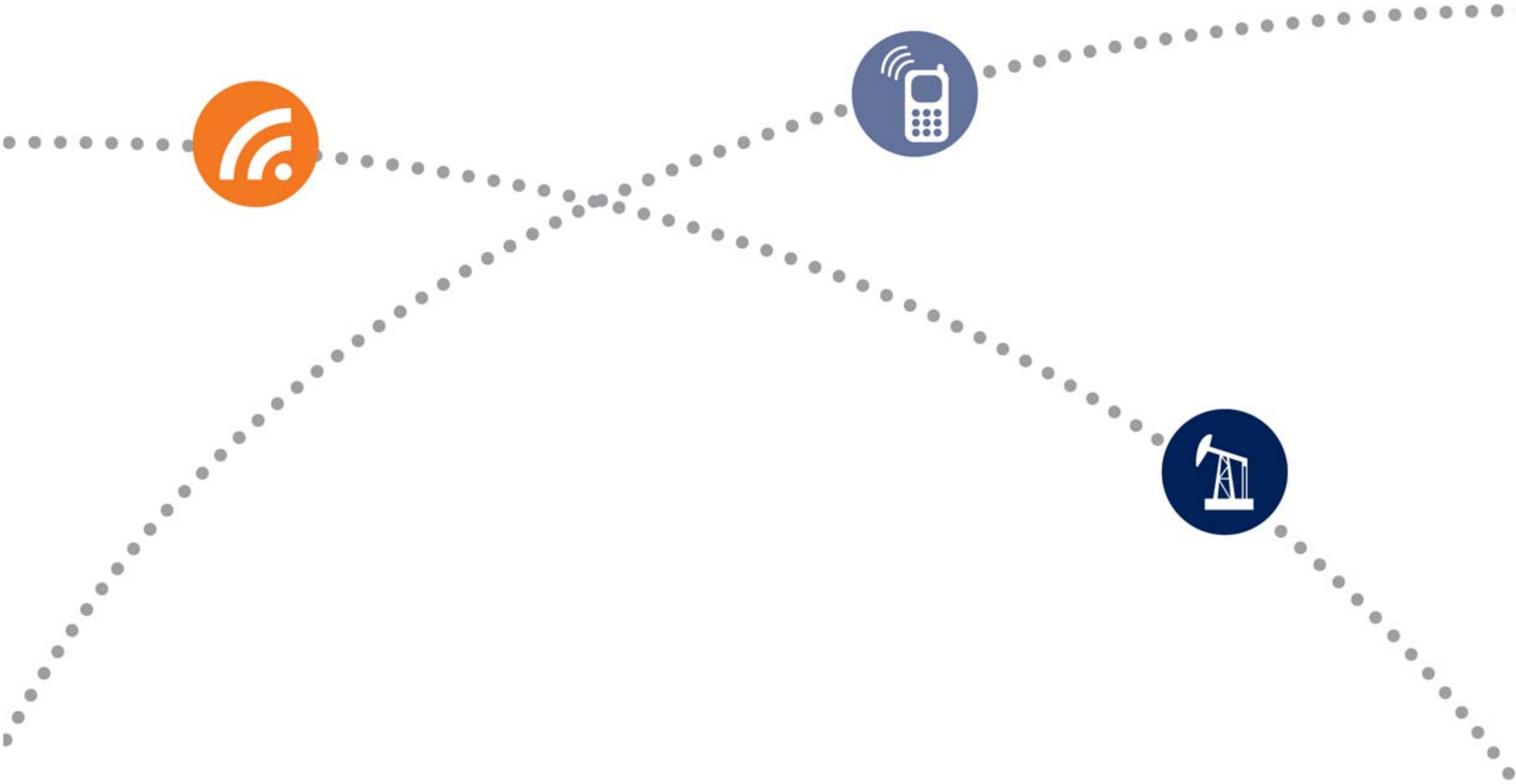


# BreezeMAX® PRO 6000

## Product Manual

Release Number: 1.5
July 2012
P/N 216035

# Document History

| Changed Item | Description | Date |
|---|---|---|
| This is the document's first publication. | | May 2012 |
| Accessing the Web Management Interface<br>Section 3.2.1 | Corrected IP addresses | July 2012 |
| Service Line<br>Section 9.4 | Default for Enable DSCP spoofing is not selected (DSCP spoofing disabled).<br>Certain configuration rules are applicable only when working with DSCP Spoofing enabled. | |

# Legal Rights

The material contained herein is proprietary, privileged, and confidential and owned by Alvarion or its third party licensors. No disclosure thereof shall be made to third parties without the express written permission of Alvarion Ltd.

Alvarion Ltd. 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

Alvarion®, BreezeCOM®, WALKair®, WALKnet®, BreezeNET®, BreezeACCESS®, BreezeMAX®, BreezeLITE®, 4Motion®, and/or other products and/or services referenced here in are either registered trademarks, trademarks or service marks of Alvarion Ltd.

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. Alvarion Ltd. 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 Alvarion Ltd. ("Alvarion") products purchased from Alvarion or through any of Alvarion's authorized resellers are subject to the following warranty and product liability terms and conditions.

## Exclusive Warranty

(a) Alvarion 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 fourteen (14) months from the date of shipment of a given Product to Purchaser (the "Warranty Period"). Alvarion will, at its sole option and as Purchaser's sole remedy, repair or replace any defective Product in accordance with Alvarion' standard R&R procedure.

(b) With respect to the Firmware, Alvarion warrants the correct functionality according to the attached documentation, for a period of fourteen (14) month from invoice date (the "Warranty Period"). During the Warranty Period, Alvarion 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. Alvarion will be obligated to support solely the two (2) most recent Software major releases.

ALVARION 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. ALVARION, ITS AFFILIATES OR ITS LICENSORS MAKE NO WARRANTIES, WHATSOEVER, WHETHER EXPRESS OR IMPLIED, WITH RESPECT TO THE SOFTWARE AND THE ACCOMPANYING DOCUMENTATION. ALVARION 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. ALVARION 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 ALVARION'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. ALVARION' WARRANTIES HEREIN RUN ONLY TO PURCHASER, AND ARE NOT EXTENDED TO ANY THIRD PARTIES. ALVARION 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) ALVARION 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 ALVARION 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).

## Federal Communication Commission (FCC) Interference Statement

This equipment has been tested and found to comply with RSS-192 and 197 of the Industry Canada Rules. This equipment also complies with the limits for a class B digital device, pursuant to ETSI EN 301 489-1 and Part 15 of the FCC 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.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:
(1) This device may not cause harmful interference, and
(2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

## Europe - EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

- EN 60950-1:2006 + A11:2009 + A1:2010 + A12: 2011
- EN 302 326-2 V1.2.2:  2007
- EN 302 326-3 V1.3.1 : 2008
- EN50385 : 2002
- EN 301 489-1 V1.8.1  (2008-04)
- EN 301 489-4 V1.4.1: 2009

## Industry Canada Statement

This device complies with RSS-192 & RSS-197 of the Industry Canada Rules. Operation is subject to the following two conditions:

1) This device may not cause harmful interference, and

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

Ce dispositif est conforme à la norme CNR-192 & CNR-197 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

NOTE!

Radiation Exposure Statement:

This equipment complies with Canada radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 60 cm between the radiator & your body.

Français

Pour l'utilisation de dispositifs mobiles

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 60 cm de distance entre la source de rayonnement et votre corps.

## Safety Considerations - General

For the following safety considerations, “Instrument” means the BreezeMAX units' components and their cables.

## 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.

## 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 Units and Antennas 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, Alvarion is not liable for any injury, damage or regulation violations associated with or caused by installation, grounding or lightning protection.

## Outdoor Units Environmental Evaluation and Exposure Limit

According to FCC part 1, 1.1307, 1.1310:

The limit for power density for general population/uncontrolled exposure is 1(mW/cm$^2$) or 10 (W/m$^2$).

The power density calculation is $S = (Pt*DC /4\pi r^2)$

Where:

- Pt - The average transmitted power (EIRP) (mW)
- r - The distance from the unit. (cm)
- DC -maximum transmitter duty-cycle

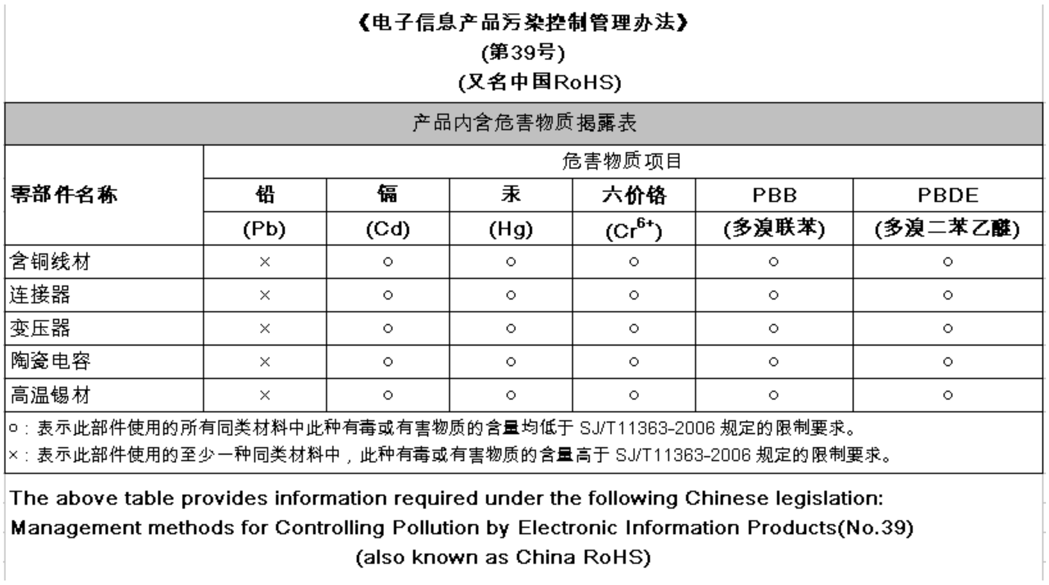
The limit 1(mW/cm$^2$) can be calculated from the above based on the following data:

- Pt- the transmitted power which is equal to the output power 27dBm plus internal antenna gain 15 dBi and 30% Duty-cycle.
- The maximum average EIRP = 36.8 dBm = 4755 mW
- Maximum allowed distance “r”, where RF exposure limit may not be exceeded, = SQRT(4755/4π). This distance is at least 19.45 cm from the antenna (for the installer). For the public this distance is 50 cm.

## Disposal of Electronic and Electrical Waste

**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.



**《电子信息产品污染控制管理办法》**
**(第39号)**
**(又名中国RoHS)**

产品内含危害物质揭露表

| **零部件名称** | 危害物质项目 | | | | | |
|---|---|---|---|---|---|---|
| | **铅** | **镉** | **汞** | **六价铬** | PBB | PBDE |
| | (Pb) | (Cd) | (Hg) | (Cr$^{6+}$) | (多溴联苯) | (多溴二苯乙醚) |
| 含铜线材 | × | ○ | ○ | ○ | ○ | ○ |
| 连接器 | × | ○ | ○ | ○ | ○ | ○ |
| 变压器 | × | ○ | ○ | ○ | ○ | ○ |
| 陶瓷电容 | × | ○ | ○ | ○ | ○ | ○ |
| 高温锡材 | × | ○ | ○ | ○ | ○ | ○ |

○：表示此部件使用的所有同类材料中此种有毒或有害物质的含量均低于 SJ/T11363-2006 规定的限制要求。
×：表示此部件使用的至少一种同类材料中，此种有毒或有害物质的含量高于 SJ/T11363-2006 规定的限制要求。

The above table provides information required under the following Chinese legislation:
Management methods for Controlling Pollution by Electronic Information Products(No.39)
(also known as China RoHS)

# Important Notice

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

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

- 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. Corporate and individual names and data used in examples herein are fictitious unless otherwise noted.

- Alvarion Ltd. 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 Alvarion Ltd. will void equipment warranty and any repair thereafter shall be charged for. It could also void the user's authority to operate the equipment.

# About This Manual

This document describes and explains how to install and manage the BreezeMAX PRO 6000 CPE. .

This document contains the following chapters:

This manual is intended for operators responsible for installing, setting and operating the system, and for system administrators and product experts responsible for managing the system.

This manual contains the following chapters and appendices:

- Chapter 1 -  Product Description - Describes the BreezeMAX PRO 6000 unit and its functionality.
- Chapter 2 -  CPE Installation - Describes how to install the BreezeMAX PRO 6000 and how to connect to subscriber's equipment.
- Chapter 3 - Commissioning - Describes how to initially configure the BreezeMAX PRO 6000 in order to test basic link operation.
- Chapter 4 -  Configuring Setup Parameters - Describes how to configure general parameters of the BreezeMAX PRO 6000.
- Chapter 5 - Configuring Local Address Parameters - Describes how to configure DHCP server and leasing parameters.
- Chapter 6 - Setting Advanced Parameters - Describes how to configure advanced parameters, such as: Authentication, security, Firewall, filters, and port forwarding/triggering parameters.
- Chapter 7 - Displaying Status Details - Describes how to view and understand the device status parameters.
- Chapter 8 -  Configuring Telephony Parameters - Describes how to configure VoIP parameters
- Chapter 9- Engineering (for Operator only)
- Glossary - Terms used in this manual.

# Contents

# Figures

# Tables

# Chapter 1 - Product Description

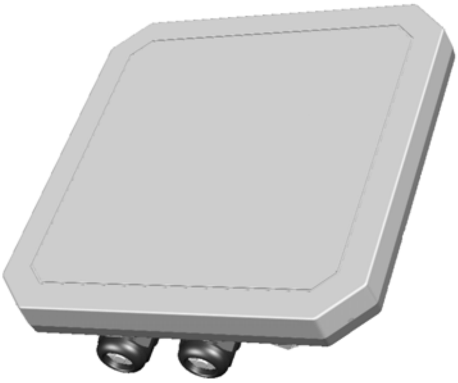
## In This Chapter:

# 1.1 Introducing the BreezeMAX PRO 6000

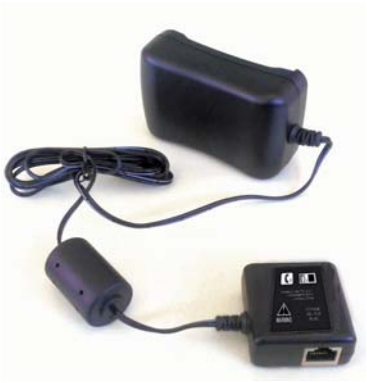
The PRO 6000 CPE comprises an Outdoor Unit (ODU) and an Indoor Unit (IDU).

