WiMAX Outdoor CPE

CPEMAX-OD250

User Manual

Rev. 4

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 here in 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.

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.

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 (8 inches) from al persons.

R&TTE Compliance Statement

This equipment is confirmed to comply with the requirements set ou 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.

IMPORTANT NOTICE:

This document describes in details the steps and procedure required to install and operate FRC WiMAX Outdoor CPE. The document also lists the different available CLI/Web commands to interact with the CPE with a detailed list of the parameters.

AUDIENCE

This user guide is intended for system administrators and operators responsible for managing and operating the WiMAX CPE.

TABLE OF CONTENTS

CHAPTER ONE: PRODUCT OVERVIEW

1.1 INTRODUCTION

The WiMAX Outdoor CPE with router/Bridge functionality provides WiMAX connectivity to wired LAN networks. The CPE functions as a WiMAX gateway providing wired and wireless broadband Internet access services through connection with a WiMAX base station. The CPE is easily installed, utilizing Plug and Play functionality. In addition to web-based configuration, users can update firmware, simplifying installation and operation of the device. The CPE operates in Router mode and Bridge mode, both providing Internet access:

1.1.1 ROUTER MODE

In Router mode, the internal IP address is acquired through dynamic host configuration protocol (DHCP), static IP address, or PPPoE connection to the WiMAX base station. With enabled DHCP service, connected PCs and notebooks can acquire addresses from the CPE.

A CPE deployed for operation in the router mode is basically used to provide a gateway to hosts on a local area network where the CPE hides all the traffic originating from the LAN behind its IP address which is assigned from the public domain, which makes the traffic appear as if it's originating from the CPE itself. A router CPE implements Network Address Port Translation protocol (NAPT).

1.1.2 BRIDGE MODE

This mode requires minimal presetting, with the internal IP address configured in the same or different network segment as the WiMAX base station. Bridging is a forwarding technique used in packet-switched computer networks.

A CPE deployed for operation in the bridge mode is basically used to provide Ethernet service to enterprise customer locations. An enterprise location has a CPE with an Ethernet interface that could support one or many user hosts in the local network through a switch. CPE supports both IP and Ethernet CS. If Ethernet CS is supported by the network then Layer 2 connectivity can be established between SS and CSN. In this case, the network service to the enterprise customer is an Ethernet service from the core network all the way to the enterprise MS.

1.2 PRODUCT OVERVIEW: WIMAX TRANSMISSION FEATURES

The following transmission features are supported by the WiMAX Outdoor CPE to provide stable and error-free connection.

1.2.1 DYNAMIC ADAPTATION

Dynamic adaptation enables the CPE to maintain a high data rate while taking into account current link conditions like half-loss, interference, and seasonal foliage changes. The CPE monitors wireless link conditions on a burst-by-burst basis and uses dynamic adaptive modulation control, based on the measured CINR (Carrier/(Interference + Noise) Ratio), to regulate the link.

1.2.2 ADAPTIVE CODING

Each data transmission to or from the CPE contains extra, redundant information to reduce the errors introduced during transmission. A coding rate is the ratio of meaningful data to this extra padding (including error correction data). Adaptive coding enables the CPE to dynamically change the coding rate depending on this ratio. This CPE supports coding rates of 1/2, 2/3, and 3/4.

1.2.3 ADAPTIVE MODULATION

Adaptive Modulation is used to specify what modulation technique is coded in to carriers composing orthogonal frequency-division multiplexing (OFDM) symbols. This CPE supports QPSK, 16 QAM, and 64 QAM modulation techniques.

1.2.4 TRAFFIC CLASSIFICATION

Traffic Classification categorizes transmission bursts by searching for pattern matches within the data. Classifications (for example, burst destination, source MAC address, and Virtual LAN tags) are defined and managed by the base station and transmitted to the CPE.

1.3 SYSTEM TOUR

1.3.1 MAIN FEATURES

- WiMAX Forum IEEE 802.16e-2005 compliance
- Modulation technique: OFDMA employing Time-Division Duplex (TDD) mechanism.
- PRBS subcarrier randomization
- Contains pilot, preamble, and ranging modulation
- FEC coding Rate (Downlink/Uplink): QPSK, 16QAM, 64QAM.
- Supports 5, 7 and 10 MHz bandwidth
- Compliant with IP67 and lightening protection (Surge) standard
- LAN /WAN port with IP Filtering Support.
- Supports DHCP Server/ Client , VPN pass-through (IPSEC/PPTP), NAT
- Ease-of-use web-based interface for managing and configuring
- Software features: Dual Image, Automatic/Manual Software Upgrade, Manual/Automatic Configuration file Support, Factory Reset and Status LED, Standard and Private MIBs, CLI support.
- Support both IP-CS and ETH-CS operation.
- Wide band frequency support.
- High output power support.

Model	**Band Frequency** MHz	**Output Power** dBm
CPEMAX-OD250	2498.5~2687.5	22.5

1.3.2 PACKAGE CONTENTS CHECKLIST

Once unpacked, ensure that all contents are included. Refer to the list below for the materials list.

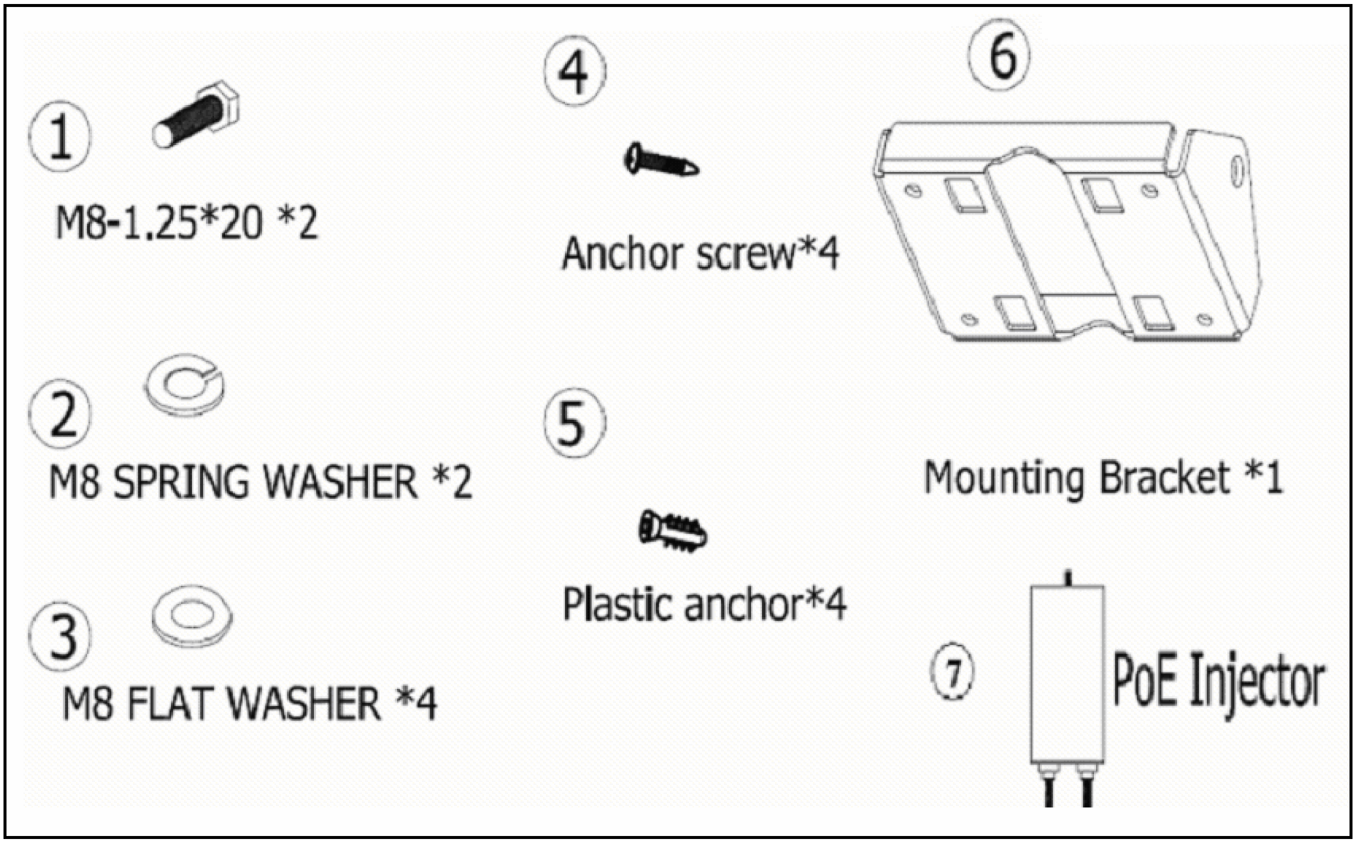


Figure 1: CPE package contents list.

CHAPTER TWO: BASIC INSTALLATION

This chapter contains information on safety and installation procedures for the WiMAX Outdoor CPE. Follow the recommendations outlined in this chapter to ensure the correct operation of the CPE and reduce the risk of damage to the device or personal injury.

