; system init is not yet completed. No Software Upgrade can be performed now; another upgrade instance is in progress. Please try again later. Software Upgrade failed Failed to Upgrade Software. Failed to log in to FTP. Failed to Upgrade Software. FTP transfer incomplete. Failed to Upgrade Software. Flash Error occurred. Failed to Upgrade Software. File read error. Failed to Upgrade Software. Invalid version format. Failed to Upgrade Software. Incomplete HW version. Failed to Upgrade Software. Incomplete SW version. Failed to Upgrade Software. Invalid Image Type. Failed to Upgrade Software. Failed to allocate memory. Failed to Upgrade Software. Invalid package length. Failed to Upgrade Software. Image size is too big. No Software Upgrade can be performed now; another upgrade instance is in progress. Please try again later. Failed to Upgrade Software. Invalid SW Upgrade State. Failed to Upgrade Software.

showSystemConfiguration

showSystemConfiguration		
Arguments	displayType	Represents which category to be displayed. Possible values are: **general:** displays the configuration parameters in the General category. **account:** displays the configuration parameters in the Account category. **snmp:** displays the configuration parameters in the SNMP category. **sysLog:** displays the configuration parameters in the SysLog category. **files:** displays the configuration parameters in the Files Names category. **upgrade:** displays the configuration parameters in the Upgrade category. **sector:** displays the configuration parameters in the Sector category. **admin:** displays the configuration parameters in the Administrator Information category.

		operatingParams: displays the operating parameters of the system. **all :** upgrades the primary image
Description	Displays the system configurations.	
Output	BS SYSTEM CONFIGURATION General BS IP Address BS Subnet Mask BS MAC Address BS Default Gateway Network Name TFTP Host IP Address FTP Host IP Address DHCP Server IP Address Account User Name Password SNMP Read Community Write Community SysLog SysLog Server IP address Is SysLog Enabled Files Names File Path File Name Configuration File Full Path Upgrade Is Auto Upgrade Enable Auto Upgrade Time in days Sector Sector Name Sector ID Sector/System Location Cell Name Administrator Information System Administrator Name System Administrator Contact System Administrator Location Operating Parameters Uplink Frequency Downlink Frequency Bandwidth Uplink Modulation Downlink Modulation Time Division Duplexing Split Operating Image	
Output Description	The system lists all the values of the configuration parameters categorized into logical groups	

Example	showSystemConfiguration showSystemConfiguration all showSystemConfiguration general showSystemConfiguration operatingParams
Error Messages	Failed to retrieve System Configurations Invalid display type. Possible Values: general, account, snmp, sysLog, files, upgrade, sector, admin, operatingParams, all.

setSystemConfiguration

setSystemConfiguration		
Arguments	bsIp	The BS IP address
	subnetMask	The BS Subnet mask
	defaultGateWay	The BS default gateway
	fTPHostIp	IP address of the FTP host
	dHCPServerIp	IP address of the DHCP server
	networkName	The name of the network
	userName	User name used for FTP access
	password	Password used for FTP access
	cliUserName	User name used for CLI authentication
	cliPassword	Password used for CLI authentication
	webUserName	User name used for Web authentication
	webPassword	Password used for Web authentication
	readCommunity	SNMP Requests' Read Community
	writeCommunity	SNMP Requests' Write Community
	sysLogServerIp	IP Address of the SysLog Server
	isSysLogEnabled	Specify whether the System logs enabled or not
	filePath	Full path to the upgrade software directory on FTP
	fileName	Filename of the BS software
	autoUpgrade	Specify if the Auto Upgrade is enabled
	autoUpgradeTime	The Auto Upgrade Time in Days
	sectorId	The Sector ID
	cellName	The Cell Name
	adminName	The System Administrator Name
	adminContact	The System Administrator Contact
	adminLocation	The System Administrator Location
	save	Save configurations to configuration file
Description	Set one or more of the system configurations and also give the option to save these configurations to flash.	
Output	Configurations updated successfully	
Output Description	None	
Example	setSystemConfiguration cellName=Cell1 If all the configuration values are to be specified then no need to write the parameter name but they must be entered in order.	
Error Messages	Invalid BS IP address format.IPv4 format is x.x.x.x Invalid subnet mask address format.IPv4 format is x.x.x.x Invalid BS default Gateway address format.IPv4 format is x.x.x.x	