The ODU includes the modem, radio, data processing, management and voice gateway components of the Subscriber Unit (SU). It also includes an integral high-gain flat antenna. The ODU connects to the IDU and to the user's equipment through a 10/100 BaseT Ethernet port.

The IDU is powered from the mains and connects to the ODU via a Category 5E Ethernet cable carrying the Ethernet data between the two units, as well as power (56 VDC) and control signals to the ODU and status indications from the ODU.



ODU



IDU

**Figure 1-1: BreezeMAX PRO 6000**

# 1.2 BreezeMAX PRO 6000 CPE Specifications

## 1.2.1 General

**Table 1-1: PRO 6000 CPE General Specifications**

| Feature | Description |
|---|---|
| Flash ROM | 32MB |
| Ethernet LAN port | One RJ-45 port<br>10/100 auto-sensing, auto-MDX |
| Channel Step Size | In 250 kHz steps |
| POTS | One RJ-11 |
| Power supply | Input: Universal range 100~240VAC<br>Output: 56 VDC<br>Frequency: 50Hz to 60Hz<br>Current: 0.8A |
| WiMAX SoC | BCS5350 and Dual Core 300MHz |
| RF IC | BCSR-200 / Dual Band 1T/2R RFIC |
| RAM | 64MB |

## 1.2.2 WiMAX Radio

**Table 1-2: PRO 6000 CPE WiMAX Radio Specifications**

| Item | Description |
|---|---|
| Radio Type | IEEE 802.16e 2005 WAVE 2 |
| Frequency Band | 3.3 - 3.7 GHz<br>(range will be increased to 3.3 - 3.8 GHz in future release) |
| Antenna Type | Two WiMAX antennas |
| Channel Bandwidth | 5.00, 7.00, and 10.00 MHz |
| Modulation Technique | ■ Scaleable OFDMA employing Time-Division Duplex (TDD) mechanism<br>■ PRBS subcarrier randomization<br>■ Contains pilot, preamble, and ranging modulation |

Table 1-2: PRO 6000 CPE WiMAX Radio Specifications

| Item | Description |
|---|---|
| FEC Coding Rates | ■ Up Link and Down Link: QPSK, 16 QAM, 64 QAM<br>■ QPSK and 16QAM - 1/2 and 3/4<br>■ 64QAM - 1/2, 2/3, 3/4, 5/6 |
| TPL (Transmit Power Level) | 27 dBm typical (maximum) |
| Channel Step Size | In 250 kHz steps |
| Synchronization | Referenced to the WiMAX BTS Timing Module |
| Frequency Accuracy | MRCT Compliant |
| Air Interface | IEEE 802.16e Wireless MAN-OFDMA |
| TDD Duty Cycle (Tx/Rx) | Rx up to 75% , Tx up to 50% |
| SISO or MIMO | MIMO (1TX, 2RX) |
| Regulatory Compliance | ■ FCC parts 15, 25, 27, 90<br>■ RSS 192, 197 |
| Frame Duration | 5 msec. |
| **RF Transmitter Specifications** | |
| RF dynamic range | 45dB minimum |
| Transmit Power Control Relative Accuracy | mRCT compliant |
| Transmit and Receive Switching Gap | 50 µS |
| **RF Receiver Specifications** | |
| Impedance | 50 ohms nominal |
| Input return loss | 10dBi |
| RX Sensitivity | Typical 3dB better than mRCT in SISO mode, and 6 dB better in MRC or MIMO mode. -94.5 dBm maximum. |
| Adjacent Channel Rejection | 4 dB min.<br>Receive signal 64QAM-3/4, 3dB above sensitivity level. |
| Non-Adjacent Channel Rejection | 23 dB min<br>Receive signal 64QAM-3/4, 3dB above sensitivity level. |
| **Antenna Specifications** | |
| Antenna Gain | Typical 15 dBi |
| Antenna Connectors | None. Embedded IPEX |

## 1.2.3 Power Specification

**Table 1-3: PRO 6000 CPE Power Specification**

| Item | Details |
|---|---|
| Power Consumptions | Outdoor CPE: 16W Maximum |
| Power Adapter | Input of 100 VAC - 240 VAC 50 Hz to 60 Hz |
| Power over Ethernet | 56 VDC |

## 1.2.4 Environmental Specifications

**Table 1-4: PRO 6000 CPE Environmental Specifications**

| Item | Details |
|---|---|
| Operating Temperature | -40°C ~ 60°C |
| Storage Temperature | -40°C ~ 70°C |
| Operating and Storage Humidity | 5% - 95% |

## 1.2.5 Regulatory Specifications

Standards for all frequency bands:

**Table 1-5: PRO 6000 CPE Regulatory Specifications**

| Standard | Specification | Applicable to |
|---|---|---|
| FCC | Part 15 | ODU |
| | Part 90, Subpart Z | |
| ETSI | ETSI EN 302 326 | ODU |
| WiMAX | IEEE-802.16-2005. | ODU |
| Environmental | ETSI 300 019-2-4 Class T4.1E | ODU |
| | ETSI 300 019-2-3 Class T3.2. | PoE (+PS) |
| Transportation & Storage | ETSI 300 019-2-2 Class T2.3.<br>ETSI 300 019-2-1 Class T1.2. | System |
| EU EMC | ETSI EN 301 489-1/4 | System |
| US EMC | FCC part 15 Subpart B (Emission test) | System |
| Immunity | Surge (Lightning protection), ITU-T K.21 | System |

**Table 1-5: PRO 6000 CPE Regulatory Specifications**

| Standard | Specification | Applicable to |
|---|---|---|
| Safety | UL/CUL 60950-1 (USA+Canada) | System |
| | EN60950 (Europe) | |
| | IEC-60950-1 | |
| | AS-3260 (Australia) | |
| Canadian standards | IC RSS-192 – 3450-3650MHz | ODU |
| | SRSP-303.4 Issue 3 - 3475-3650 MHz | |
| | IC RSS-197 - 3650-3700 MHz | |
| | SRSP-303.65 Issue 1 | |
| | ICES-003 - Digital Apparatus | |

## 1.2.6 Reliability Specifications

**Table 1-6: PRO 6000 CPE Reliability Specifications**

| Item | Details |
|---|---|
| MTBF | The MTBF for CPE is not less than 300,000 hours. |

# Chapter 2 - Installation

## In This Chapter:

## 2.1 Installation Requirements

The BreezeMAX PRO 6000 CPE is installed by the operator's installation technicians.

**CAUTION**

ONLY experienced installation professionals who are familiar with local building and safety codes and, wherever applicable, are licensed by the appropriate government regulatory authorities should install outdoor units and antennas.

Failure to do so may void the product warranty and may expose the end user or Service Provider to legal and financial liabilities. Alvarion and its resellers or distributors are not liable for injury, damage or regulation violations associated with the installation of Outdoor Units or antennas.

Français

SEULS les installateurs professionnels expérimentés qui sont familiers avec les codes locaux des bâtiments et de la sécurité et, lorsque cela s'applique, qui sont autorisés par les autorités gouvernementales de régulation, doivent installer les unités extérieures et les antennes. Le non-respect de cette clause peut invalider la garantie du produit et exposer l'utilisateur final ou le prestataire de services à des responsabilités légales et financières. Le fabricant et ses revendeurs ou distributeurs ne sont pas responsables pour toute blessure, dommage ou violation de la réglementation associée à l'installation d'unités extérieures ou d'antennes.

Italiano

ATTENZIONE: SOLO professionisti esperti che hanno familiarità con le norme di costruzione locali e coi codici di sicurezza e, ove applicabile, sono autorizzati dalle autorità governative competenti possono installare unità esterne ed antenne. Assicurarsi che le unità esterne, antenne e strutture di supporto siano installate correttamente per eliminare ogni pericolo fisico a persone o cose. In caso contrario, ciò può invalidare la garanzia del prodotto e può esporre l'utente finale o il fornitore di servizi a responsabilità legali ed economiche. Anche quando la messa a terra non è obbligatoria in base alla normativa regolatoria applicabile e ai codici nazionali, è obbligatorio garantire che l'unità esterna e il palo dell'antenna siano messi a terra e idonei dispositivi di protezione contro i fulmini siano utilizzati in modo da fornire protezione contro le sovratensioni e le scariche statiche. In ogni caso, il Fornitore e i suoi rivenditori non sono responsabili per eventuali danni fisici, danni ad oggetti o violazioni del regolamento associati con o causati dall' installazione, la messa a terra o di protezione contro i fulmini.

### 2.1.1 Package Content

Make sure that each package contains the items listed below:

- BreezeMAX PRO 6000 Outdoor Unit (ODU)
- Indoor power supply unit (IDU) Power Over Ethernet 802.3af compliant
- Crossed Ethernet cable with two RJ-45 connectors for connecting the IDU power injector to a PC/HUB/switch.
- Pole mounting kit
- Optional - Tilt Accessory kit (ordered separately)
- Quick Installation Guide

### 2.1.2 Additional Installation Requirements

- Indoor-to-outdoor Category 5E PoE Ethernet cable with two shielded RJ-45 connectors* and an RJ-45 connectors crimping tool. For details on approved cables and maximum length, refer to Section 2.1.4.

- Mains plug adapter or termination plug (if the power plug on the supplied AC power cord does not fit local power outlets).
- Grounding cable with an appropriate termination
- Sealing gland fastening tool*
- Installation tools and materials
- Sealing materials: mastic tape (Scotchfil™ Electrical Insulation Putty), Cold Shrink sealing kit.

**INFORMATION**

Items marked with an asterisk (*) are available from Alvarion.

## 2.1.3 Guidelines for Positioning the ODU

This section provides guidelines for selecting the optimal installation locations for the ODU.

Select the optimal locations for the equipment using the following guidelines:

- The ODU should be mounted on a 1"- 4" pole. Its location should enable easy access to the unit and its connectors for installation and testing.
- Place the ODU as high as possible to achieve the best possible link quality.
- Place the ODU away from power and telephone lines.
- Avoid placing the ODU too close to any metallic reflective surfaces.
- Be sure to ground the ODU with an appropriate grounding wire (not included) by attaching it to the grounding screw on the unit and to a good ground connection.
- An optional Tilt accessory for the ODU providing a tilt range of ±15° is available from Alvarion. The tilt option might be necessary to either improve the link conditions or, if the ODU is too close to the BTS, to reduce the receive signals strength. As a rule of thumb, if the ODU is located at a distance of less than 300 meters from the BTS, it is recommended to up-tilt the antenna by approximately 10° to 15° (especially in line-of-sight conditions) to avoid saturation of the receivers by too strong signals.

## 2.1.4 IDU-ODU Cables

**INFORMATION**

The length of the Indoor-to-Outdoor cable should not exceed 90 meters. The length of the Indoor-to-Outdoor cable, together with the length of the Ethernet cable connecting the CPE-IDU-1D to the data equipment, should not exceed 100 meters.

Use only Category 5E PoE Ethernet cables from either Alvarion or any of the approved manufacturers, listed in Table 2-1 below. Consult with Alvarion's specialists on the suitability of other cables.

**Table 2-1: Approved Category 5E Ethernet Cables**

| Manufacturer | Part Number |
|---|---|
| UNIXTAR<br>www.unixtar.com.tw | C5ES4P24 |
| WESTERN<br>www.westernwire.org | KF804E1D |

In case of missing information in the manufacturer's WEB site (product specifications, ordering issues, etc.), it is highly recommended to contact the manufacturer's sales representative directly.

# 2.2 Pole Mounting the ODU

## 2.2.1 Pole Mounting the ODU

The ODU can be mounted on a 1" to 4" pole using one of the following options:

- A pole mounting kit is supplied with each unit. The kit includes a special clamp and a pair of threaded rods, flat washers, spring washers and nuts. There are two pairs of threaded holes on the back of the unit, enabling to use the mounting kit for installing the unit using either vertical or horizontal polarization. The clamp enables installing the unit on diverse pole diameters from 1" to 4".
- A Tilt Pole Mounting kit, providing a tilt range of +/-15° is available from Alvarion. The Tilt kit can be attached to the ODU and be mounted on a 1" to 4" pole using two 9/16" wide metal bands.

**To mount the ODU using the clamp:**

1 Thread the M10*100 mm bolt through the M10 spring washer, M10 nut, and the bracket holes.

2 With the connector facing downward, attach the ODU to a 1"- 4" pole.

3 Attach the bracket to the other side of the pole.

4 Thread the M10*100 mm bolts through both holes on either side. Tighten the nuts.

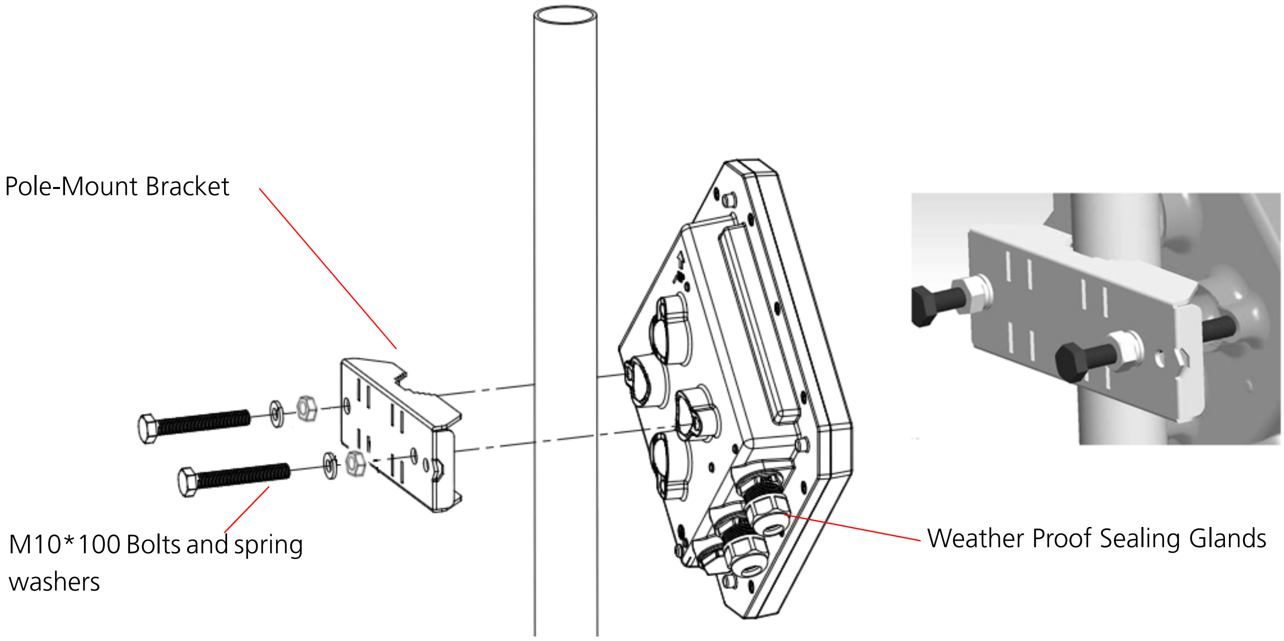

Pole-Mount Bracket
M10*100 Bolts and spring washers
Weather Proof Sealing Glands

**Figure 2-1: Mounting the ODU on the Pole**

### to mount the ODU using the Tilt accessory:

1 Attach the Tilt accessory to the ODU using the two pairs of flat washers, spring washers and nuts supplied in the Tilt kit.