2.1 SAFETY MEASURES

Before installing and using the CPE, take note of the following precautions:

- Read all instructions carefully
- Use only the Power over Ethernet adapter supplied
- Follow all warnings and cautions in this manual and on the unit case

2.2 SYSTEM REQUIREMENTS

Proper installation of the CPE requires the following minimal configuration:

- A PC with a 10Base-T/100Base-TX adapter.
- A Web browser installed such as Microsoft Internet Explorer, Firefox, Chrome or Safari.

2.3 HARDWARE INSTALLATION

This section describes the proper steps required to install the CPE, and to align the antenna.

2.3.1 CHOOSING A LOCATION

To make optimal use of the CPE, a suitable location is important. The range of the CPE largely depends upon the position of the antenna. It is recommended that CPE is within 2Km from the BS and an overall survey performed, observing the following requirements, before installing the CPE:

- Do not place the CPE near the floor or near metal objects, such as drain pipes.
- The location must allow easy disconnection of power to the CPE if necessary.
- Air must be able to flow freely around the hardware.
- The CPE unit must be kept away from vibration and excessive heat.
- The installation must conform to national and local electrical codes

2.3.2 POLE INSTALLATION STEPS

To pole mount the CPE, perform the following steps:

1. Ensure that the pole intended for installation is securely attached to a solid base.
2. Fasten the CPE on the pole with Mounting Bracket and bolt as shown below.

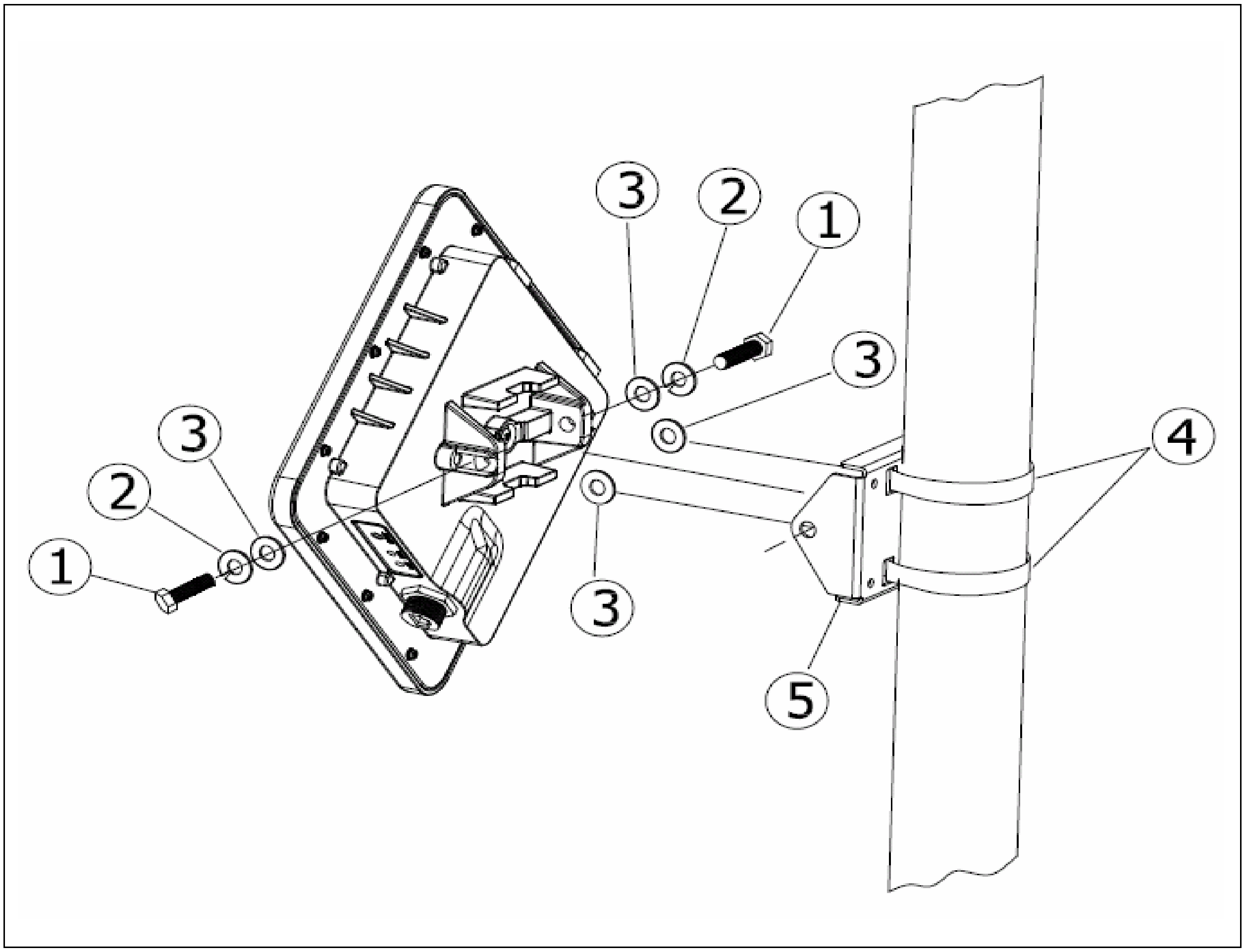


Figure 2: CPE Pole Mounting.

3. Install weather-proof CAT-5e cable between Ethernet port of CPE and “DC+Data output” port of POE injector as shown in Figure 3.

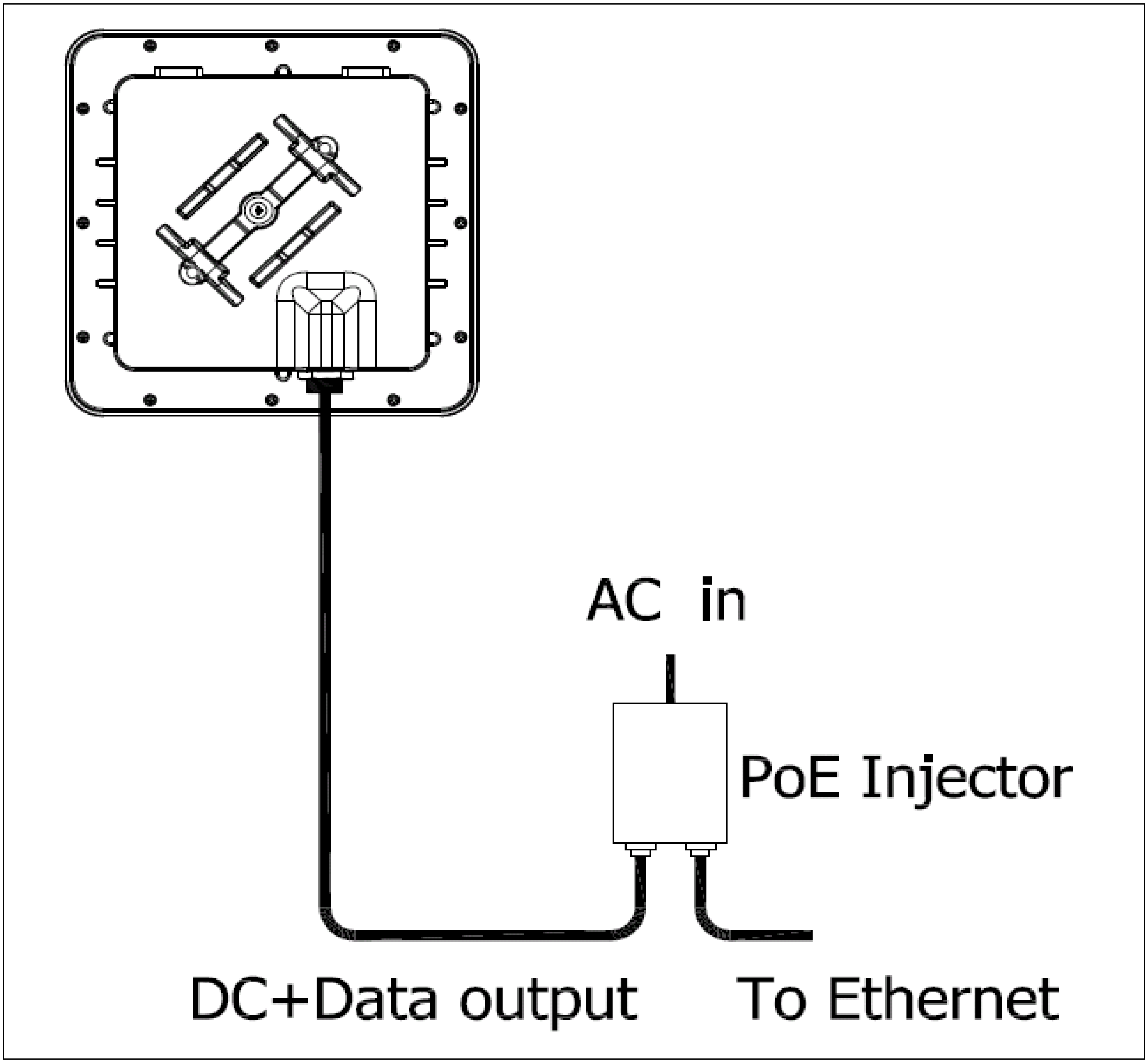


Figure 3: POE Connection Setup.