	Invalid DHCP Server IP address format.IPv4 format is x.x.x.x Invalid SysLog IP address format.IPv4 format is x.x.x.x Invalid FTP Host IP address format.IPv4 format is x.x.x.x Please enter at least one value. Invalid Sector ID value. Sector ID should have values 1->6 only CLI User Name and Password Must be set together Web User Name and Password Must be set together Failed to Set FTP Host IP Failed to set Is SysLog enabled. Failed to Set User Name Failed to Set Password Failed to set CLI User Name and Password Failed to set WEB User Name and Password Failed to Set Software File Path Failed to Set Software File Name Failed to save network parameters values to flash. Failed to save configuration values to flash.

getMIB

getMIB		
Arguments	module	The module of the MIB variable
	name	The Name of the MIB variable
	index1	Key to get the specified MIB from a table
	index2	Key to get the specified MIB from a table
	index3	Key to get the specified MIB from a table
	index4	Key to get the specified MIB from a table
	index5	Key to get the specified MIB from a table
	oid	The object identifier of the MIB variable. The OID value should contain the required indices of the table for accessing a specific entry in a table.
Description	Get the value of the specified MIB. If the MIB module is specified, a MIB name should also be specified; otherwise the MIB OID should be specified. If the index is a MAC address it should be entered in a dotted decimal format.	
Output	The Value of <oid> is: <value>	
Output Description	The output specifies the value of the MIB specified by the OID.	
Example	getMIB oid = 1.0.8802.16.2.1.3.1.1.3 getMIB module = WMAN-DEV-MIB name = wmanDevBsCurrentSwVersion index1 = 1	
Error Messages	You must enter MIB module and name or object ID. Wrong module or MIB name. You should enter 1 key(s) to get wmanDevBsCurrentSwVersion MIB variable. Invalid Object ID Failed to get MIB value. No such object. No such instance.	

	End of MIB. Unknown data type. Value = <type>

setMIB

setMIB		
Arguments	module	The module of the MIB variable
	name	The Name of the MIB variable
	index1	Key to get the specified MIB from a table
	index2	Key to get the specified MIB from a table
	index3	Key to get the specified MIB from a table
	index4	Key to get the specified MIB from a table
	index5	Key to get the specified MIB from a table
	oid	The object identifier of the MIB variable
	type	The type of the assigned MIB value. Possible values are: **i :** integer value **c:** counter value **g:** gauge value **a:** IP address value **s:** String value **t:** Time Ticks value **h:** hex value representing a bitmap
	value	The value assigned to the MIB
Description	Set the value of specific MIB. If the MIB module is specified, a MIB name should also be specified; otherwise the MIB full OID should be specified. If the index is a MAC address it should be entered in a dotted decimal format. For hexadecimal format, two digits should be entered for each byte, i.e. a value of 0 in a byte must be entered as 00.	
Output	MIB Value has been Set Successfully	
Output Description	"MIB Value has been Set Successfully" is displayed when the system succeeded to set the MIB value	
Example	setMIB oid=1.0.8802.16.2.1.3.1.1.1 type=i value=5 setMIB module = WMAN-IF2F-BS-MIB name = wmanIf2fBsSfDirection index1 = 1 index2 = 0.1.2.3.4.5 index3 = 2 type=i value=5 setMIB oid=1.0.8802.16.2.1.3.1.1.1 type=h value=01A437BC00	
Error Messages	You must enter MIB module and name or object ID. Wrong module or MIB name. You should enter 3 key(s) to set wmanIf2fBsSfDirection MIB variable. Invalid Object ID Failed to set MIB value	

getNextMIB

getNextMIB		
Arguments	module	The module of the MIB variable

	name	The Name of the MIB variable
	index1	Key to get the specified MIB from a table
	index2	Key to get the specified MIB from a table
	index3	Key to get the specified MIB from a table
	index4	Key to get the specified MIB from a table
	index5	Key to get the specified MIB from a table
	oid	The object identifier of the MIB variable
Description	Get the value of the MIB after the specified one. If the MIB module is specified, a MIB name should also be specified; otherwise the MIB OID should be specified. If the index is a MAC address it should be entered in a dotted decimal format.	
Output	The Value of <oid> is: <value>	
Output Description	Displays the OID next to the specified OID along with its value.	
Example	getNextMIB oid=1.0.8802.16.2.1.3.1.1.3 getNextMIB module = WMAN-DEV-MIB name = wmanDevBsCurrentSwVersion index1 = 1	
Error Messages	You must enter MIB module and name or object ID. Wrong module or MIB name. You should enter 1 key(s) to get wmanDevBsCurrentSwVersion MIB variable. Invalid Object ID Failed to get MIB value No such object. No such instance. End of MIB. Unknown data type. Value = <type>	