2 Mount the Tilt accessory on a 1" to 4" pole using two 9/16" metal bands.

3 Slightly release the Tilt Control Screw, tilt the ODU downward/upward as required, and re-tighten the screw.

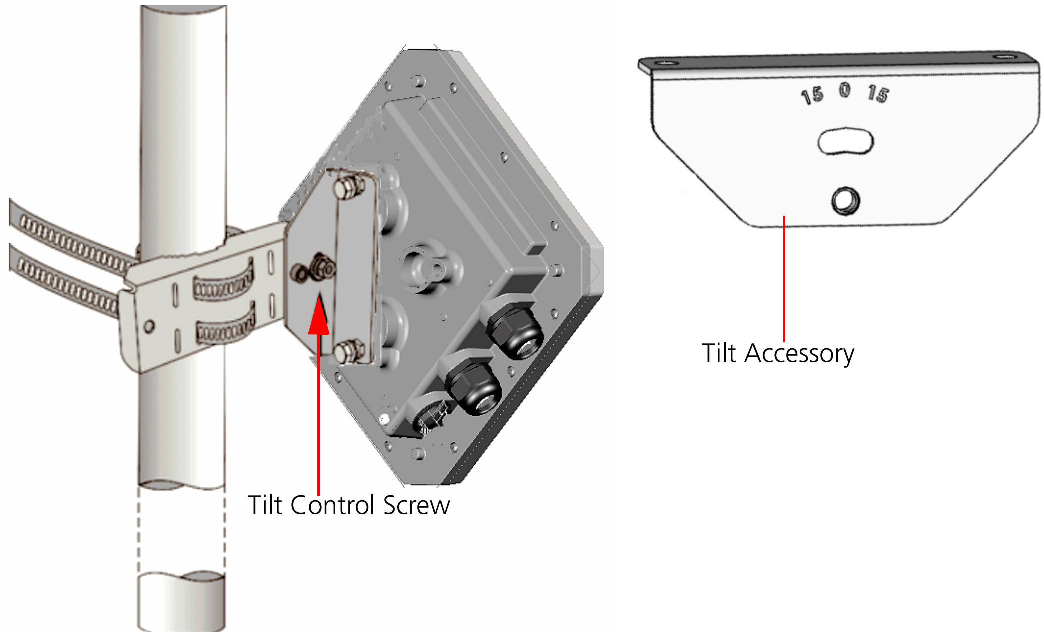


**Figure 2-2: ODU Pole Installation Using the Tilt Accessory, Vertical Polarization**

# 2.3 Connecting the ODU Cables

## 2.3.1 The PRO 6000 CPE Connectors

The PRO 6000 CPE has the following connectors:

- One RJ-45 connector for connecting to the power injector indoor unit (ODU PoE ☎/🖧).
- One Indoor /Outdoor connector (connects to GPS or used for distribution automation) (I / O, currently not applicable)
- A grounding screw on the rear panel.

The following figure illustrates the CPE connections:

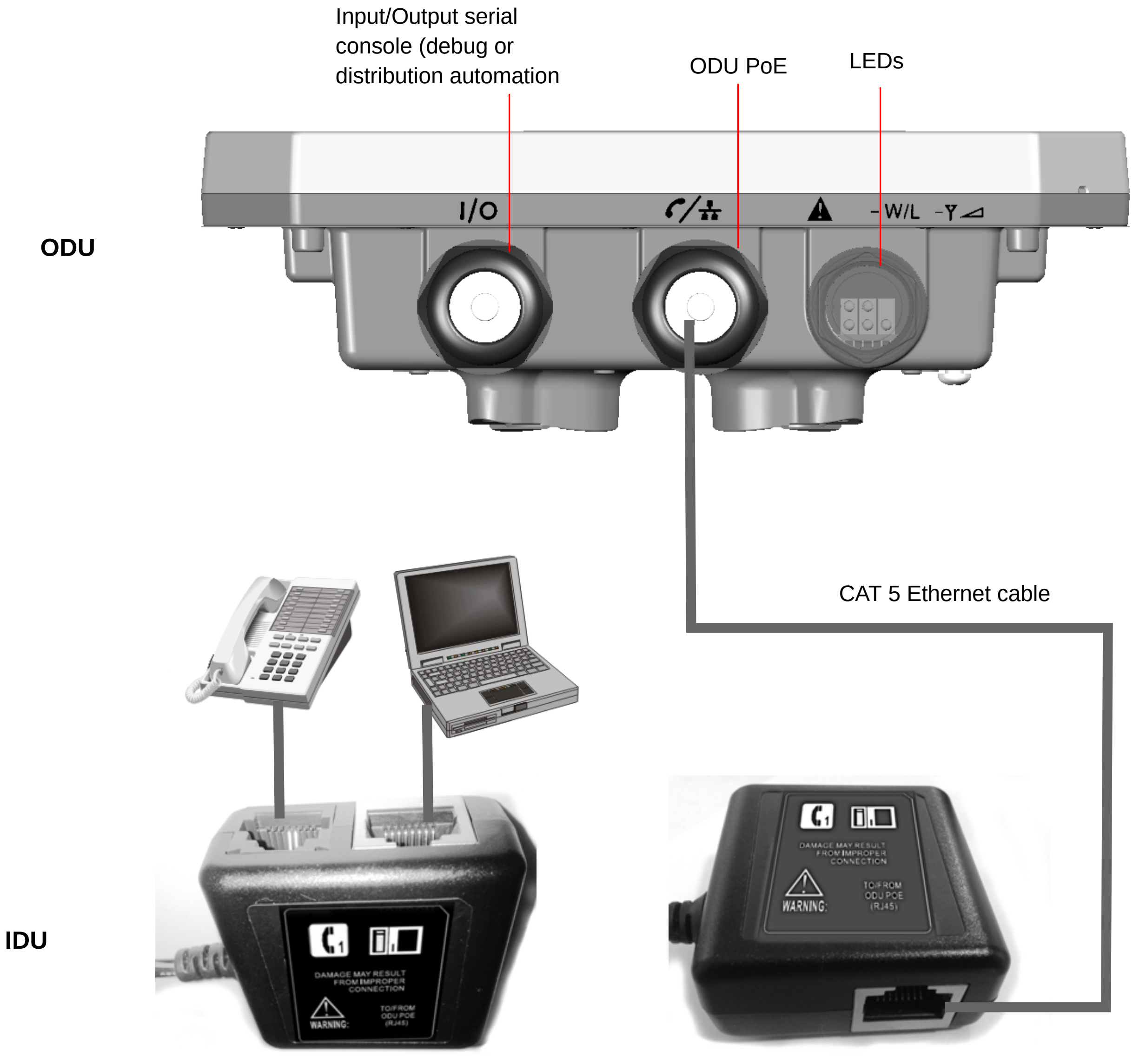

Input/Output serial console (debug or distribution automation
ODU PoE
LEDs
ODU
I/O
W/L
CAT 5 Ethernet cable
IDU
DAMAGE MAY RESULT FROM IMPROPER CONNECTION
WARNING:
TO/FROM ODU POE (RJ45)

Figure 2-3: CPE Connections

## 2.3.2 Connecting the Grounding Cable

The Grounding screw (marked ⏚ ) is located on the rear panel of the ODU.

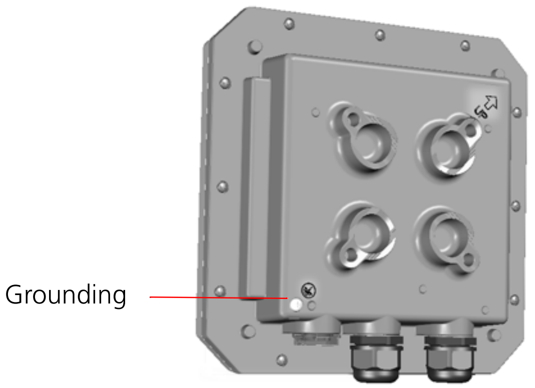


**Figure 2-4: Rear View of the ODU**

**To connect the grounding cable:**

1. Connect one end of a grounding cable to the grounding screw and tighten the grounding screw firmly.
2. Connect the other end of the grounding cable to a good ground (earth) connection.

## 2.3.3 Connecting and Sealing the IDU-ODU PoE Cable

**CAUTION**

Use only Category 5E 4x2x24# FTP outdoor cables from an approved manufacturer. See list of approved cables in Table 2-1.The length of the Indoor-to-Outdoor cable should not exceed 90 meters. The length of the Indoor-to-Outdoor cable, together with the length of the Ethernet cable connecting the IDU to the data equipment, should not exceed 100 meters.

**To prepare the IDU-ODU cable:**

Use a crimp tool for RJ-45 connectors to prepare the wires. Insert them into the appropriate pins and use the tool to crimp the connector. Make sure to do the following:

- Remove as small a length as possible of the external jacket. Verify that the external jacket is well inside the sealing cover when connected to the unit, to ensure good sealing.
- Pull back the shield drain wire before inserting the cable into the RJ-45 connector to ensure a good connection with the connector's shield after crimping.

The IDU-ODU cable provides pin-to-pin connection on both ends.

The following figure shows the required wire pair connections. The color codes used in standard cables supplied by Alvarion are as listed in the table.

| Wire color | Pin |
|---|---|
| Blue | 1 |
| Blue/white | 2 |
| Orange | 3 |
| Orange/white | 6 |
| Brown | 4 |
| Brown/white | 5 |
| Green | 7 |
| Green/white | 8 |

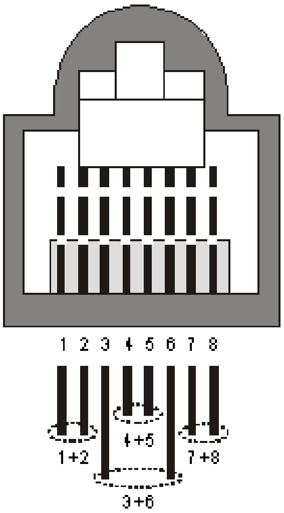


Figure 2-5: Ethernet Connector Pin Assignments

### To connect and seal the IDU-ODU cable:

1 Remove the sealing gland plug from the gland nut.

2 Open the sealing gland nut and remove it. *Do not* disassemble the gland base from the bracket.

3 Insert the cable into the sealing gland base and connect it to the RJ-45 connector at the bottom of the CPE, labeled ☎/🖧. Make sure that the connector is completely inserted and tightened.

4 Insert the rubber bushing on the cable into the gland base.

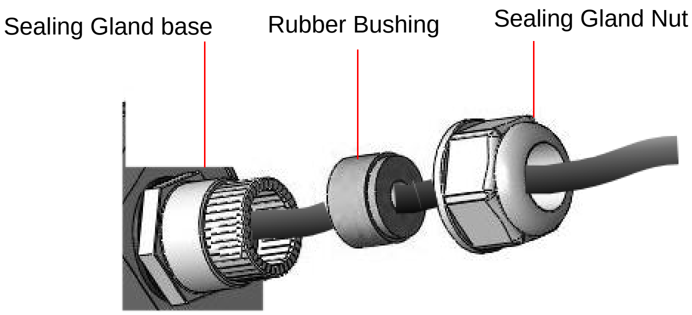


Figure 2-6: Inserting the Cable into the Sealing Cap

5 Tighten the gland nut. Use the dedicated tool for fastening the sealing glands.

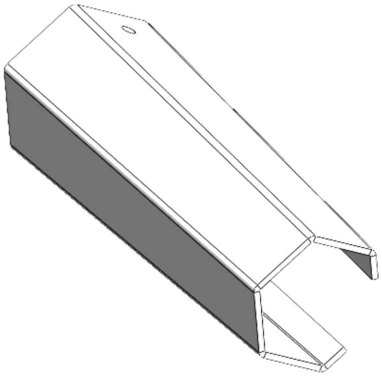


**Figure 2-7: Sealing Gland Fastening Tool**

6 Attach the mastic tape (Scotchfil™ Electrical Insulation Putty) and wrap it around the connector butting up against the connector. Do not over stretch.

7 Squeeze to tighten the mastic sealer. Make sure there are no air bubbles.

8 Slide the cold shrink sleeve on top of the connector. Make sure that the sleeve covers both cable connector and unit connector.

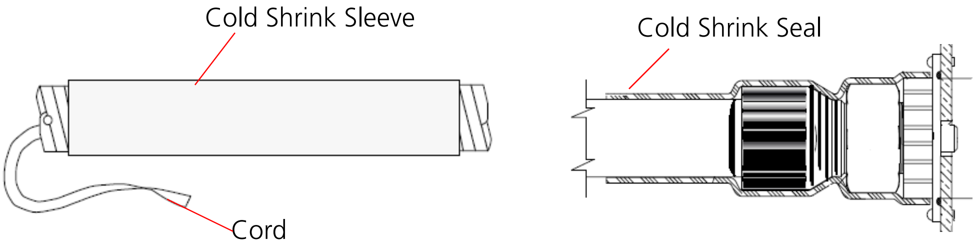


**Figure 2-8: Cold Shrink Tubing**

9 Pull the cord slowly to shrink the sleeve.

10 Route the cable to the location selected for the indoor equipment.

11 Assemble an RJ-45 connector with a protective cover on the indoor end of the IDU-ODU cable. Refer to the pin assignment and color codes in standard cables described above.