4. Install CAT-5e cable to "To Ethernet" port of POE Injector as shown in Figure 4.

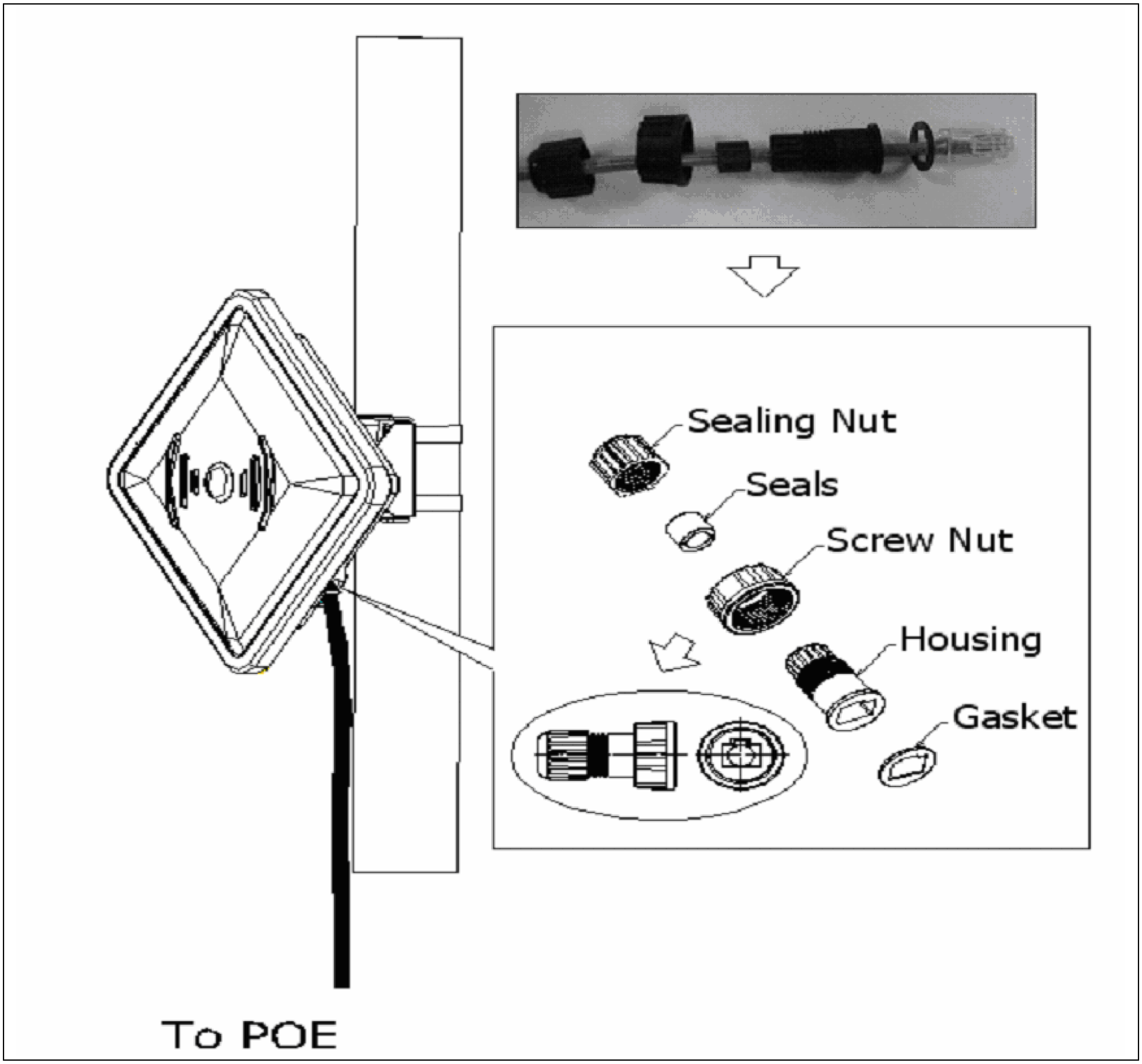


Figure 4: Ethernet installation.

2.3.3 WALL INSTALLATION STEPS

To wall mount the CPE, perform the following steps:

1. Ensure that the wall intended for installation is securely solid base.
2. Fasten the CPE on the wall with Mounting Bracket and bolt as shown below.

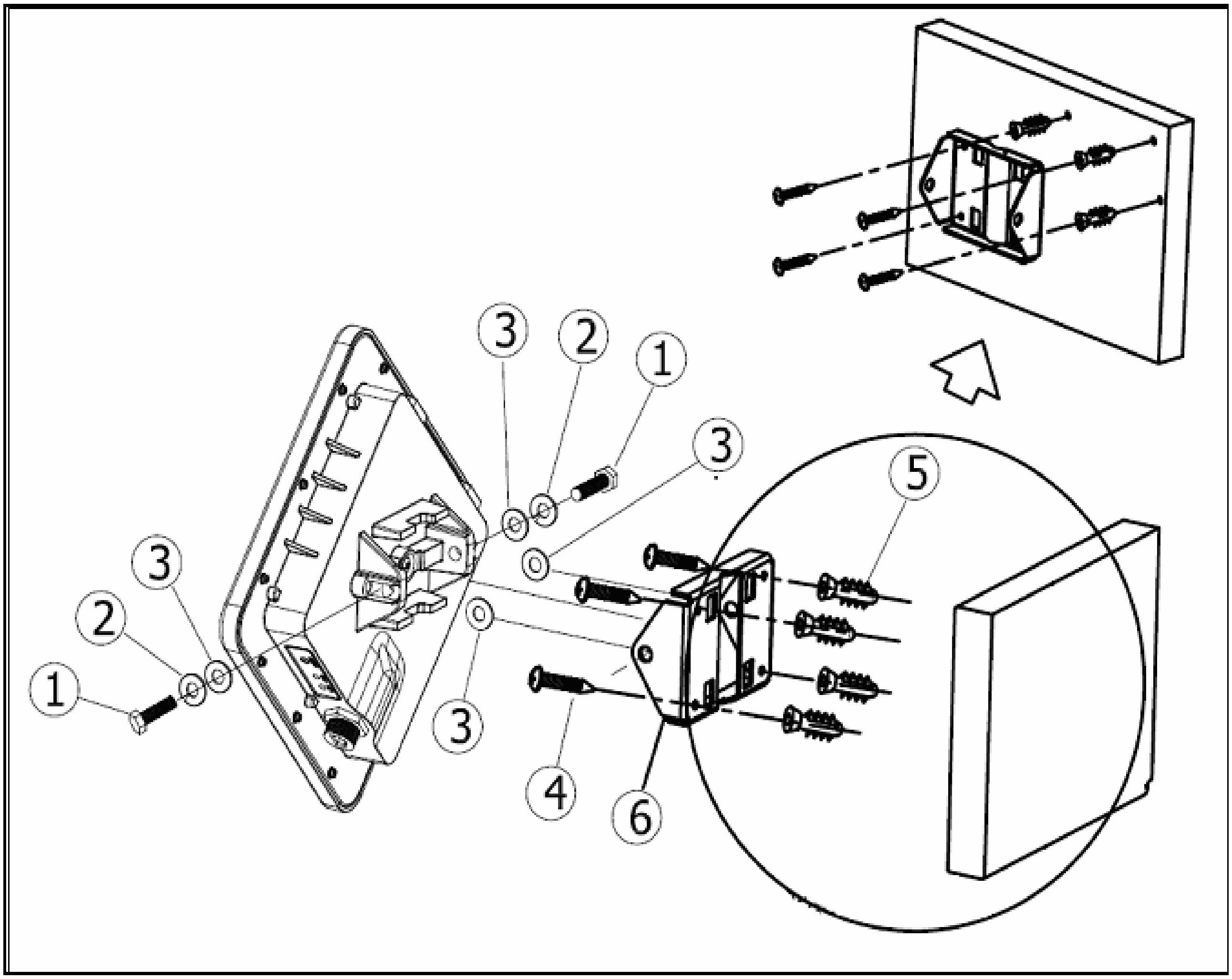


Figure 5: CPE Wall Mounting.

3. Install weather-proof CAT-5e cable between Ethernet port of CPE and "DC+Data output" port of POE injector as shown in Figure 3.

4. Install CAT-5e cable to "To Ethernet" port of POE Injector as shown in Figure 4.

2.3.4 INSTALLATION CHECK UP

For correct installation, please check the following:

1. Ensure the CPE is directed towards the WiMAX Base Station.

2. Adjust the direction of the CPE in small increments (both horizontally and vertically) while checking signal strength LEDs until the best RSSI level is achieved.

3. Optionally you can monitor live RF statistics by clicking RF-Stat through web interface. Please refer to "Web Graphic User Interface" section for more details.