getBulk

getBulk		
Arguments	module	The module of the MIB variable
	name	The Name of the MIB variable
	index1	Key to get the specified MIB from a table
	index2	Key to get the specified MIB from a table
	index3	Key to get the specified MIB from a table
	index4	Key to get the specified MIB from a table
	index5	Key to get the specified MIB from a table
	oid	The object identifier of the MIB variable
	maxRepetitions	The max repetition value in the get bulk request
Description	Gets a bulk of MIBs starting at the specified OID.	
Output	The Value of <type> <oid> is: <value>	
Output Description	Displays all the MIBs starting from the specified OID until the maximum number of MIBs has been reached.	
Example	getBulk oid=1.0.8802.16.2.1.3.1.1 maxRepetitions= 15 getBulk module = WMAN-DEV-MIB name = wmanDevBsCurrentSwVersion index1 = 1 maxRepetitions = 10	
Error Messages	You must enter MIB module and name or object ID.	

	Wrong module or MIB name. You should enter 1 key(s) to get wmanDevBsCurrentSwVersion MIB variable. Invalid Object ID Failed to get MIB value. No such object. No such instance. End of MIB. Unknown data type. Value = <type>

4. FILES AND ENVIRONMENT

The lists of files required for correct operation of the BS are listed below categorized by the location in which they are saved.

Files on flash (*ls "/tffs/"*)

*/tffs/***vxWorks1.Z** – The OS image considered as the primary image.

*/tffs/***appb1.Z.out** – The BS application image considered as the primary BS application.

*/tffs/***primary.sh** – The startup script that is run after the primary OS image loading to load the primary BS application. The startup script should contain the correct path of the primary application.

*/tffs/***vxWorks2.Z** – The OS image considered as the secondary image.

*/tffs/***appb2.Z.out** – The BS application image considered as the secondary BS application.

*/tffs/***secondary.sh** – The startup script that is run after the secondary OS image loading to load the secondary BS application. The startup script should contain the correct path of the secondary application.

*/tffs/***bsconfig.conf** – The configuration file downloaded by the BS from the TFTP server.

The file path and name of the upgrade software are specified in the configuration file **bsconfig.conf** and can be modified through the CLI commands.

Files on Network Server

*samba/***vxWorks.Z** – The OS image placed on the network server.

*samba/***appb.Z.out** – The BS application image on the network server.

*samba/***net.sh** – The startup script that is run after the OS image loading to load the BS application. The startup script should contain the correct path of the application.

5. UPGRADING FIRMWARE

The following parameters should be set correctly in the BS configurations either in the configuration file or in the runtime configurations using CLI commands or specified in the upgradeSw command:

- FTP Server IP address
- FTP user name
- FTP password
- File path
- File name

Upgrade files are to be placed in FTP server, as described in previous chapter.

If any of the configuration parameters are not correct, the system will use the default values for configurations. If the system can't find a newer version or fails to find the specified version the system will keep running with the old SW version.

The minimum auto-upgrade time that can be configured is 3 minutes, if the configuration file contains a value less than 3 minutes, the system will ignore the value specified and wait for 3 minutes before autoupgrade.

6. MIB TABLE CONFIGURATION WITH MG-SOFT

This chapter explains how to configure MIB tables via SNMP protocol using MG-Soft MIB browser. To obtain MG-SOFT MIB Browser software, refer to http://www.mg-soft.com/download.html.

6.1 ENTERING DATA TO READ-CREATE TABLES

The system supports the following read-create MIB tables:

- wmanIf2fBsProvServiceFlowTable
- wmanIf2fBsProvClassifierRuleTable
- wmanDevCmnSnmpV1V2TrapDestTable

The read-create tables are empty by default and their entries are filled by the NMS. Read-Create tables are controlled by a RowStatus variable which is defined to be the last variable in the entry.

The entry can be in any of the following conceptual states:

- Does not exist – In this state the entry has not been yet created.

- Not ready – In this state one or more of the entry data column variables (except the Row Status) are filled with values using the Set MIB command.
- Not in service – In this state all the entry column variables (except the Row Status) are filled with values using the Set MIB command.
- Active – In this state the entry data is completely filled and the Row Status is set to Active.

The state of the entry is controlled by the values of the RowStatus variable which can take one of the following values:

- Create And Go
- Create And Wait
- Active
- Not In Service
- Destroy

An entry in the table is thus defined by three columns categories:

- Indices Column(s) – This uniquely identifies the entry. The indices columns are defined as not accessible so no values can be entered directly to them.

- Data Columns – Vary from one table to the other depending on the MIB variables maintained by the table and are defined with read write permissions.

- Row Status Column – Indicates the status of the entry and is defined with read-write permissions.