## 2.3.4 Installing the Power Injector IDU

The unit can be placed on a desktop or a shelf, or it may be wall-mounted.

**INFORMATION**

The length of the Ethernet cable connecting CPE to the user's equipment, together with the length of the IDU-ODU cable, should not exceed 100 meters.

### To install and connect the Power Injector IDU:

1 It is assumed that the IDU-ODU cable is already connected to the ODU. Assemble an RJ-45 connector with a protective cover on the indoor end of the IDU-ODU cable. Refer to Section 2.3.3 for instructions on preparing the cable.

2 Connect the IDU-ODU cable to the single port, labled “TO/FROM ODU PoE (RJ45)” (Figure 2-9).

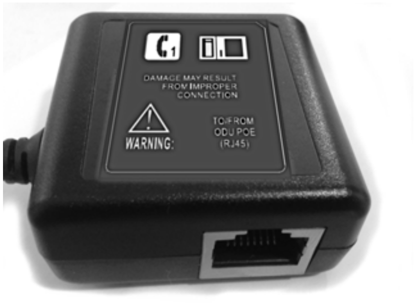


**Figure 2-9: IDU-ODU PoE port (“TO/FROM ODU PoE (RJ45)”)**

3 Connect one end of the supplied Ethernet cable to a PC/Hub/Switch.

4 Connect the other end of the Ethernet cable to the RJ-45 IDU port, labled with a computer illustration (see Figure 2-10).

5 Use a telephone cable to connect a phone to the RJ-11 IDU port labled with a telephone illustration (see Figure 2-10).

6 Connect the indoor unit to the AC mains using the power cable supplied with the unit.

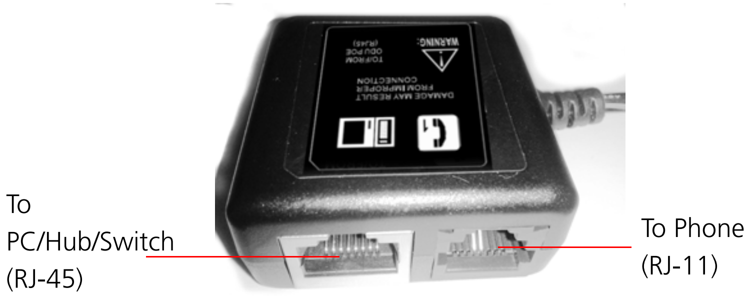


**Figure 2-10: Data Equipment and Telephone Ports**

CAUTION

Do *not* connect the data equipment to the PoE port on the IDU, as it supplies DC power to the ODU, and this may harm other equipment connected to it.

# 2.4 Checking for Proper Operation

1 Verify data connectivity by sending a ping command to the BTS or by connecting to the Internet.

2 Check the LED functionality according to the following table:

**Table 2-2: LED Functionality**

| Description | Color | Functionality |
|---|---|---|
| Fault + Eth indication LED | Red | ■ Lights at start up<br>■ During the built-in test (BIT) blinks (300ms on, 300ms off).<br>■ Off/On - If BIT finished successfully. If BIT is failed it will continue lightning.<br>■ On - If fatal error/critical alarm appears during run time.<br>■ Blinking - If PoE Eth connected and no errors found (1sec on, 3sec off). |
| WiMax W/L link availability LED | Green | ■ Lights at start up<br>■ Off - upon BIT completion<br>■ Blinking - the CPE is synchronized to the BS and 5>SNR ≥ 3dB.<br>■ On - when the CPE is synchronized to the BS and the SNR ≥ 5dB |
| 3 x WiMax link signal strength LEDs | Green | ■ Lights at start up.<br>■ Off - upon BIT completion<br>Signal strength display:<br>■ LED1 blinks when 12>SNR≥8dB<br>■ LED1 lights when SNR≥12dB<br>■ LED2 blinks when 18>SNR≥15dB<br>■ LED 2 lights when SNR≥18dB<br>■ LED3 (right side) blinks when 25>SNR≥20dB<br>■ LED3 (right side) lights when SNR≥25dB |

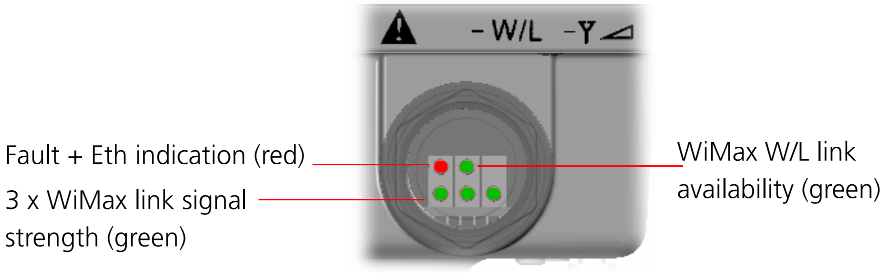

- W/L
Fault + Eth indication (red)
3 x WiMax link signal strength (green)
WiMax W/L link availability (green)

**Figure 2-11: LEDs**

# Chapter 3 - Commissioning

## In This Chapter:

# 3.1 Introduction

After completing the installation process, as described in the preceding chapter, several actions should be performed to ensure connectivity with a base station (BS) and provisioning of services. After the subscriber unit is connected with a BS, it can be fully managed via the wireless link:

1. The basic parameters must be configured to ensure that the unit operates correctly and can communicate with a BS.
2. Proper operation should be verified, including data connectivity.
3. The unit must be positioned correctly to ensure optimal performance of the wireless link.

The following methods are available for configuring the unit:

- The web-based management interface - accessed using a PC/Notebook with a web browser (see "Configuring the Unit Using the Web Management Interface" on page 23).
- An automatic configuration tool provided on a CDROM for the subscribers (see "Configuring the Unit Using the WiMAX Modem Application CD" on page 26).
- Upgrading the CPE using an auto-configuration file, or IPKG (in *.ipk format) (see "Configuring the CPE Using the IPKG Upgrade" on page 30).

The device may be delivered with the operator's default settings already configured in the FLASH memory.

The following parameters must be configured in order for a link to be established.

**Table 3-1: Basic Parameters**

| Item | Default Value | Comment |
|---|---|---|
| User Name (WiMAX) | WAN mac address and WiMax.com realm, e.g: 0026824EE12C@WiMax.com | Should be supplied by system administrator. Configured in the Advanced> Authentication window |
| WiMAX Password | quickynikynyoky | |
| Domain | wimax.com<br>(also Eng > WiMAX Config > Realm) | |
| Frequency | Full Scan | Should be supplied by system administrator. |
| Telephony - SIP Server, phone number, authentication, enable the phone | Disabled | Optional<br>VoIP is disabled by default and should be enabled by the operator |
| WiFi | Enabled | Enabled by default |

# 3.2 Configuring the Unit Using the Web Management Interface

The BreezeMAX PRO 6000 supports multi-user permissions: Operator and Subscriber modes are available by downloading different configuration files (IPKGs) from the web and upgrading the unit. Each level has different permissions to access various pages for configuration.

## 3.2.1 Accessing the Web Management Interface

By default, the BreezeMAX PRO 6000 enables a DHCP server and computers, or network devices connected to a LAN port, to automatically get an IP address from the unit. If the unit's DHCP server is disabled, you can set in the PC the IP address, netmask, and gateway manually using the following values:

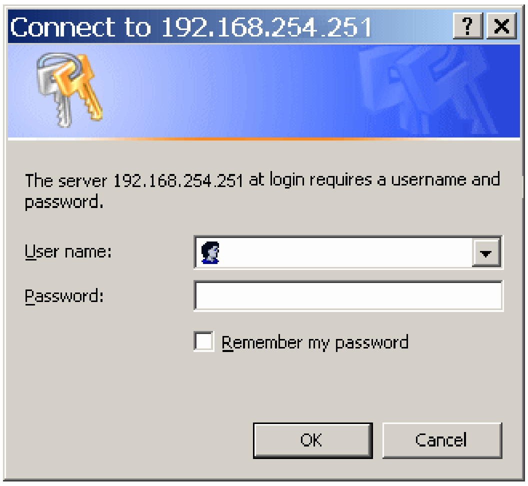
IP address: 192.168.254.x ( (1 ≤ x ≤ 253, excluding 251)

Netmask: 255.255.255.0

Gateway: 192.168.254.251

**To log in:**

1 Open a web browser and enter the Gateway IP address: http://192.168.254.251. The web browser displays the login page.



The server 192.168.254.251 at login requires a username and password.

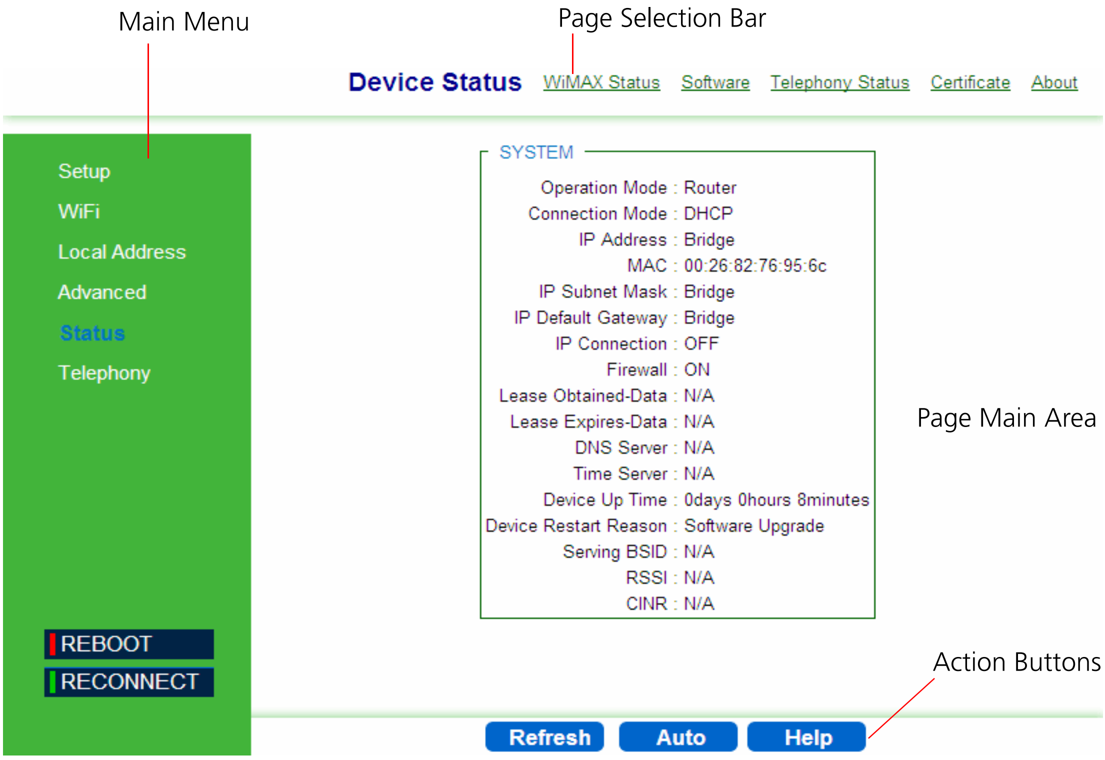
**Figure 3-1: Login Window**

2 Enter the user name and password, and click **Login**.

The system supports multi-level user login: Operator and Subscriber, and Debug modes are available. Each level has different permissions to access various pages for configuration.

- Subscriber:
  - Username: admin
  - Password: admin
- Operator:
  - Username: operator
  - Password: wimax

After successful login, the Status - Device Status page is displayed.



SYSTEM

Operation Mode : Router
Connection Mode : DHCP
IP Address : Bridge
MAC : 00:26:82:76:95:6c
IP Subnet Mask : Bridge
IP Default Gateway : Bridge
IP Connection : OFF
Firewall : ON
Lease Obtained-Data : N/A
Lease Expires-Data : N/A
DNS Server : N/A
Time Server : N/A
Device Up Time : 0days 0hours 8minutes
Device Restart Reason : Software Upgrade
Serving BSID : N/A
RSSI : N/A
CINR : N/A

**Figure 3-2: Main Window (Device Status)**

The Web Management Interface consists of a number of menu links (to the left). Clicking on each of them will display the configuration/status page for the selected menu item, with the applicable content (configurable parameters/options or status information) in the main area. Several pages include a page selection bar at the top of the page, enabling selection between several pages related to the same menu item. The displayed pages may vary depending on user privileges.

Use the Main Menu items and the specific sub-items in the menu-bar at the top of the window to configure settings for the current operating mode. The menus and configuration steps are described in the next chapters of this manual.

In Operator mode only, additional parameters are available in the Engineering menu item, for more detailed configuration. The Engineering features are available in a software package, and can only be activated after uploading it to the system from the Status page See "Software Status" on page 72.

## 3.2.2 Applying Changes and Using Help

There are common buttons that appear in most of the interface pages. Use these buttons as follows:

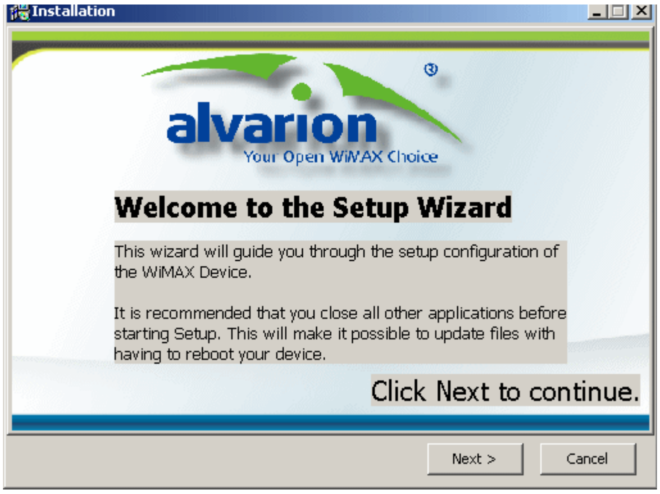
- **Apply** - Click this button to save the changes you have made in each page of the device system. For changes that require device reset, the device will automatically initiate reset after clicking the Apply button.
- **Undo** - Click this button to clear the input data in the specific window.
- **Reboot** - Click this button to restart your unit. The device returns to the last applied settings.
- **Reconnect** - Click this button to attempt reconnecting the device to the Base Station. This step is normally not required, unless suspecting that connection is problematic.
- **Help** - Click this button to open context-sensitive on-line help.