4. Tighten all mounting hardware screws and clamps.

2.3.5 CPE SIGNAL STRENGTH

The CPE is equipped with LEDs of four different colors to indicate the RSSI of the WIMAX CPE as shown in Figure 6. The LEDs indicate the signal strength as follow:

- Very Weak Signal ➔ Red Light
- Weak Signal ➔ Orange Light
- Good Signal ➔ Blue Light
- Excellent Signal ➔ Green Light

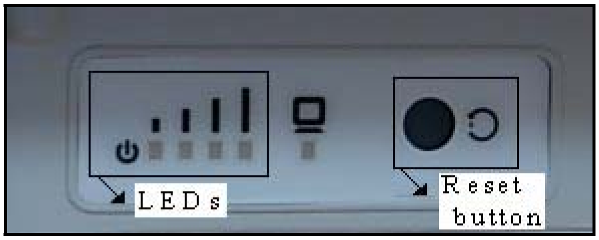


Figure 6: CPE LEDs and factory reset button.

Red LED also acts as Status LED with the following modes:

- During Firmware loading ➔ Rapid flashing.
- Scanning for BS ➔ Slow flashing.
- Connected to a BS ➔ On.

2.3.6 FACTORY RESET PROCEDURE

The factory reset procedure may be needed in the installation setup. It is used to restore the system configurations to their defaults. The factory reset can be triggered by:

- Push the reset button shown in Figure 6.

The reset button must be pressed for at least 5 seconds in order to trigger a system reset.

CHAPTER THREE: WEB CONFIGURATION

The WiMax Outdoor CPE's Web-based Graphical User Interface (GUI) enables quick, simple and essential setup. The web interface consists of the following main functionalities:

- Current settings and status display.
- Connection of the configured CPE to WiMAX base stations.
- Network setting changes, such as internal IP address, IP address pool, DHCP settings and more.
- Wireless security setup.
- Internal password change.

⚠ The system configuration parameters are maintained in the configuration file saved on flash.

⚠ If the CPE is connected to the BS, operating in bridge mode, then it will get an IP from DHCP and the default IP will no longer be accessible.

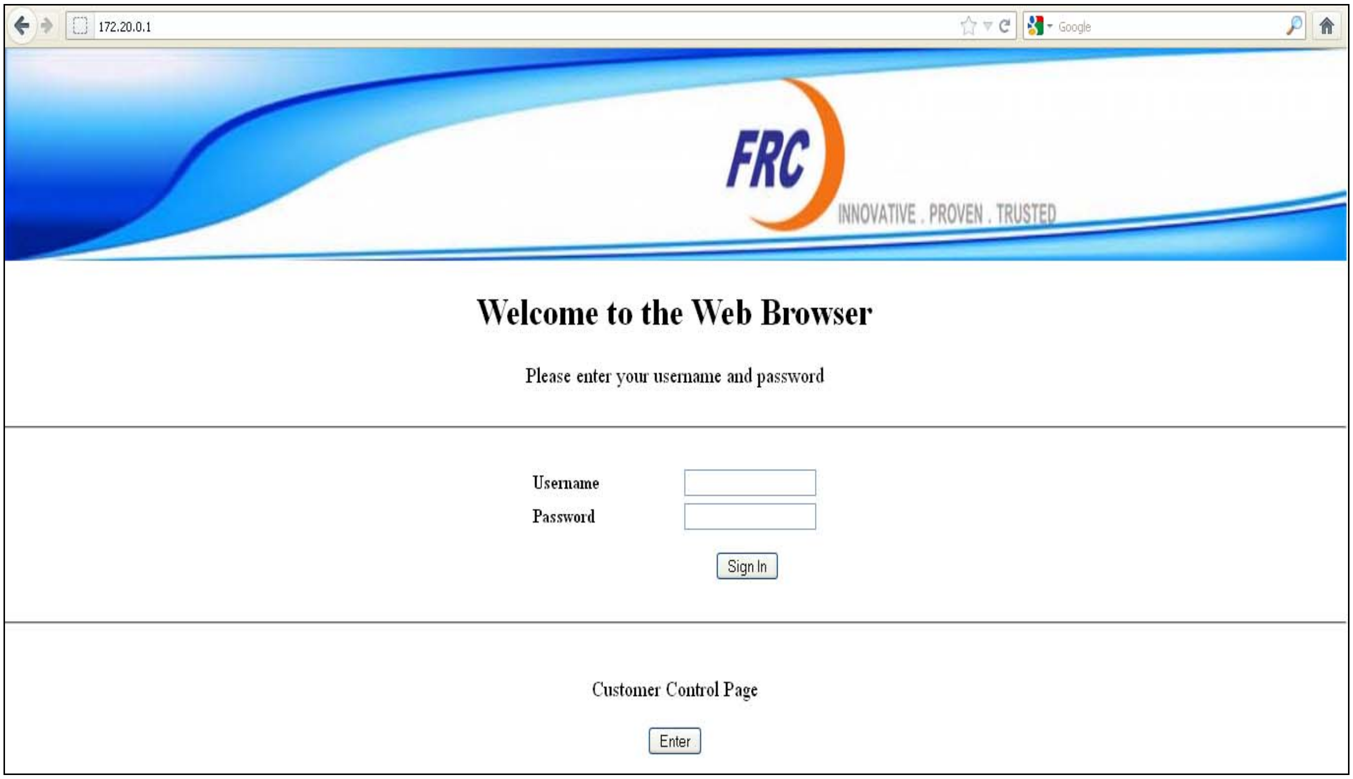
3.1 LOGGING IN

To log in to the administrator GUI, perform the following steps:

1. Ensure the installation described in Chapter 2 is complete. Check that the CPE has power and that the signal strength is good.

2. Launch an Internet browser on the administrator’s PC.

3. Enter the default IP address 172.20.0.1 in the browser address field and press Enter. The Login screen displays as shown in Figure 7:

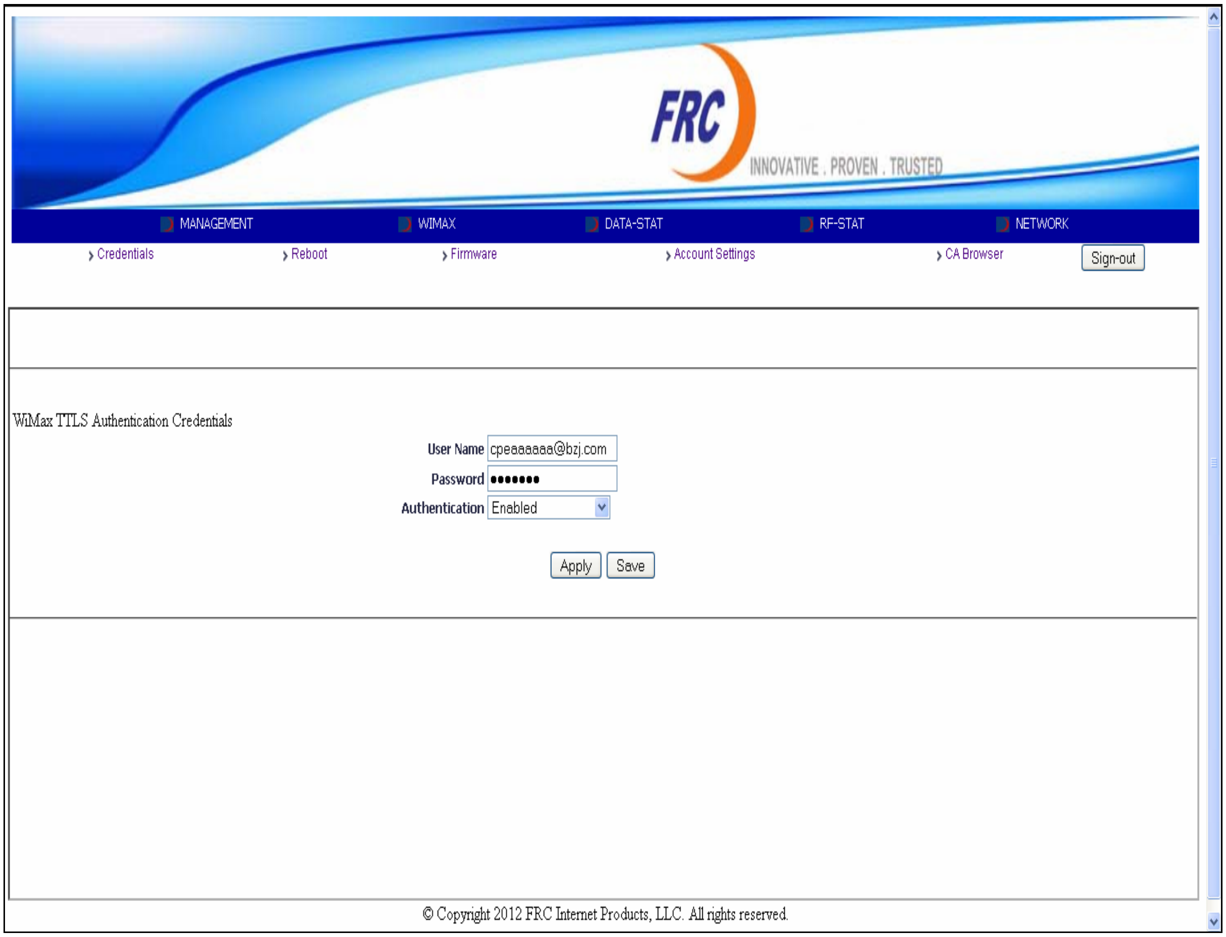


Welcome to the Web Browser

Please enter your username and password

Figure7: Sign-In Page.