Entry Creation:

1. Creating the entry:

There are 3 ways to create an entry in the table:

- Enter a value in one of the data columns specifying the full qualified OID of the column including the indices values.

- Set the RowStatus column to "Create And Go": To set the RowStatus column to this value, all the data columns should have been filled with appropriate values otherwise the agent will refuse this action. This action will trigger the system to activate the entry, i.e. start using the values entered in the data columns. The entry is conceptually in the “Does not exist” state before this action is triggered and moves to the “Active” state.

- Set the RowStatus column to "Create And Wait": To set the RowStatus column to this value, it is not necessary to fill any of the data columns with appropriate values. The entry is conceptually in the “Does not exist” state before this action is triggered and moves to the “Not Ready” or “Not in Service” states.

2. Setting the values in data columns:

Once the entry exists, i.e the indices are known, the data in the data columns can be entered and modified as desired.

3. Setting the RowStatus column:

- Active: To set the RowStatus column to this value, all the data fields must have been entered.
- Not In Service: This value is set when all the data columns are set but the entry is not yet activated.
- Destroy: Setting the RowStatus to this value will trigger a deletion of the entry. The entry will be in the “Does not exist” state after this action.

Entry Modification after Creation:

There are 2 ways to modify an entry while the entry in the "Active" state:

1. Change the RowStatus to "Not in Service", change all the needed data in the data columns, and then return the RowStatus back to "Active".

This method is used when many data columns need to be changed.

2. Change the value of the date column to the needed value. (Without changing the RowStatus).

This method is used when only one data column needs to be changed.

Dependency among Multiple Tables:

Sometimes there is a dependency among the data stored in multiple tables (for example, the Provisioned service flow data are stored in the wmanIf2fBsProvServiceFlowTable and the wmanIf2fBsProvClassifierRuleTable.

In that case, when the user changes the RowStatus in the wmanIf2fBsProvServiceFlowTable to "Active", all the classifiers in the wmanIf2fBsProvClassifierRuleTable which belongs to the same service flow and with RowStatus "Not in Service" are activated automatically.

As well, when the user changes the RowStatus in the wmanIf2fBsProvServiceFlowTable to "Not in Service", all the classifiers in the wmanIf2fBsProvClassifierRuleTable which belongs to the same service flow and with RowStatus "Active" are automatically changed to "Not in Service".

The following example shows how to set the value of the wmanIf2fBsSfDirection in the wmanIf2fBsProvServiceFlowTable.

The indices of the entry are:

wmanIf2fBsSsProvMacAddress = 00.29.11.23.15.11

wmanIf2fBsSfId = 3

The value to be set is:

wmanIf2fBsSfDirection = 1

1. Expanding the entry.

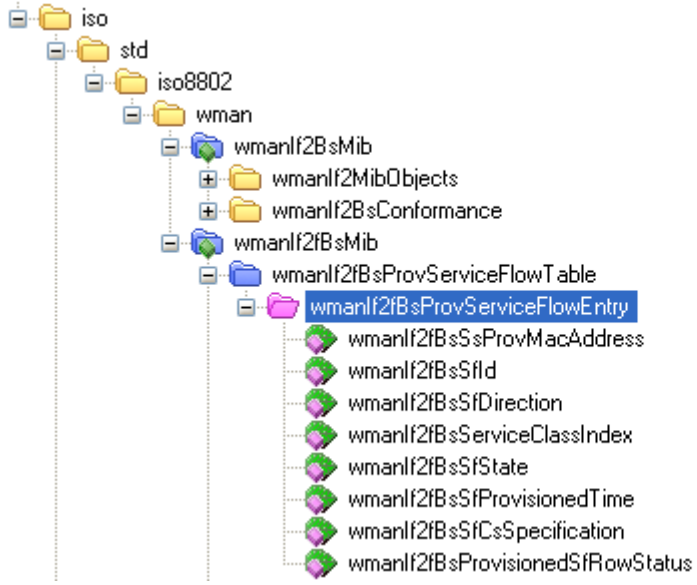


Figure 8: Expanding MIB table entry

2. Setting the first data column.

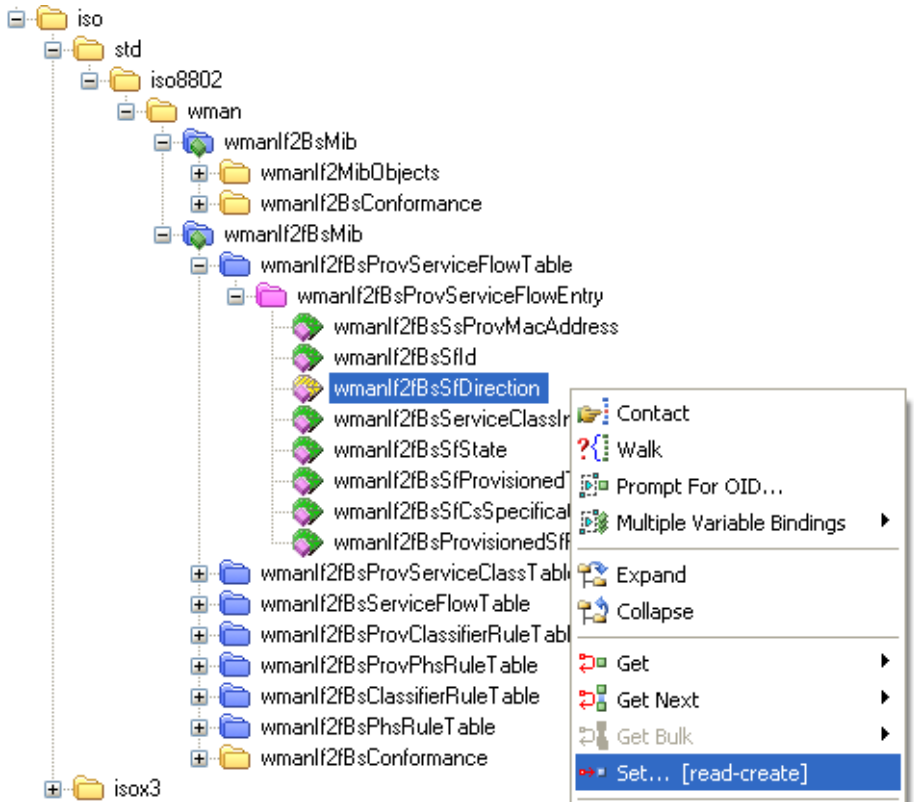


Figure 9: Setting data column

The NMS by default selects the index zero as highlighted in the following figure.