# 3.3 Configuring the Unit Using the WiMAX Modem Application CD

This section explains how to use the automatic configuration tool, delivered on a CDROM with the unit, to automatically configure a CPE. This procedure is usually performed by the subscriber.

**To configure the unit using the Auto-Configuration tool:**

1 From the CDROM supplied with the unit, run the CPE Auto Configuration Tool: CPEAutoConfigTool.exe; The Installation Setup Wizard window is displayed.



Welcome to the Setup Wizard

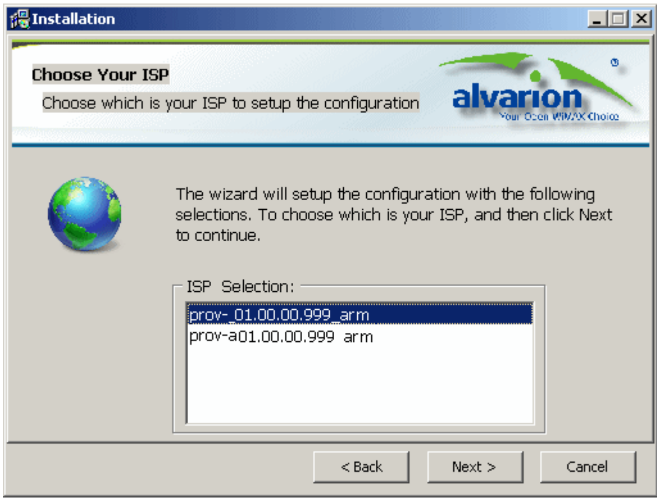
This wizard will guide you through the setup configuration of the WiMAX Device.

It is recommended that you close all other applications before starting Setup. This will make it possible to update files with having to reboot your device.

Click Next to continue.

**Figure 3-3: Installation Setup Wizard Window**

2 Click **Next** to continue; The Choose Your ISP window is displayed.



**Choose Your ISP**

Choose which is your ISP to setup the configuration

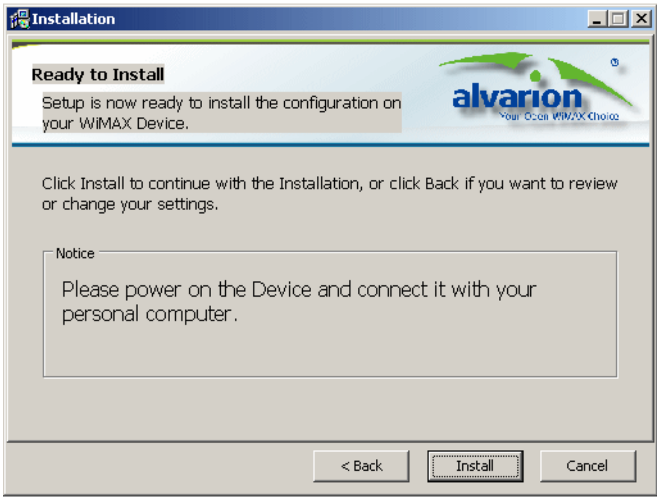
The wizard will setup the configuration with the following selections. To choose which is your ISP, and then click Next to continue.

ISP Selection:

- prov-_01.00.00.999_arm
- prov-a01.00.00.999 arm

Figure 3-4: Choose Your ISP Window

3 Choose the ISP (Internet Service Provider) ConfigFile from the list and click **Next**. The Ready To Install window is displayed.



**Ready to Install**

Setup is now ready to install the configuration on your WiMAX Device.

Click Install to continue with the Installation, or click Back if you want to review or change your settings.

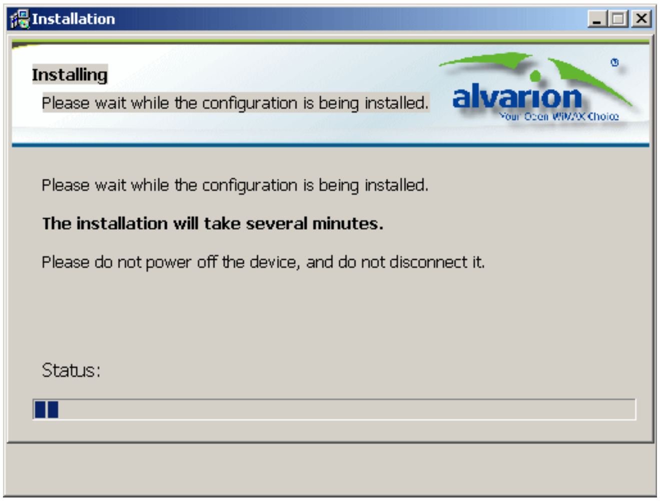
Notice

Please power on the Device and connect it with your personal computer.

Figure 3-5: Ready To Install Window

4 Click **Install**. If your CPE is powered up, click **OK** for performing system reboot. If not, power on the CPE and click **OK**.

The tool starts the auto-configuration process of the unit settings. It will change default settings by using the *.ipk file, and then run “reset to factory default” by using default configuration in the file.



Installing

Please wait while the configuration is being installed.

Please wait while the configuration is being installed.

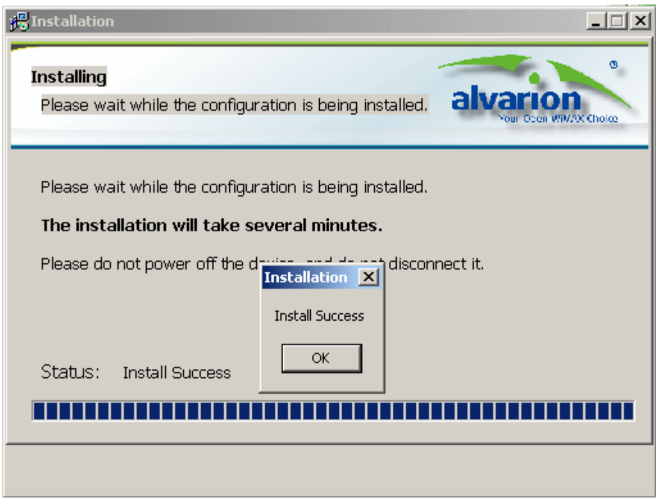
**The installation will take several minutes.**

Please do not power off the device, and do not disconnect it.

Status:

**Figure 3-6: Installing Window**

**5** When the installation is complete, an Installation Success window is displayed. Click **OK**.



Installing

Please wait while the configuration is being installed.

Please wait while the configuration is being installed.

**The installation will take several minutes.**

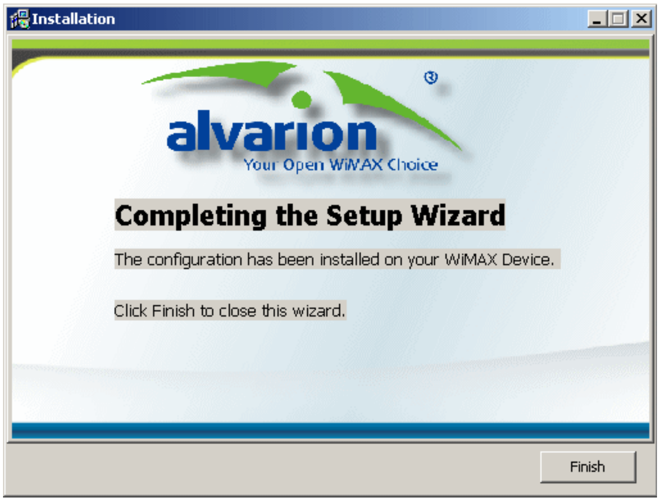
Please do not power off the device, and do not disconnect it.

Install Success

Status: Install Success

**Figure 3-7: Installation Succeeded**

**6** Click **Finish**. The CPE is now configured with the parameters from the ConfigFile.



Completing the Setup Wizard

The configuration has been installed on your WiMAX Device.

Click Finish to close this wizard.

Figure 3-8: Installation Complete

# 3.4 Configuring the CPE Using the IPKG Upgrade

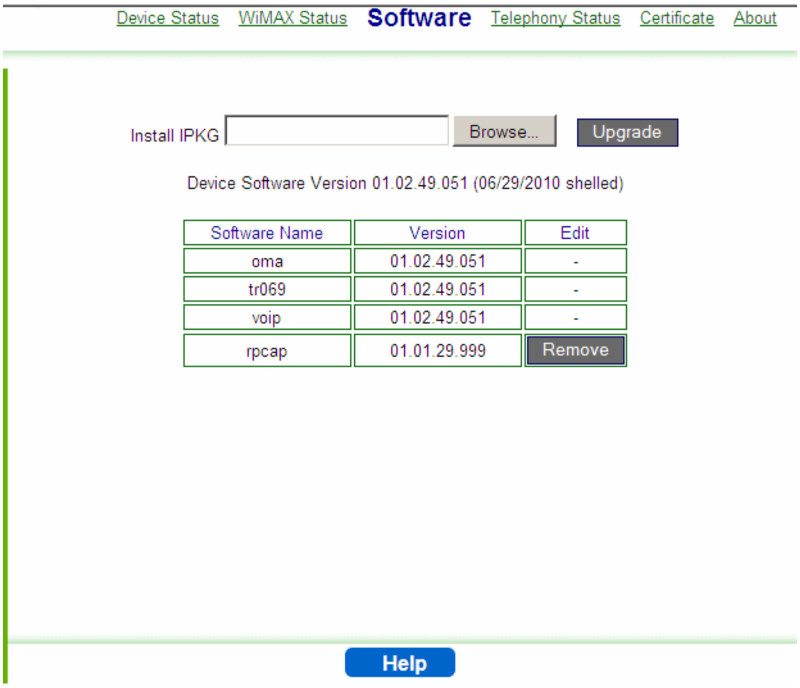
This section explains how to use the IPKG (ITSY Package Management System), provided by the operator, to automatically configure a CPE and sometimes upgrade its features. Subscribers should use this procedure upon specific instruction from the operator.

**To upgrade the unit using the IPKG:**

1 From the main menu at the left pane select **Status** and open the **Software** page (Figure 3-9).

2 Click **Browse** to upload the *ipk  file provided for this unit.

3 Click **Upgrade** to apply all the parameters in the IPKG file to this unit.



Device Software Version 01.02.49.051 (06/29/2010 shelled)

| Software Name | Version | Edit |
|---|---|---|
| oma | 01.02.49.051 | - |
| tr069 | 01.02.49.051 | - |
| voip | 01.02.49.051 | - |
| rpcap | 01.01.29.999 | Remove |

**Figure 3-9: Status - Software Page**

# 3.5 Creating a Default Configuration File

This section explains how to create a default configuration file (*.ipk) for automatic configuration. When applying this file to CPEs, all the parameters will automatically be configured with the values from the file. When resetting the unit to factory defaults - this file is reloaded, overriding any configuration changes you may have performed on the CPE.

Creating a configuration file involves converting a *.tar file into an *.ipk file.

When the *.ipk file is ready, copy it onto a CDROM along with the subscriber documentation and include it in the CPE package.

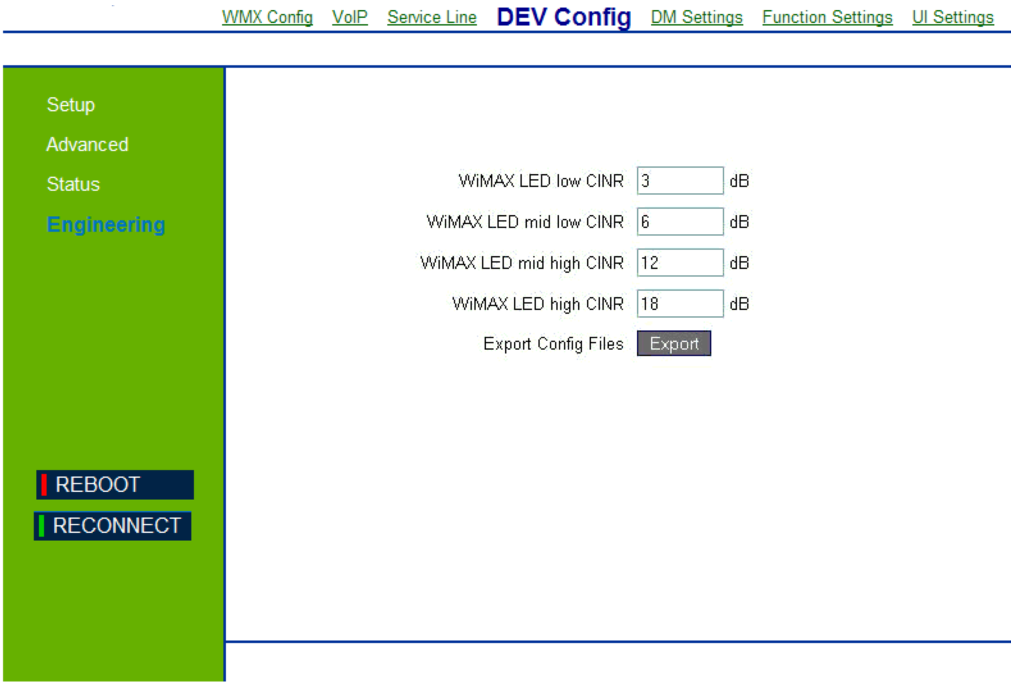
**To create a configuration *.**tar **file:**

1 Choose a CPE from which to create the default configuration file.

2 Configure the settings of the CPE as described in this manual.

3 Select **Engineering** from the main menu and open the **Dev Config** page (Figure 3-10).

4 Click **Export**. A *.tar file is created and you can save it for later auto-configuration of additional CPEs.



WiMAX LED low CINR 3 dB

WiMAX LED mid low CINR 6 dB

WiMAX LED mid high CINR 12 dB

WiMAX LED high CINR 18 dB

Export Config Files Export

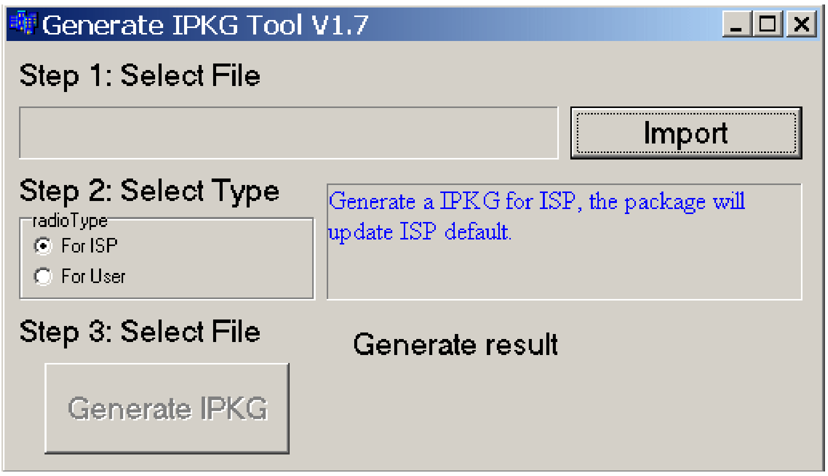
Figure 3-10: Engineering - Dev Config Page

### To generate an ipk file:

1 Create a new folder and copy the following files into it:

- » Generate_Provision_V2.0.rar (provided on a CDROM)
- » The *.tar file created previously.