4. Enter user name *frcweb* and password *frcadmin* and click **Sign In**. Then CPE configuration homepage appears as shown in Figure 8:



WiMax TTLS Authentication Credentials

User Name cpeaaaaaaa@bzj.com

Password •••••••

Authentication Enabled

© Copyright 2012 FRC Internet Products, LLC. All rights reserved.

Figure 8: Home page.

NOTE: The CPE functions in Router or Bridge mode.

3.2 SYSTEM MANAGMENT

The system management is used to review, change and save all CPE system settings. Only the administrator can make changes to this screen.

3.2.1 WIMAX AUTHENTICATION

3.2.1.1 WIMAX AUTHENTICATION CREDENTIALS

To change the CPE credentials, perform the following steps:

1. Enter into the **Management** Tab field.

2. Select **credentials** field.

3. Enter the **user name** in the form *someone@thebluezone.com*.

4. Enter the **password.**

5. Click **Apply.**

3.2.1.2 WIMAX AUTHENTICATION SUPPORT

To enable TTLS authentication mode, perform the following steps:

1. Enter into the **Management** Tab field.

2. Select **credentials** field.

3. Select to enable or disable **Authentication**.

4. Click **Apply.**

⚠ The WiMAX authentication will take effect by next WiMAX session.

⚠ Click Save to preserve the credentials after rebooting the CPE.

3.2.2 SYSTEM REBOOT

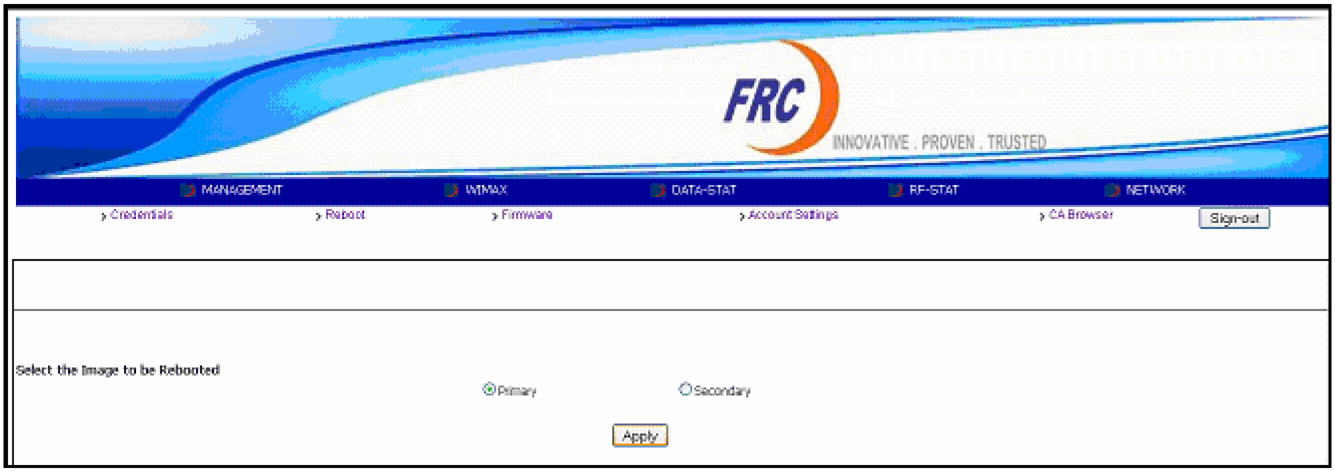
To reboot CPE, perform the following steps as shown in Figure 9:

1. Enter into the **Management** Tab field.

2. Select **Reboot** field.

3. Select to **Primary** or **Secondary** image.

4. Click **Apply.**



Select the Image to be Rebooted

● Primary ○ Secondary

Figure 9: System reboot.

3.2.3 UPGRADE SYSTEM FIRMWARE

To Upgrade the CPE firmware system based on FTP, perform the following steps:

1. Enter into the **Management** Tab field.

2. Select **Firmware** field.

3. Fill the ftp setting, as shown in Figure 10.

4. Click **Apply.**

⚠ Consult your WiMAX service provider for this process, wrong image could damage your CPE.

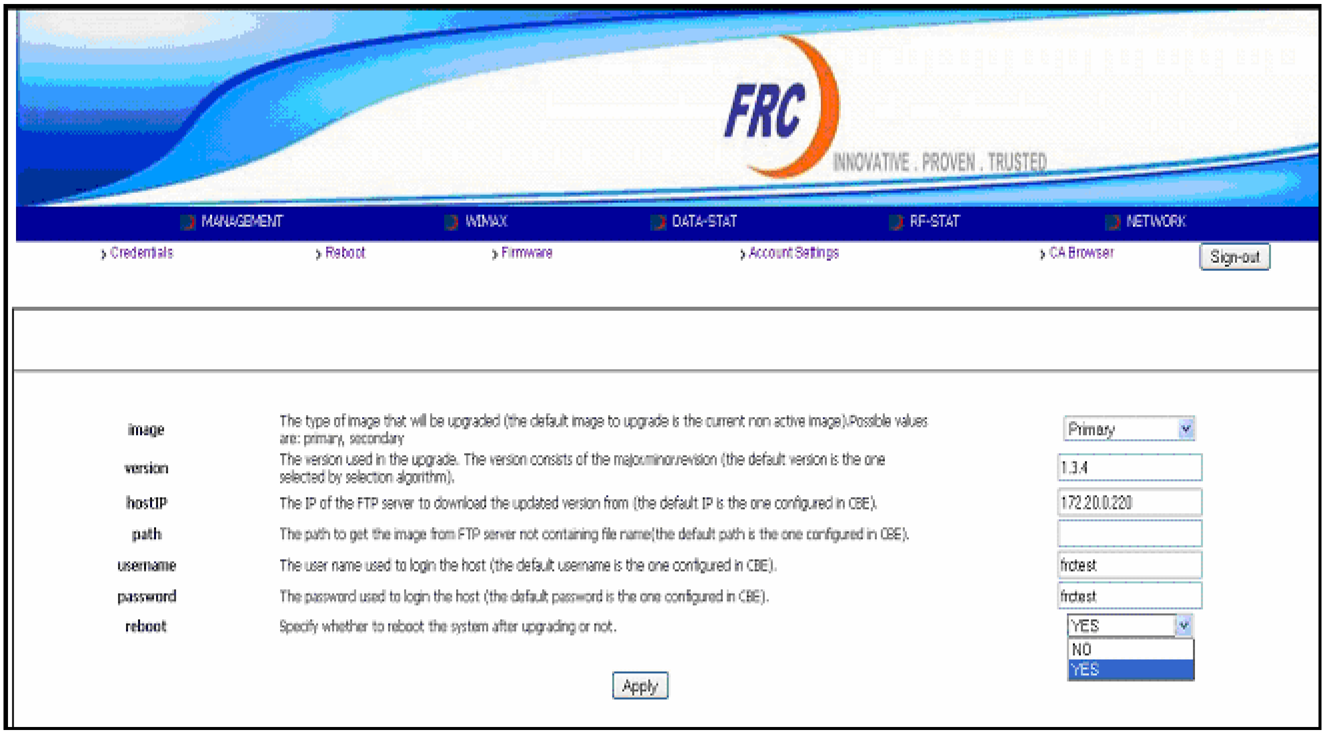


image	The type of image that will be upgraded (the default image to upgrade is the current non active image).Possible values are: primary, secondary	Primary
version	The version used in the upgrade. The version consists of the major.minor.revision (the default version is the one selected by selection algorithm).	1.3.4
hostIP	The IP of the FTP server to download the updated version from (the default IP is the one configured in CBE).	172.20.0.220
path	The path to get the image from FTP server not containing file name(the default path is the one configured in CBE).	
username	The user name used to login the host (the default username is the one configured in CBE).	frctest
password	The password used to login the host (the default password is the one configured in CBE).	frctest
reboot	Specify whether to reboot the system after upgrading or not.	YES NO YES

Figure 10: Firmware upgrade.

The following parameters should be set correctly in the CPE configurations for SW Upgrade:

FTP Server IP address

FTP user name

FTP password

File path

File name

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.