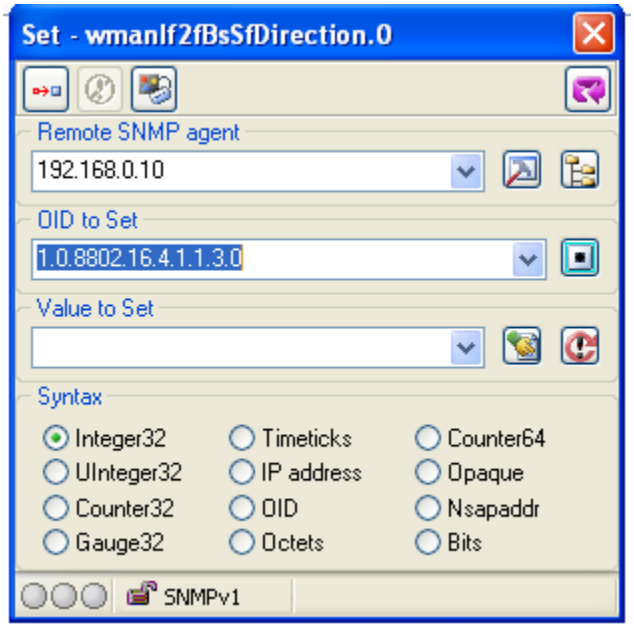


Figure 10: Default index

3. Entering the indices of the entry.

4. Setting the value.

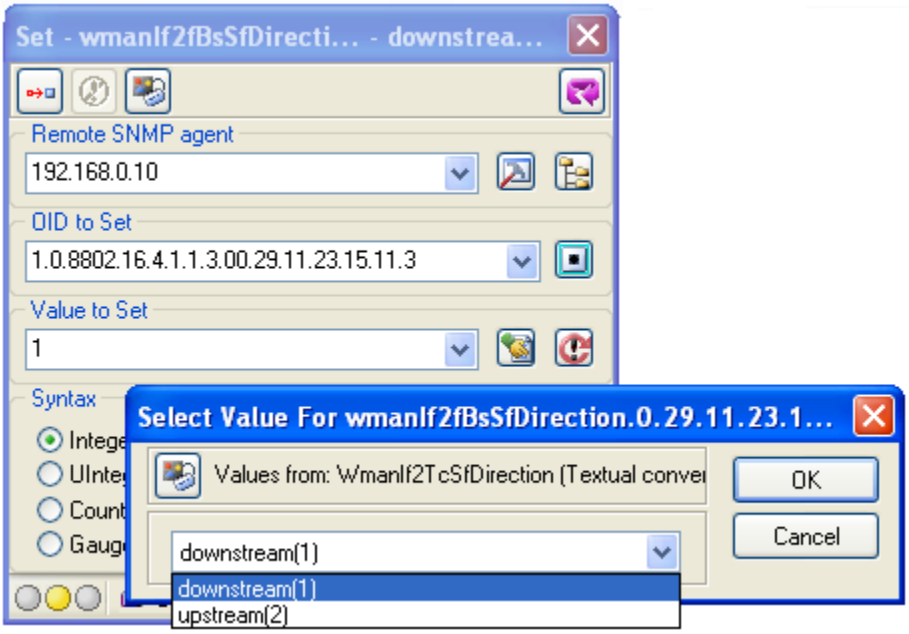


Figure 11: Setting table entry value

Please note that the MG-Soft license expired, so the current supported version is only v1. Data types defined only in v2c of the SNMP standard are not supported anymore. Example of these types is COUNTER64. This type affects the following tables outputs, however when tested from both the CLI and the linux snmp commands, it worked fine.

- wmanBsPriSuStatisticsTable
- wmanBsPriBsSectorLevel
- wmanIf2BsOtaUsageDataRecord
- wmanIf2BsPacketErrorRate

6.2 Filling the wmanBsPriEventLogTable

The wmanBsPriEventLogTable maintains the different events that occur on the BS. The implementation of the event able provides two accessing functions, one to read an event from the table and the other to write an event in the table namely the eventRead and eventWrite functions.

Any entity in the system can use the event table to enter an event in the table using the eventWrite function.

6.3 Saving Private MIBs

The private MIB variables can be saved to flash, by setting the value of the wmanBsPriSaveConfigurations to ONE. This is exactly equivalent to running the setSystemConfigurations command with the save option specifed.

6.4 Event Logging and Traps

The event logging on the CPE is managed by three MIB tables:

- wmanDevCmnEventLogTable: This table contains the actual logs of the system. All the Sequans logs and SDS logs have been integrated in this table.
- wmanDevCmnEventLogConfigTable: This table is responsible for the configurations of the wmanDevCmnEventLogTable, like the number of entries that shall be held in it, whether or not the entries wrap around when the table is full, whether a trap should be sent when the table is approaching being full, whether the logs should be saved on a permanent storage, etc…
- wmanDevCmnEventTable: This table contains predefined entries identifying the different events that will be logged in the wmanDevCmnEventLogTable. Each entry in this table defines a textual description of the event, its severity level, whether or not notification should be sent to the management system when this type of event is logged, and the OID of the trap which will be sent to the management system.

Following are the contents of the predefined values in the wmanDevCmnEventTable:

EventId	Description	Severity	EventNotification	NotificationOID
1	A fatal error occurred due to a wrong condition.	Warning	TRUE	1.3.6.1.4.1.32604.15.1
2	A fatal error occurred caused a hardware reset.	Emergency	TRUE	1.3.6.1.4.1.32604.15.2
3	A fatal error occurred caused a hardware reset.	Emergency	TRUE	1.3.6.1.4.1.32604.15.3
4	A fatal error occurred caused a software reset.	Alert	TRUE	1.3.6.1.4.1.32604.15.4
5	A fatal error occurred caused a software reset.	Alert	TRUE	1.3.6.1.4.1.32604.15.5
6	A log message	Informational	FALSE	1.3.6.1.4.1.32604.15.6
7	A log message with arguments	Informational	FALSE	1.3.6.1.4.1.32604.15.7
8	A log message	Informational	FALSE	1.3.6.1.4.1.32604.15.8
9	A log message with arguments	Informational	FALSE	1.3.6.1.4.1.32604.15.9
10	A warning message	Warning	TRUE	1.3.6.1.4.1.32604.15.10
11	A warning message with arguments	Warning	TRUE	1.3.6.1.4.1.32604.15.11
12	A warning message	Warning	TRUE	1.3.6.1.4.1.32604.15.12
13	A warning message with arguments	Warning	TRUE	1.3.6.1.4.1.32604.15.13
14	Logs the entering of a function with the specified function name	Debug	FALSE	1.3.6.1.4.1.32604.15.14
15	Logs the exit of a function with the specified function name	Debug	FALSE	1.3.6.1.4.1.32604.15.15
16	Logs the entering of a function with the specified function name	Debug	FALSE	1.3.6.1.4.1.32604.15.16
17	Logs the exit of a function with the specified function name	Debug	FALSE	1.3.6.1.4.1.32604.15.17

Table 3: wmanDevCmnEventTable

In order to enable logging on the CPE, the following steps should be followed:

- Adjustments in the wmanDevCmnEventLogConfigTable
    - Configure the wmanDevCmnEventLogEntryLimit with the maximum number of entries that should be held in the wmanDevCmnEventLogTable
    - Configure the wmanDevCmnEventLifeTimeLimit with the time after which the events are considered obsolete.
    - Configure the wmanDevCmnEventLogEntryLimitPerEventId which defines how many entries shoukd exist in the table for each type of event defined in wmanDevCmnEventTable.
    - Configure the wmanDevCmnEventLogSeverityThreshold which defines the minimum severity that should be included in the table. All logs of severities less than the wmanDevCmnEventLogSeverityThreshold will not be logged in the table.