2 Extract the Generate_Provision_V2.0.rar and run the CPE Auto Configuration Tool: generate_provision_2.0exe; The Generate IPKG Tool window is displayed.



radioType
● For ISP
○ For User

Generate a IPKG for ISP, the package will update ISP default.

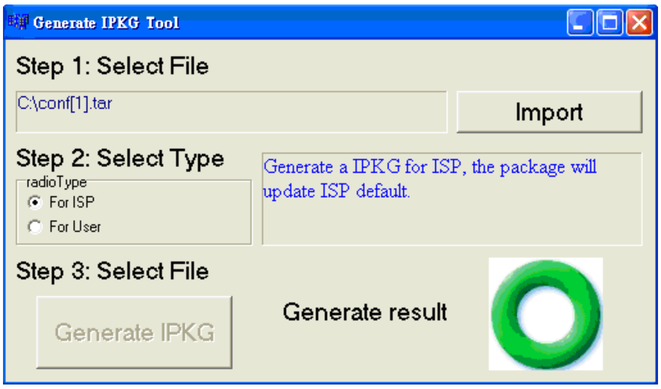
**Figure 3-11: Generate IPKG Tool**

3 Click **Import** and select the tar file you created  previously.

4 Select the type of IPKG to generate:

- » For Internet Service Provider (ISP) - the package will override the default configuration file.
- » For User - the package will update the local subscriber configuration file only.

5 Click **Generate IPKG** and save the file as .*ipk file. A green circle  appears next to “Generate result” at the end of the ipk generation process.



Generate IPKG Tool

Step 1: Select File

C:\conf[1].tar

Step 2: Select Type

radioType

● For ISP

○ For User

Generate a IPKG for ISP, the package will update ISP default.

Step 3: Select File

Generate result

Figure 3-12: Generation Results

6 Use the ipkg file to configure CPEs, and/or include it in a CDROM for the subscriber.

# 3.6 Operation Verification

To verify proper operation of the unit, examine the LED indicators on the front panel.

To verify data connectivity, from the end-user's PC or from a portable PC connected to the unit, ping a known device in the network, or connect to a known internet site (e.g www.Alvarion.com). This site can be reached by clicking the Alvarion logo on the top of any page in the GUI.

Operation can also be verified from Web GUI (Status > Device Status page, see Figure 3-2)

# Chapter 4 - Configuring Setup Parameters

## In This Chapter:

# 4.1 Introduction

The BreezeMAX PRO 6000’s Setup menu allows you to implement general management functions for the unit, including setting connection modes, the system time zone, configuring the device name and access password, and restore settings to factory defaults.

INFORMATION

You can use the web browser interface to access the WAN IP address only if the unit already has an IP address that is reachable through your network.

The default LAN IP address of the BreezeMAX PRO 6000 is 192.168.254.251. The unit operates by default in DHCP mode.

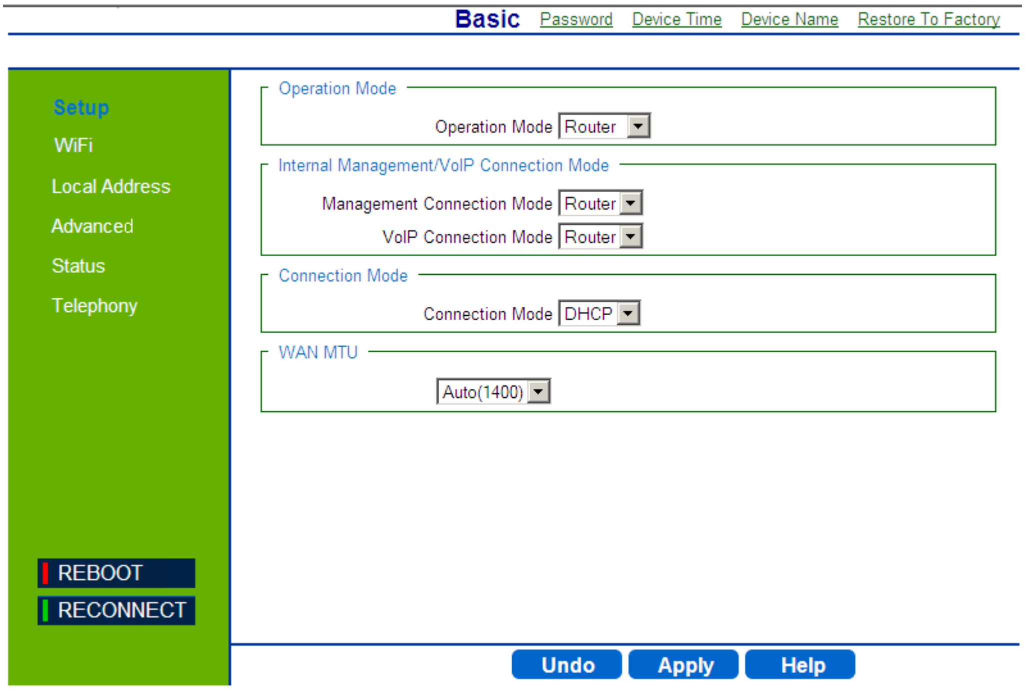
When you make a configuration change in the Setup pages, the following message is displayed after clicking Apply: “Configuration setting”. After the configuration is applied, a “Prepare for Reboot” message is displayed. The system performs a reboot and counts 60 seconds.

When applying Factory Defaults, a "Restore to factory default settings" message appears and then a Rebooting message and 60 seconds countdown are displayed.

# 4.2 Setting Basic Parameters

The Basic Setup allows you to configure the main system parameters.

**NOTE!** Do not change parameters in this page unless specifically instructed by your service provider. Doing so may cause your internet/VoIP connection to fail, and you will need to reset the unit to default parameter values.



Operation Mode

Operation Mode: Router

Internal Management/VoIP Connection Mode

Management Connection Mode: Router

VoIP Connection Mode: Router

Connection Mode

Connection Mode: DHCP

WAN MTU

Auto(1400)

**Figure 4-1: Setup - Basic Parameters**

The following table describes the configurable Basic parameters:

**Table 4-1: Basic Parameters**

| Parameter | Description | Default | Possible Values |
|---|---|---|---|
| **Operation Mode** | | | |
| Operation Mode | Specifies the mode for forwarding data packets from the service provider's WiMAX network to the local network. | Router | ■ Router (the only option, unless differently configured by Alvarion)<br>■ Bridge IPCS<br>■ Bridge ETHCS |

**Table 4-1: Basic Parameters (Continued)**

| Parameter | Description | Default | Possible Values |
|---|---|---|---|
| **Internal Management/VoIP Connection Mode** | | | |
| Management Connection Mode | Sets the forwarding mode for sending management packets to the WiMAX network:<br>■ Bridge mode - forwards packets based on Layer 2 MAC addresses. Bridge mode means that management connection has a different IP than data connection. This IP is used for communication with the management server, for web access from WAN, ping, etc.<br>■ Router mode - forwards packets based on Layer 3 IP addresses. Uses data interface for Management communication. | Router | ■ Bridge<br>■ Router |
| VoIP Connection Mode | Sets the forwarding mode for sending VoIP packets to the WiMAX network:<br>■ Bridge mode forwards packets based on Layer 2 MAC addresses. Bridge mode means that voice connection has a different IP than data or management connections. This IP is used only for SIP/RTCP and RTP messages sent and received by the device’s POTS (plain old telephone service) lines.<br>■ Router mode forwards packets based on Layer 3 IP addresses. Uses data interface for VoIP communication.<br>■ None - No forwarding. VoIP interface is not available. | Router | ■ Bridge<br>■ Router<br>■ None |

**Table 4-1: Basic Parameters (Continued)**

| Parameter | Description | Default | Possible Values |
|---|---|---|---|
| **Connection Mode** | | | |
| Connection Mode | Sets the connection type for the unit:<br>■ DHCP - The system will assign IP addresses to the unit on the wide area network (WAN).<br>■ Static - The IP address is predefined and fixed. When you select this option, new menu items are displayed for configuration:<br>» WAN IP Address<br>» WAN Subnet Mask<br>» WAN Gateway Address<br>» DNS1- Domain Name System<br>» DNS2 | DHCP | ■ DHCP<br>■ Static |
| **WAN MTU** | | | |
| WAN MTU | Sets the WAN maximum transmission unit (MTU) size in bytes<br>■ Auto (1400) - transmission unit size is 1400 (maximum) bytes<br>■ Manual - enter the value for transmission unit size (Range: 576-1500) | Auto (1400) | ■ Auto (1400)<br>■ Manual |

**INFORMATION**

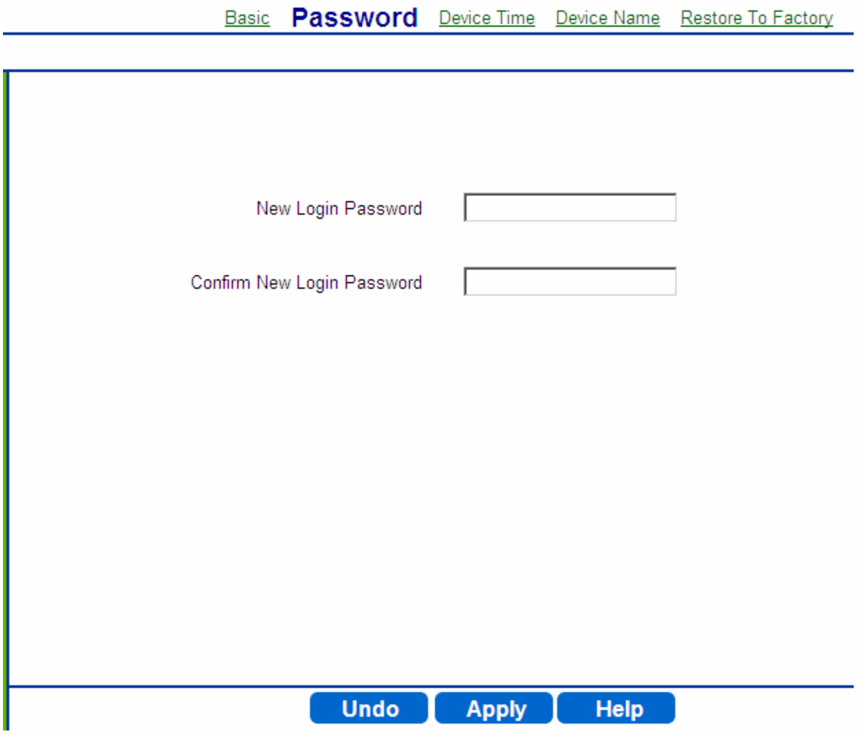
Static IP is not supported by 4Motion equipment.

## 4.3 Setting Password

The Password page enables you to change the default password for remote and local access to the Graphical User Interface (GUI).

**INFORMATION** It is strongly recommended that you configure your own password. If a password is not configured, the management interface is not protected and your network security may be compromised since the default password is not secure.

Keep a record of the password in a safe place, in case you will need to restore it.



New Login Password

Confirm New Login Password

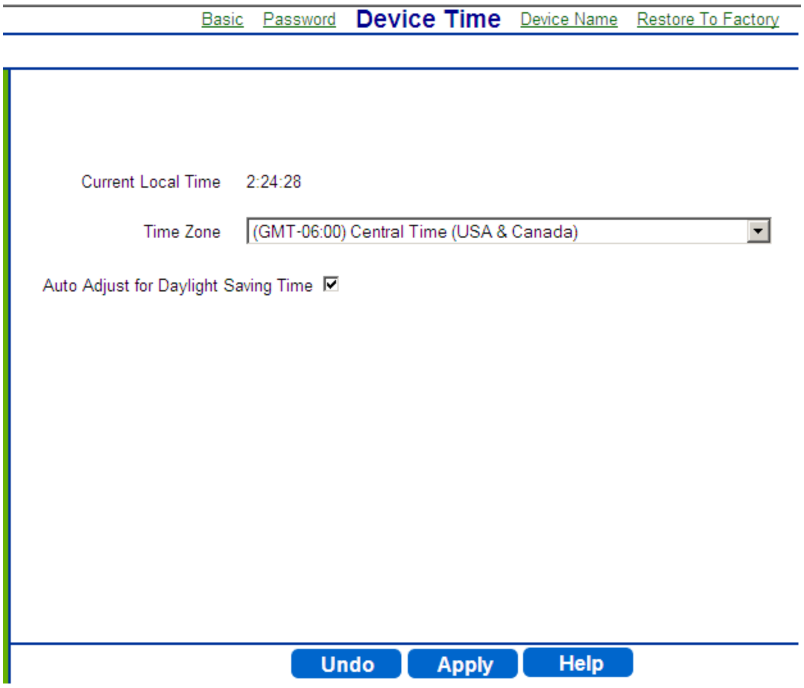
**Figure 4-2: Setup - Password**

**To change the login password:**

1. Enter a new login password (up to 19 characters).
2. Enter the new password again for verification.
3. Click **Apply**.

# 4.4 Setting Device Time Zone

The BreezeMAX PRO 6000 uses the Simple Network Time Protocol (SNTP) to set its internal clock based on periodic updates from a time server. Maintaining an accurate time on the device enables the system log to record meaningful dates and times for event entries. This time value may also be passed to telephone handsets connected to the unit's phone line connections, depending on the capabilities of your phone.