3.2.4 WEB CREDENTIAL

To Change the CPE web access credentials, perform the following steps:

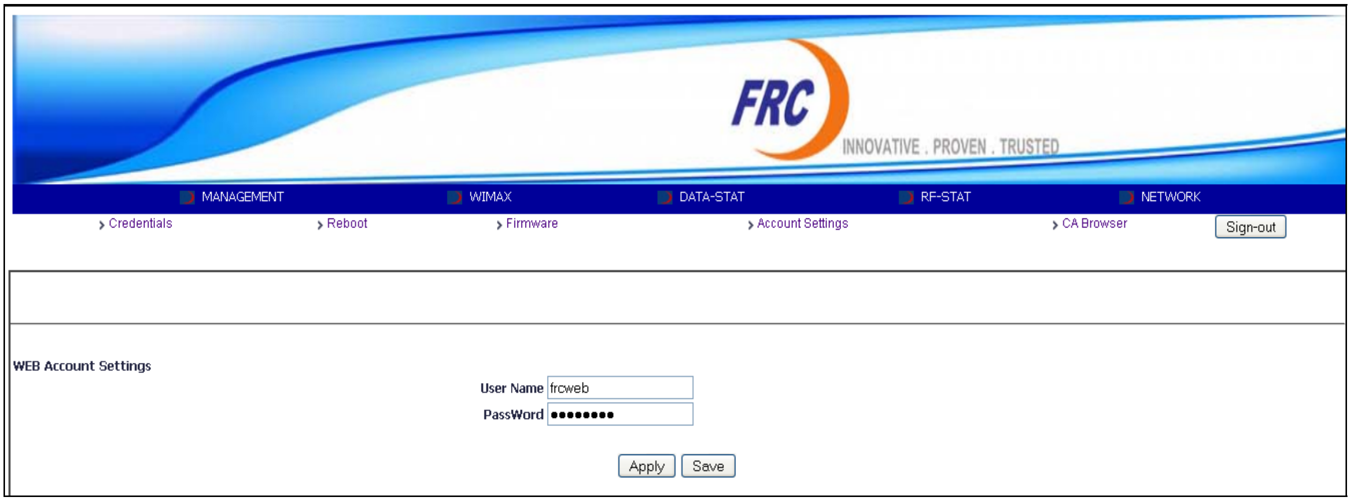
1. Enter into the **Management** Tab field.

2. Select **Account Settings** field.

3. Fill the user name and password, as shown in Figure 11.

4. Click **Apply.**

⚠ Click Save to preserve the web credentials after rebooting the CPE.



WEB Account Settings

User Name frcweb

PassWord ●●●●●●●●

Figure 11: Web Credential.

3.2.5 TTLS CERTIFICATE

To download the TTLS root certificate, perform the following steps:

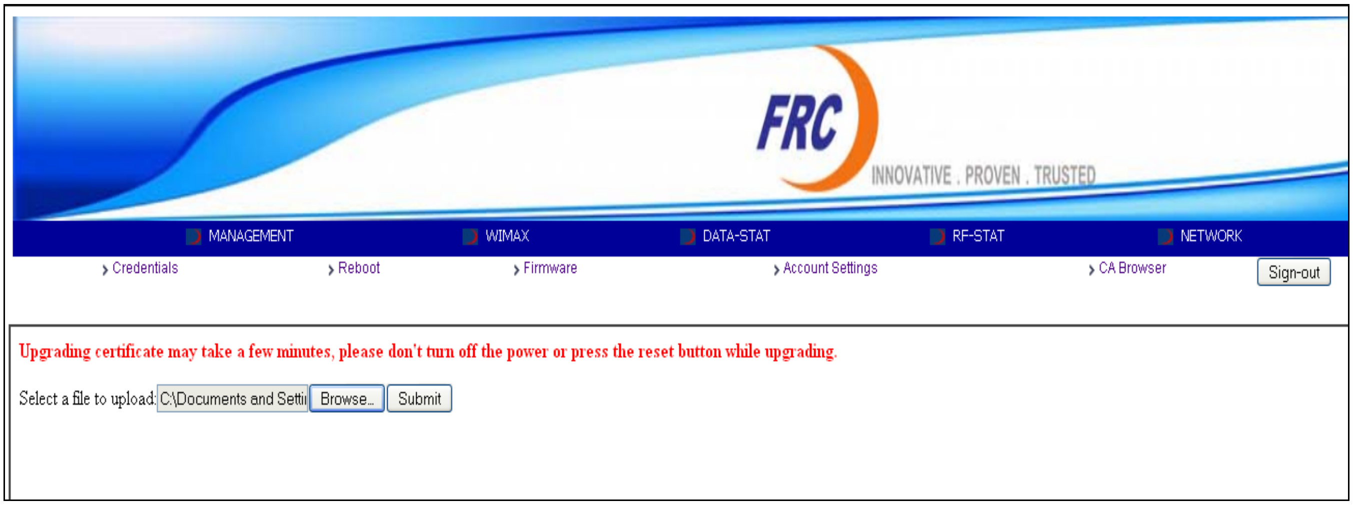
1. Enter into the **Management** Tab field.

2. Select **CA Browser** field.

3. Browse the certificate as shown in Figure 12:

4. Click **Submit.**

⚠ The maximum TTLS certificate size allowed is 8kbyte.



Upgrading certificate may take a few minutes, please don't turn off the power or press the reset button while upgrading.

Select a file to upload: C:\Documents and Setti

Figure 12: Certificate upgrade.

3.3 WIMAX SETTINGS

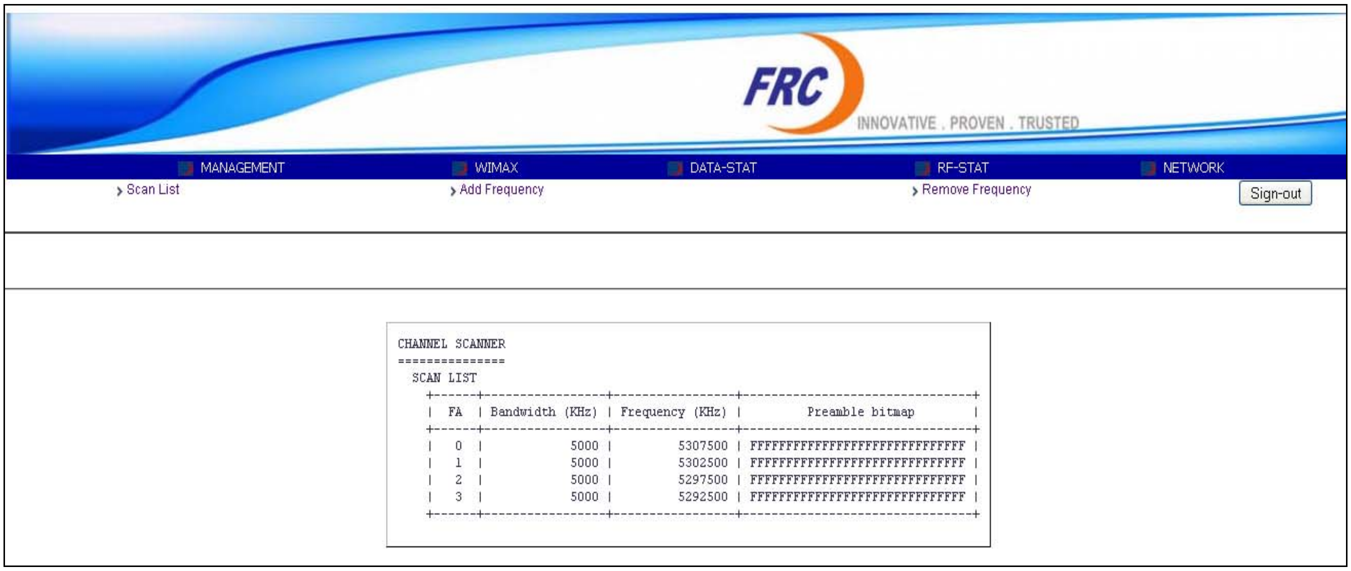
The WiMAX settings are used to add, remove and display all channels settings. Only the administrator can make changes to this screen.

3.3.1 OPERATIONAL FREQUENCIES

To display the scan list of the CPE, perform the following steps:

1. Enter into the **WIMAX** Tab field.

2. Select **Scan list** field.



```
CHANNEL SCANNER
===============
  SCAN LIST
    +------+-----------------+-----------------+--------------------------------+
    |  FA  | Bandwidth (KHz) | Frequency (KHz) |         Preamble bitmap        |
    +------+-----------------+-----------------+--------------------------------+
    |   0  |            5000 |         5307500 | FFFFFFFFFFFFFFFFFFFFFFFFFFFFFF |
    |   1  |            5000 |         5302500 | FFFFFFFFFFFFFFFFFFFFFFFFFFFFFF |
    |   2  |            5000 |         5297500 | FFFFFFFFFFFFFFFFFFFFFFFFFFFFFF |
    |   3  |            5000 |         5292500 | FFFFFFFFFFFFFFFFFFFFFFFFFFFFFF |
    +------+-----------------+-----------------+--------------------------------+
```

Figure 13: Operational frequencies display.