- Configure the wmanDevCmnEventLogWrapAroundBuffEnable to enable the entries in the table to be overwritten when the table is full.
- Configure the wmanDevCmnEventLogResidualBuffThreshold which defines the limit after which a trap will be sent with each entry logged in the table.

- Adjustments in the Configuration parameters to save logs on FTP
  - The MIBs define whether or not logs should be saved in permanent storage or not, however it doesn't enable modifying this option at runtime. For this purpose a configuration parameter has been added to the configuration file to control this. The IS_WRITING_LOGS_ON_FTP_ENABLED is used for this option.
- Adjustments in the wmanDevSsNotification for sending traps
  - The traps generally are enabled and disabled as desired. The administrator can configure the traps to be enabled or disabled across the whole system or per trap.
  - To enable or disable traps across the whole system, the wmanCpePriTrapGeneration should be configured.
  - To enable or disable the event logging traps, the wmanDevSsTrapControlRegister should be configured.
  - The traps should be sent to a preconfigured management system, in order to do this the details of this management system should be configured on the wmanDevCmnSnmpV1V2TrapDestTable.
- Enabling logging
  - To enable logging in the module, select the modules as desired and run "enableLog" command.
  - For example:
    - ✓ *cbe "enableLog WWW"*
    - ✓ *cbe "enableLog PKMB"*

6.5 Provisioned Service Flows

The standard MIBs support provisioning of service flows' through NMS. This is done through the following tables:

- wmanIf2fBsProvServiceFlowTable - Each entry defines a provisioned service flow associated with a certain SS. The entry contains the generic service flow parameters.
- wmanIf2fBsProvClassifierRuleTable – Each entry defines a provisioned classifier rule associated with a provisioned SF.
- wmanIf2fBsProvPhsRuleTable – Each entry defines a provisioned PHS rule associated with a provisioned classifier.

- wmanIf2fBsProvServiceClassTable – Each entry defines a provisioned service class defining a set of QoS parameters. The service class is not linked to a specific service flow, i.e the same QoS parameter set can be used with multiple service flows.

The relations between the service flow, its associated classifiers and PHS rules are as follows:

- Each provisioned service flow can have one or more provisioned classifier rules.
- Each provisioned classifier rule can have zero or one provisioned PHS rule.
- Each provisioned PHS rule must be associated with a provisioned classifier rule.
- Each provisioned service flow can use zero or one activated service class.

The steps needed to create a provisioned service flow, with one classifier, one PHS rule and uses a service class is described below. This example is the general example; however steps needed for the service class, PHS and classifier rules can be omitted.

- Creation of a provisioned Service Flow - Add the parameters of the service flow without changing the RowStatus to Active.
- Creation of a provisioned Classifier Rule - Add the parameters of classifier rule without changing the RowStatus to Active.
- Creation of provisioned PHS Rule - Add the parameters of PHS rule without changing the RowStatus to Active.
- Creation and Activation of a provisioned Service Class – Add the parameters of the service class and activate it by setting the RowStatus column to active. Note that this step is independent of the service flow activation, since the same service class can be used with multiple service flows.
- Activation of the Provisioned Service Flow – Change the RowStatus of the service flow entry to active, this will activate all associated entries in the classifier and PHS tables. Whenever the SS connects/reconnects the service flow will be added to the SS.
- Reconfiguring parameters while provisioned service Flow is active – Change the RowStatus of the service flow to notInService. Modify the service flow, associated classifier or PHS rules parameters, and then change the RowStatus of the service flow to active. Whenever the SS reconnects the service flow will be added to the SS.

7. STARTUP SCRIPTS

A default startup scripts used to start the basic Wimax functions is provided in the on board flash. This script can be copied from on board flash to FTP server, customized and modified, then copied back to on board flash.