Current Local Time 2:24:28

Time Zone (GMT-06:00) Central Time (USA & Canada)

Auto Adjust for Daylight Saving Time ☑

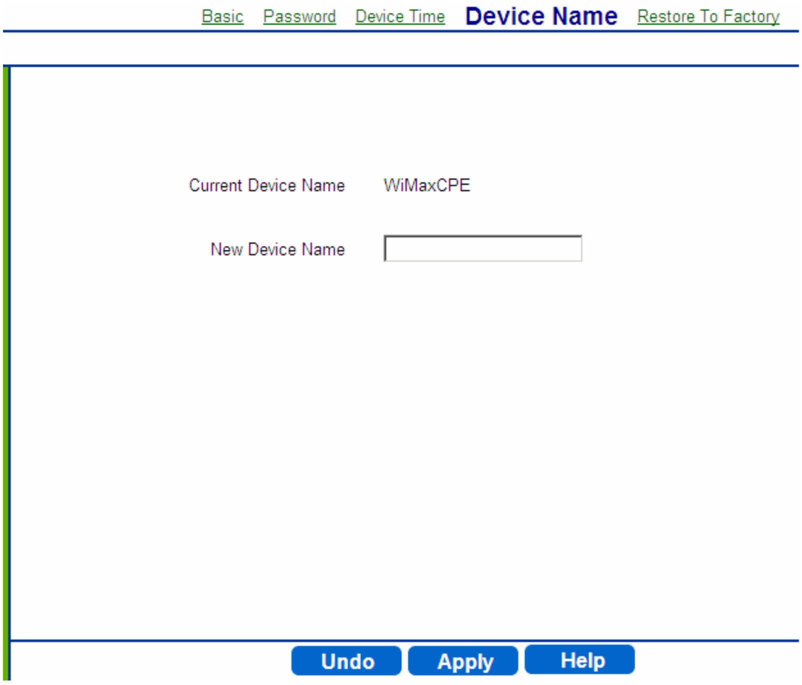
**Figure 4-3: Setup - Device Time**

The Device Time page displays the following information:

- **Current Local Time (hh:mm:ss)** – Displays the current time of the system clock.
- **Time Zone** – SNTP uses Greenwich Mean Time, or GMT (also known as Universal Time Coordinated, or UTC) based on the time at the Earth’s prime meridian, zero degrees longitude. To display a time corresponding to your local time, select your time zone from the pull-down list. The default is GMT -6, for Central Time (USA and Canada.)
- **Auto Adjust for Daylight Saving Time** - Select this check-box to set the daylight saving time if the unit operates in a region that observes daylight saving time. The default is Enabled.

# 4.5 Setting Device Name

This page allows you to define a name that identifies your unit. Using an easy-to-remember name instead of the default one will simplify access to the unit's GUI Setup menu. You can type the device name, followed by a dot(.) in the address bar of the Web browser to login from LAN (for example: *http://mycpe.*).



Current Device Name WiMaxCPE

New Device Name

Figure 4-4: Setup - Device Name

The Device Name page displays the following information:

- **Current Device Name** - Displays the current name of the unit (Default: BMAX6000)
- **New Device Name** - Enter a new name for your device (up to 20 ASCII printable characters) and click **Apply**.

## 4.6 Restore to Factory Default Configuration

This page resets the unit to its factory default settings. When returning to factory defaults, the default configuration file (IPKG) is reloaded, resetting all the parameters to those defined in this file.

All the changes from the default factory settings will be lost, including voice. Essential Voice service settings will be restored automatically within a short period of time by the network once the device is operational after the reboot. You need to manually restore any parameter changes, such as voice settings that you have made, since these settings will not exist after the unit reboots following the default restoration.

**NOTE!**

Do not change parameters in this page unless specifically instructed by your service provider.

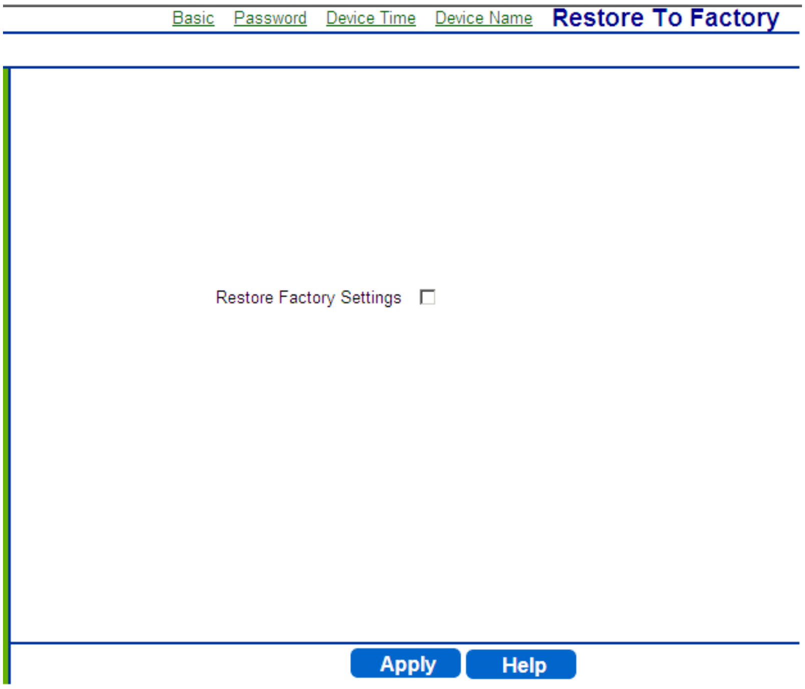


**Figure 4-5: Setup - Restore to Factory Warning**

To restore settings to factory defaults, select the checkbox on this page and click **Apply** to confirm the action. After applying factory defaults, the unit reboots.

# Chapter 5 - Configuring Local Address Parameters

## In this chapter:

# 5.1 Introduction

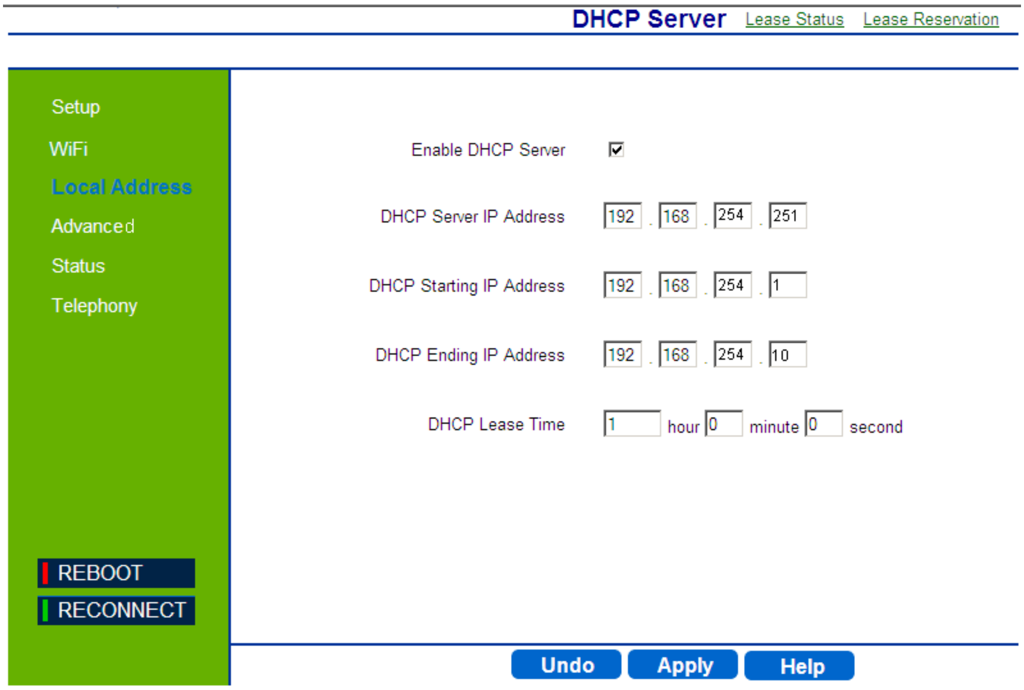
This chapter describes how to configure internal unit parameters such as DHCP server details and leasing parameters.

**INFORMATION**

Any changes to this section should only be carried out by a network administrator familiar with the functionality of these settings.

# 5.2 DHCP Server

The unit has a built-in DHCP server that can be used for managing the distribution of IP addresses for the devices connected to the local Ethernet ports. In the DHCP Server page you set DHCP parameters for dynamic IP assignment.



Enable DHCP Server ☑

DHCP Server IP Address 192 . 168 . 254 . 251

DHCP Starting IP Address 192 . 168 . 254 . 1

DHCP Ending IP Address 192 . 168 . 254 . 10

DHCP Lease Time 1 hour 0 minute 0 second

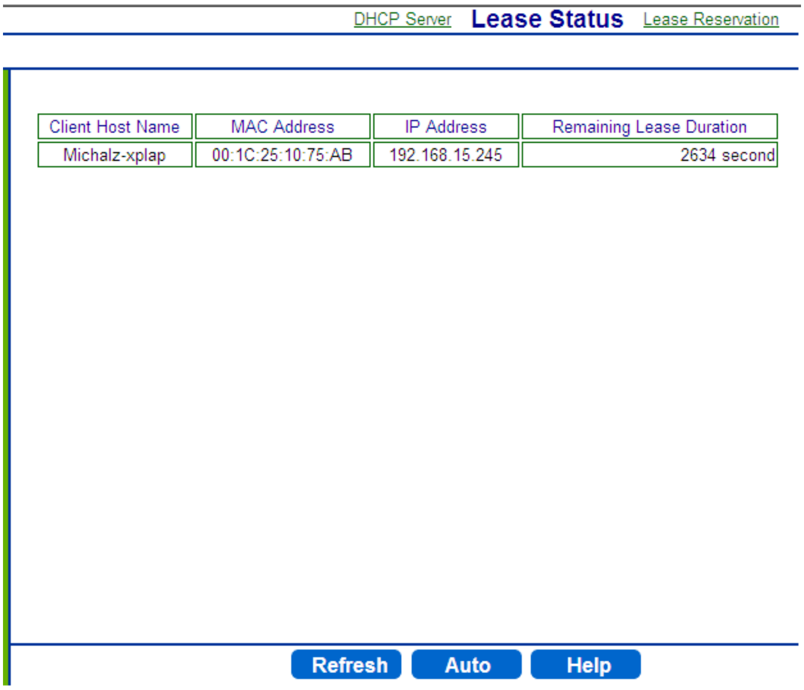
**Figure 5-1: DHCP Server**

- **Enable DHCP Server** - Select this check-box dynamically assign a leased IP address to clients that connect to the device from the local network. This option is applicable to IP CS modes only. For Bridge IPCS and Bridge ETHCS this option is disabled.
- **DHCP Server IP Address** - Enter a DHCP server IP address. The default address is 192.168.254.251.
- **DHCP Starting IP Address** - Enter the first IP address assigned by the DHCP server. The default address is 192.168.254.1.
- **DHCP Ending IP Address** - Enter the last IP address assigned by the DHCP server. The default address is 192.168.254.5.
- **DHCP Lease Time** - Set the time for renewing the IP Lease. Default: 15 minutes.

# 5.3 Lease Status

The Lease Status page displays information regarding the leased IP address(es):

- Client Host PC Name
- Host PC MAC Address
- IP Address
- Remaining Lease Duration (seconds)



| Client Host Name | MAC Address | IP Address | Remaining Lease Duration |
|---|---|---|---|
| Michalz-xplap | 00:1C:25:10:75:AB | 192.168.15.245 | 2634 second |

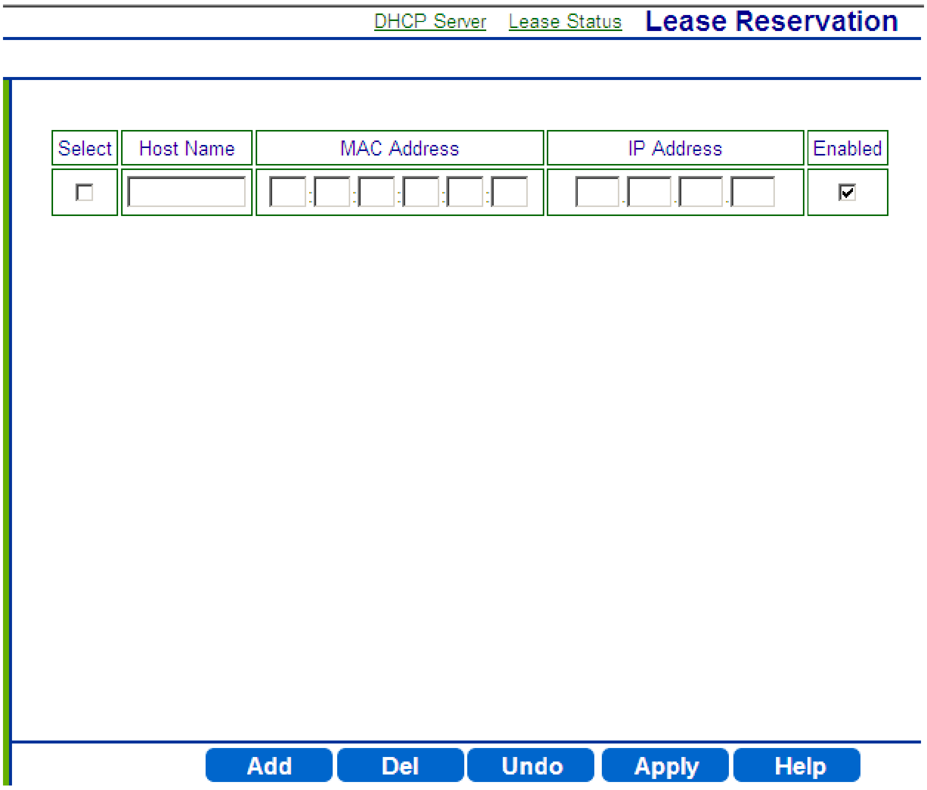
**Figure 5-2: Lease Status**

Click **Refresh** to display the updated information of the client host PC.

Click **Auto** to refresh the information automatically.