3.3.2 ADD FREQUENCY

To add a frequency channel, perform the following steps:

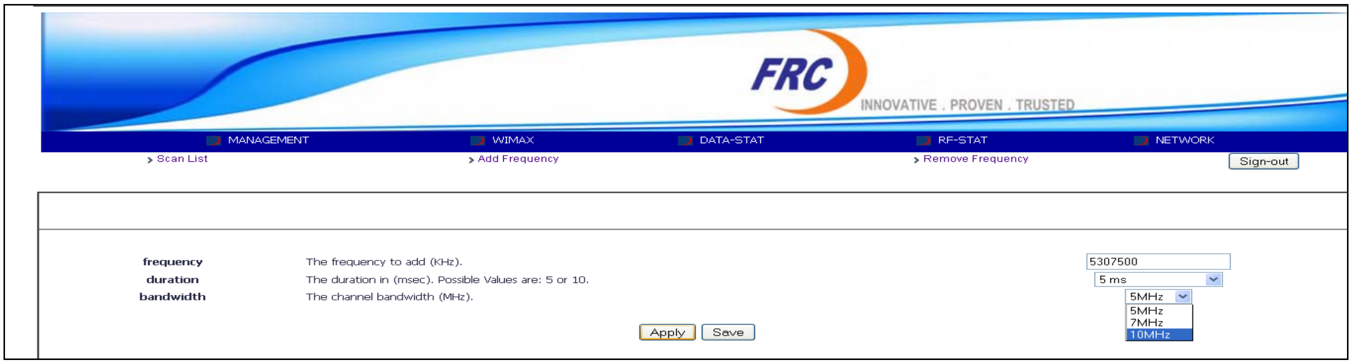
1. Enter into the **WIMAX** Tab field.

2. Select **Add Frequency** field.

3. Specify the channel **frequency**, **duration** and **bandwidth** as shown in Figure 14.

4. Click **Apply.**

⚠ Click Save to preserve the added frequencies after rebooting the CPE.



frequency	The frequency to add (KHz).	5307500
duration	The duration in (msec). Possible Values are: 5 or 10.	5 ms
bandwidth	The channel bandwidth (MHz).	5MHz 5MHz 7MHz 10MHz

Figure 14: Add frequency.

3.3.3 REMOVE FREQUENCY

To remove a frequency channel, perform the following steps:

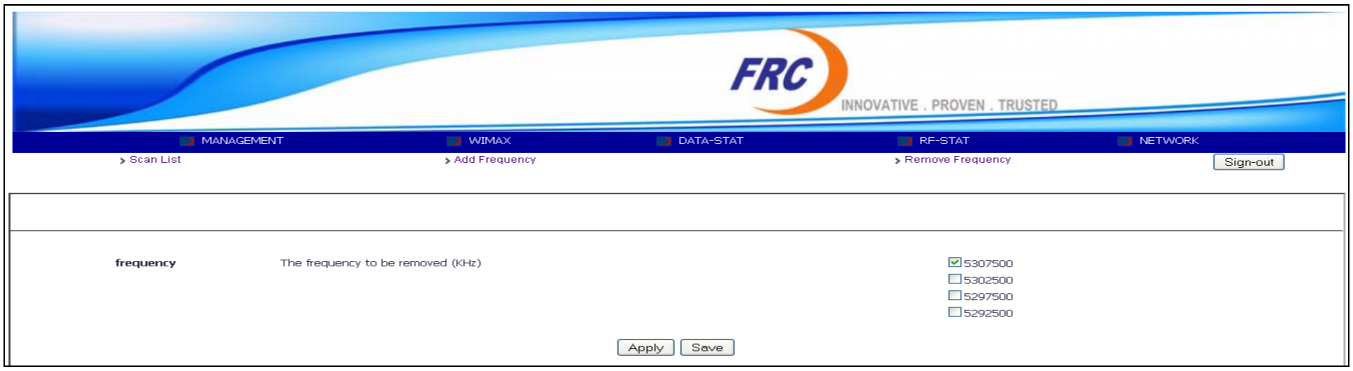
1. Enter into the **WIMAX** Tab field.

2. Select **Remove Frequency** field.

3. Specify the channel **frequency** to remove as shown in Figure 15.

4. Click **Apply.**

⚠ Click Save to preserve the removed frequencies after rebooting the CPE.



frequency	The frequency to be removed (KHz)	☑5307500 □5302500 □5297500 □5292500

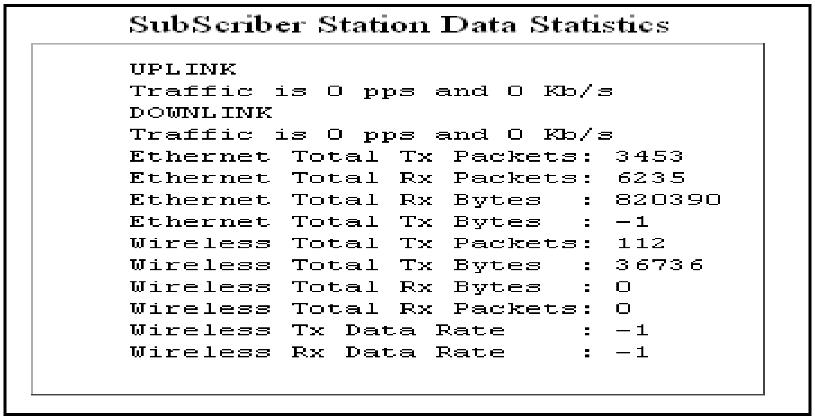
Figure 15: Remove frequency.

3.4 SYSTEM STATISTICS

3.4.1 DATA STATISTICS

To display the Data Statistics of the CPE, perform the following steps:

1. Enter into the **DATA-STAT** Tab field as shown in Figure 16:



SubScriber Station Data Statistics

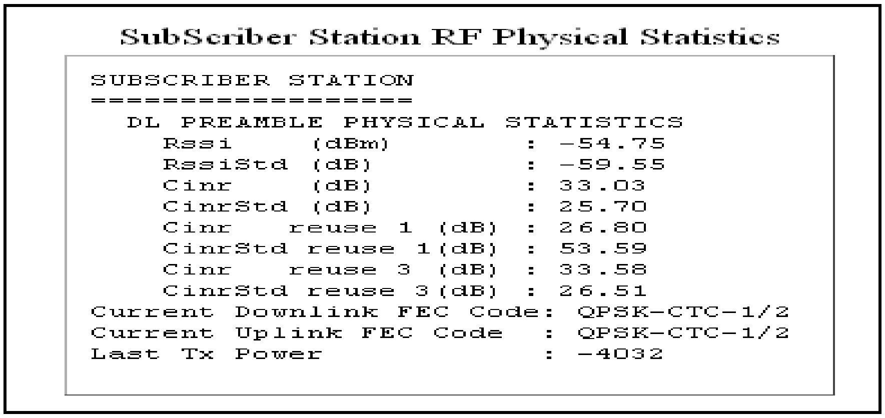
```
UPLINK
Traffic is 0 pps and 0 Kb/s
DOWNLINK
Traffic is 0 pps and 0 Kb/s
Ethernet Total Tx Packets: 3453
Ethernet Total Rx Packets: 6235
Ethernet Total Rx Bytes   : 820390
Ethernet Total Tx Bytes   : -1
Wireless Total Tx Packets: 112
Wireless Total Tx Bytes   : 36736
Wireless Total Rx Bytes   : 0
Wireless Total Rx Packets: 0
Wireless Tx Data Rate     : -1
Wireless Rx Data Rate     : -1
```

Figure 16: Data Statistics

3.4.2 RF STATISTICS

To display the RF Statistics of the CPE, perform the following steps:

1. Enter into the **RF-STAT** Tab field as shown in Figure 17:



SubScriber Station RF Physical Statistics

```
SUBSCRIBER STATION
==================
  DL PREAMBLE PHYSICAL STATISTICS
    Rssi      (dBm)          : -54.75
    RssiStd   (dB)           : -59.55
    Cinr      (dB)           : 33.03
    CinrStd   (dB)           : 25.70
    Cinr     reuse 1  (dB)   : 26.80
    CinrStd  reuse 1(dB)     : 53.59
    Cinr     reuse 3  (dB)   : 33.58
    CinrStd  reuse 3(dB)     : 26.51
Current Downlink FEC Code: QPSK-CTC-1/2
Current Uplink FEC Code   : QPSK-CTC-1/2
Last Tx Power              : -4032
```

Figure 17: RF Statistics

3.4 NETWORK SETTING

3.4.1 WAN

3.4.1.1 NETWORK MODE

To set network mode to be bridge mode, router mode or router mode without DHCP server, perform the following steps:

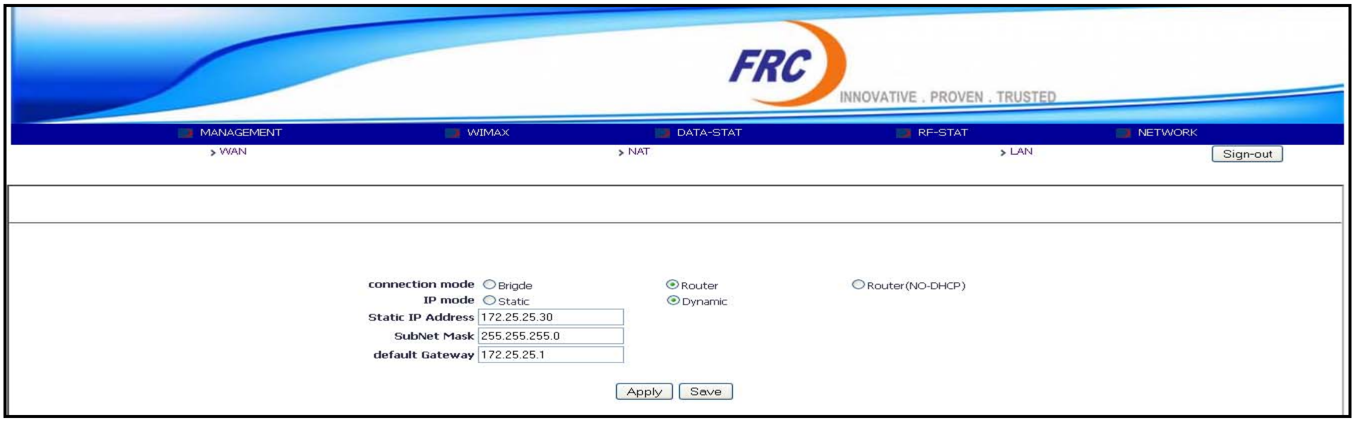
1. Enter into the **Network** Tab field.