The content of this default script is as follows:

#load WiMAX application package from flash
ldz "/tffs/appb.Z.out"

#RF driver definition, not to be changed
APPB_RFC_DRIVER_NAME = "PM8850"

#RF calibration data definition, not to be changed
RFC_PM880X_CALIBRATION_FILE = "/tffs/calibration.cfg"

#RF frequency support range, not to be changed
RFC_PM880X_MIN_FREQ = 2497750
RFC_PM880X_MAX_FREQ = 2688250
APPB_RFC_MIN_FREQUENCY = RFC_PM880X_MIN_FREQ
APPB_RFC_MAX_FREQUENCY = RFC_PM880X_MAX_FREQ

#MIMO/SISO channel scheme, for MIMO set to 2, for SISO set to 0
wmdDbgChannelScheme = 0

 # Set Ethernet port configuration, not to be changed
APPB_BSP_TO_FORWARDING = 1
APPB_EXTERNAL_MII = 1
 # Set maximum number of SS can be served by the base station
APPB_MAX_SS_QTY = 55

#enable 1pps synchronization support, to be removed if 1pps is not used
appbDbgGpsSynchro = 1
gpsApplyRfCorrection = 1
appbDbgGpsLoopFilterValue = 0.01

#Hardware system initialization, mandatory, not to be changed
swmSysInit

#Set mode for fatal error handling -- reboot
epsSetFatalErrorMode 2

#Set mode of operation to be super user, to enable access to all commands
cbe "setuser super"

#Set Ethernet port speed to 100Mbps
cbe "setmii speed=100"

#Set MAC frame (FFT size, channel size, number of sub channel, preamble index)
cbe "setMacFrame fft=1024 band=10 subch=63 preamble-index=0"

#Set downlink frequency and power level
cbe "setMacDl fr=2550000 tx-power=0"

#Set uplink frequency

cbe "setMacUl fr=2550000"

 # Disable HARQ support if no mobility is going to be used
cbe "createprovsf mac=FF:FF:FF:FF:FF:FF dir=uplink sfid=0 classifier1=any"
cbe "createprovsf mac=FF:FF:FF:FF:FF:FF dir=downlink sfid=0 classifier1=any"

 # Set link adaptation mode
cbe "setlinkadaptationdl mode=manual"
cbe "setlinkadaptationul mode=manual"

 # Set PKM version
cbe "setcaps pkm-version=none"

#Enables air interface to accept connection request from SS
cbe "setMacFrame started=1"

Other commands can be added to this startup script to be executed automatically during system boot up.

8. MIMO OPERATION

To use MIMO mode in the base station, the steps listed below are to be followed.

a. modify startup script:

set wmdDbgChannelScheme=2

add following commands immediately after *swmSysInit*:

cbe "setuser super"

cbe "addDlZone mat=matrix-b st=stc-2"

cbe "setschedulertdd spli=75"

b. After air interface is started, set the size of SISO zone to minimum, the size of MIMO zone to maximum.

cbe "dmsb:setZoneProperties zone-id=0 min-slot=2 max-slot=4"

cbe "dmsb:setZoneProperties zone-id=1 min-slot=0 max-slot=20"

c. After a SS has registered into the base station over the standard SISO zone, assign the SS to the MIMO zone

cbe "setssphydl mimo-kind=matrix-b zone=1"

9. R6 OPERATION WITH ASN-GW

FRC BSMax-250 supports R6 interface as defined by the Wimax Forum NWG. It had been successfully tested with WiChorus ASN GW. Following ASN GW instructions are based on a WiChorus devcie.

9.1 OPERATION WITHOUT AUTHENTICATION

The CPE and BS start-up scripts should contain the following line:

cbe "setcaps pkm-version=none"

The ASN-GW should be configured with null authentication as follows:

#config t

(config)#null-authentication-enable

9.2 OPERATION WITH AUTHENTICATION

The CPE and BS start-up scripts should contain the following line:

cbe "setcaps pkm-version= pkm-v2"

The ASN-GW should be configured with the null authentication disabled as follows:

#config t

(config)#no null-authentication-enable

9.3 RE-AUTHENTICATION

The re-authentication procedure is controlled by the following equation:

$$x\text{-}600 = 0.75*x$$

where x is the session timeout value configured on the AAA server.

(x-600) is the time at which the SS starts the re-authentication procedure.

(0.75*x) is the time at which the authenticator (ASN-GW) starts the re-authentication procedure.

To trigger re-authentication from the SS:

$$600 < x-600 < 0.75*x \rightarrow 1200 \text{ seconds} < x < 2400 \text{ seconds}$$

To trigger re-authentication from the ASN-GW:

$$x-600 > 0.75*x \rightarrow x > 2400 \text{ seconds}$$

RF exposure warning

This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 100 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provided with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.