2. Select **WAN** field.

3. Specify the required network mode as shown in Figure 18.

4. Click **Apply.**

⚠ Click Save to preserve the network mode after rebooting the CPE.



connection mode ○ Brigde ● Router ○ Router(NO-DHCP)

IP mode ○ Static ● Dynamic

Static IP Address 172.25.25.30

SubNet Mask 255.255.255.0

default Gateway 172.25.25.1

Figure 18: WAN settings.

The available network modules are:

- **Bridge Mode**: if enabled, CPE act as transparent layer two bridge.
- **Router Mode**: if enabled, CPE act as layer three router with enabled DHCP server for LAN.
- **Router Mode(NO-DHCP)**: if enabled, CPE act as layer three router without DHCP server for LAN.

When DHCP Server enabled, CPE automatically assigns IP addresses to computers connected to Ethernet port.

3.4.1.2 IP MODE

By default, the CPE's WAN interface IP mode is automatically configured with IP settings from a Dynamic Host Configuration Protocol (DHCP) server. Alternatively, you can set a static IP address for the WAN interface.

To set WAN interface in static IP mode, perform the following steps:

1. Enter into the **Network** Tab field.

2. Select **WAN** field.

3. Select **Static**.

4. Specify the required **IP Address**, **subnetMask** and **Gateway** settings.

- **IP Address:** Specifies an IP address for wireless interface of the CPE. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. (Default: 172.25.25.30.)
- **Subnet Mask:** Indicates the local subnet mask. (Default: 255.255.255.0)
- **Gateway:** The default gateway is the IP address of the router for the CPE, which is used if the requested destination address is not on the local subnet. (Default: 172.25.25.1)

5. Click **Apply.**

3.4.2 NAT

To enable or disable the NAT setting, perform the following steps:

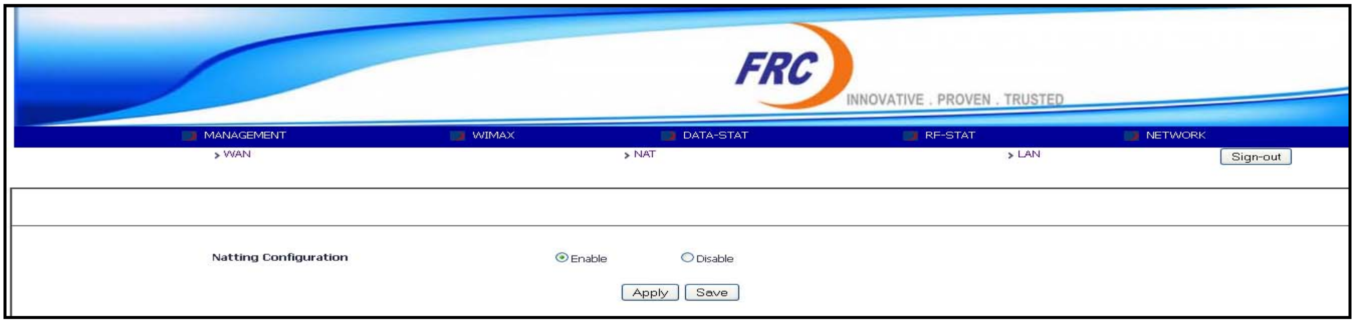
1. Enter into the **Network** Tab field.

2. Select **NAT** field.

3. Select **Enable** or **Disable**.

4. Click **Apply.**

⚠ Click Save to preserve the **NAT setting** after rebooting the CPE.



Natting Configuration ● Enable ○ Disable

Figure 19: NAT setting.

3.4.3 LAN

3.4.3.1 IP SETTING

To set the IP Address for the CPE Ethernet interface, perform the following steps:

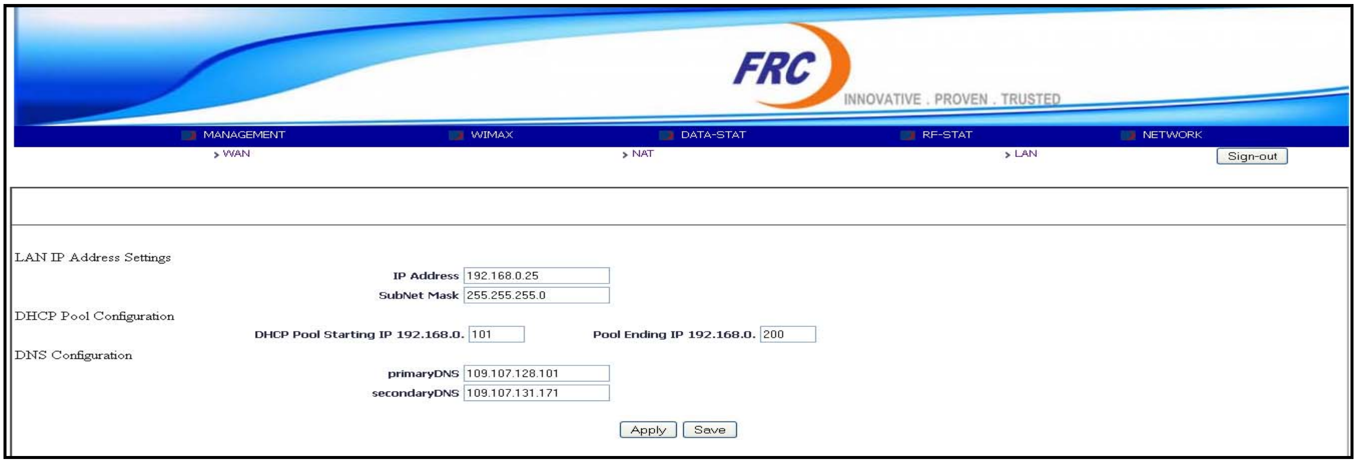
1. Enter into the **Network** Tab field.

2. Select **LAN** field.

3. Specify the **IP Address** and **Subnet Mask** as shown in Figure 19.

4. Click **Apply.**

⚠ Click Save to preserve the **IP Address** after rebooting the CPE.



LAN IP Address Settings

IP Address 192.168.0.25

SubNet Mask 255.255.255.0

DHCP Pool Configuration

DHCP Pool Starting IP 192.168.0. 101 Pool Ending IP 192.168.0. 200

DNS Configuration

primaryDNS 109.107.128.101

secondaryDNS 109.107.131.171

Figure 19: LAN settings.

3.4.3.2 DHCP POOL CONFIGURATION

To set the DHCP pool range for the CPE, perform the following steps:

1. Enter into the **Network** Tab field.

2. Select **LAN** field.

3. Specify the **DHCP Pool Range.**

4. Click **Apply.**

⚠ Click Save to preserve the **DHCP POOL Range** after rebooting the CPE.

⚠ **DHCP Pool Range:** Specifies the start and end of the DHCP server's IP address pool.

3.4.3.3 DNS CONFIGURATION

To set the DNS options for the DHCP server, perform the following steps:

1. Enter into the **Network** Tab field.

2. Select **LAN** field.

3. Specify the **primaryDNS** and **secondaryDNS.**

4. Click **Apply.**

⚠ Click Save to preserve the **DNS Configuration** after rebooting the CPE.

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 airs 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 Router, the person who sets up the Router and makes changes to the settings.

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

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.

CPE Customer Premise Equipment is communications equipment that resides on the customer's premises.

CS Convergence Sublayer.

CSN Connectivity Service Network

DNS Domain Name System is 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.

DHCP Dynamic Host Control 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. Ethernet networks are connected by special cables and hubs, and move data around at up to 10 million bits per second (Mbps).

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

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

Firmware Software stored in a non-volatile memory.

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

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

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

LAN Local Area Network 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 is 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.

MIB Management Information Base.

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

PoE Power over Ethernet is 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.

NAT Network Address Translation is a process that 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 is a method of secure data transmission originally created for dial-up connections; PPPoE is for Ethernet connections.

PPTP Point-to-Point Tunneling Protocol is 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.

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

Subnet Mask A subnet mask 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 / IP Transmission Control Protocol over Internet Protocol is the standard protocol for data transmission over the Internet.

UTP Unshielded twisted-pair cable.

WAN Wide Area Network is a network that connects computers located in geographically separate areas, (i.e., different buildings, cities, countries).

VPN Virtual Private Network.

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.