## 5.4 Lease Reservation

The Lease Reservation page displays information on reserved IP addresses for leasing. In this page you assign the specific IP addresses to the specific client device connected to the Ethernet ports. You can also add, delete, or modify the reservation settings.



| Select | Host Name | MAC Address | IP Address | Enabled |
|---|---|---|---|---|
| □ | | : : : : : | . . . | ☑ |

**Figure 5-3: Lease Reservation**

- **Select** - Choose an IP to delete.
- **Host Name** - Enter a name to the host
- **MAC Address** - Add a device MAC address
- **IP Address** - Specify a reservation IP address for a specified MAC address
- **Enabled** - Select if to enable or disable a specified IP setting.

Use the **Add** or **Delete** buttons to add or clear reserved IPs for leasing. Click **Apply** to activate your changes.

# Chapter 6 - Setting Advanced Parameters

## In this chapter:

# 6.1 Introduction

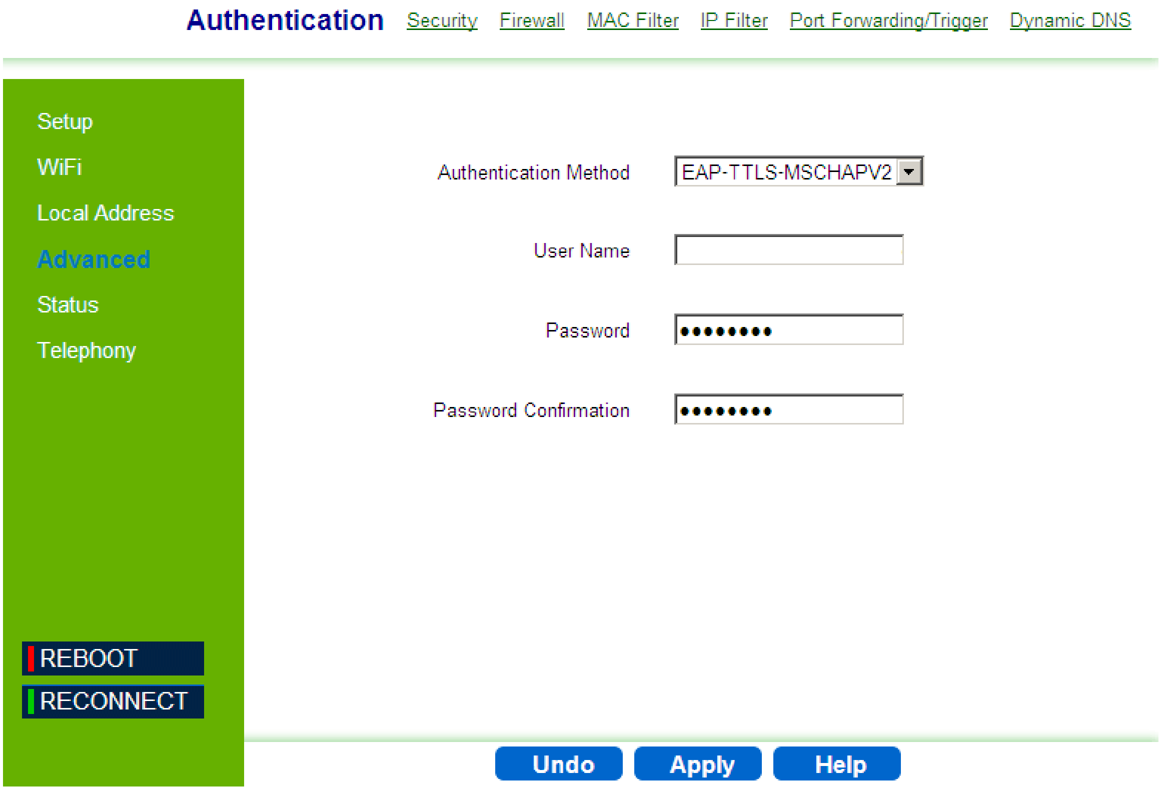
This chapter describes how to configure advanced parameters, such as: Firewall protection, authentication methods, security parameters, filters for blocking the access of unauthorized clients, port forwarding and triggering, and also the Dynamic DNS (Domain Name System) provider.

# 6.2 Authentication

The Authentication page allows you to set the parameters for the authentication method in order to gain access to the WiMAX network.

**NOTE!**

Do not change parameters in this page unless specifically instructed by your service provider.



Authentication Method: EAP-TTLS-MSCHAPV2

User Name:

Password: ••••••••

Password Confirmation: ••••••••

**Figure 6-1: Advanced - Authentication**

The Authentication page includes the following parameters:

- **Authentication Method** - Select one of the following WiMAX security methods:
  - None - Authentication is disabled
  - EAP-TTLS-MSCHAPV2 (Default) - EAP-Tunneled Transport Layer Security, supporting the Microsoft version of the Challenge-handshake authentication protocol, version 2.
  - EAP TLS - EAP-Transport Layer Security (available only if enabled by the operator)

When Authentication is enabled, set the following parameters:

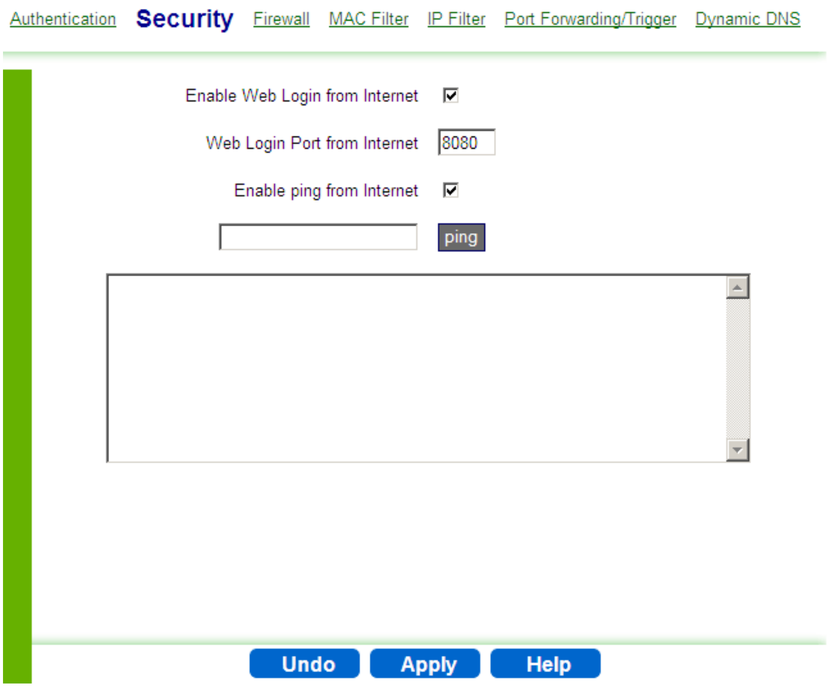
- **User Name** - Enter the user name supplied by the service provider (Default:  CPE MAC address@WiMAX.com, e.g. 0026824EE12C@WiMAX.com).
- **Password** - Enter the user password (supplied by the service provider). Default: quickynikynyoky
- **Password Confirmation** - Re-enter the user password to confirm it.

## 6.3 Security

The Security page enables to configure the firewall feature. The firewall feature can be used to block unauthorized access while allowing only authorized communications from the Internet network. This feature also allows the device to be managed over the Internet by authorized personnel.

NOTE!

Do not change parameters in this page unless specifically instructed by your service provider.



Enable Web Login from Internet ☑

Web Login Port from Internet 8080

Enable ping from Internet ☑

**Figure 6-2: Advanced - Security**

The Security page includes the following parameters:

- **Enable Web login from Internet** - Select this check-box to access the device from other networks. When web login is enabled and a port is defined, you can access the device from another network Simply by opening a browser and entering the address of the device (Default: Enabled
- **Web Login Port from Internet** - Define a specific port number for security access control (the default port number is 8080). Available only if Web Login from Internet is enabled.
- **Enable ping from Internet** - Enables to set the unit to respond to ping commands for troubleshooting purposes (Default: Disabled).

INFORMATION

The Enable Ping From Internet option is used for testing, therefore it is recommended to keep it disabled during normal operation.

You can ping and receive a replay from the LAN network while ping is disabled. However, when this option is disabled, you cannot ping from WAN to the unit.

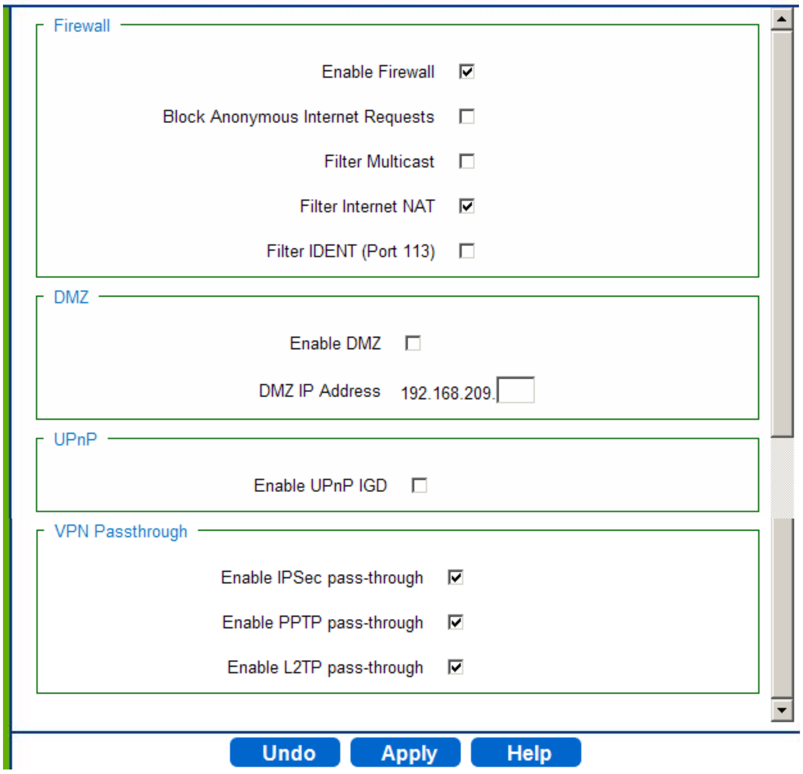
To issue a Ping command, enter the destination address and click **Ping**. The response will be displayed in the area below the Ping button.

To access the unit from WAN, use https://CPE_WAN_IP_Address:8080.

# 6.4 Firewall

The BreezeMAX PRO 6000 provides extensive firewall protection by restricting connection parameters to limit the risk of intrusion and defending against a wide array of common hacker attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a demilitarized zone (DMZ).

**NOTE!** Changes made on this page may affect your internet connection. If you notice an undesirable change in your internet service after making a change to the firewall, you may want to return to the previous setting.



Firewall

Enable Firewall ☑

Block Anonymous Internet Requests ☐

Filter Multicast ☐

Filter Internet NAT ☑

Filter IDENT (Port 113) ☐

DMZ

Enable DMZ ☐

DMZ IP Address 192.168.209.

UPnP

Enable UPnP IGD ☐

VPN Passthrough

Enable IPSec pass-through ☑

Enable PPTP pass-through ☑

Enable L2TP pass-through ☑

**Figure 6-3: Advance - Firewall**

The following configuration parameters are available:

- **Firewall** settings
  - **Enable Firewall** - Select this check-box to enable or disable firewall.
  - **Block Anonymous Internet Requests** - Select this check-box to reject anonymous Internet requests.
  - **Filter Multicast** - Select this check-box to filter out mutlicast packets.
  - **Filter Internet NAT Redirection -** NAT Redirection is used to block access to the local server from the local PC via unit's WAN IP. If this feature is enabled, local PC can only access the local server via unit's LAN IP.
  - **Filter IDENT (Port 113)** - Select this check-box to drop incoming packets from the unit WAN side with destination port 113.
- **DMZ ("Demilitarized Zone")**
  - **Enable DMZ -** Set a server that acts as a "neutral zone"and separates an internal network from a public one in order to prevent outside access to private data. The DMZ forwards the network traffic to specific hosts based on the protocol and port number.
  - **DMZ** - DMZ IP Address.
- **UPnP** - **Enable UPnP IGD** - Select this check-box to enable/disable Universal Plug and Play Internet Gateway Device - a protocol that simplifies device connection and network implementation. When this option is enabled, certain Windows applications would setup the port forwarding rule dynamically.
- **VPN Passthrough -** Select one of the following security protocols to define the Virtual Private Network traffic sessions.

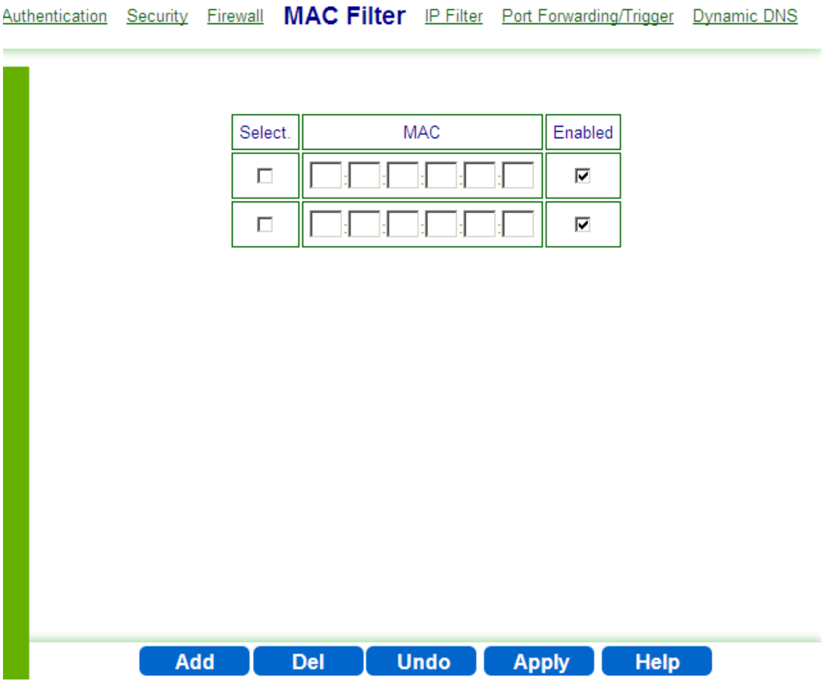
**NOTE!**

Do not change parameters in this page unless specifically instructed by your service provider.

  - **Enable IPSec pass-through** - Internet Protocol Security. IPSec provides encrypted security services at the IP layer, and enables to use encrypted tunnels /traffic between two hosts.
  - **Enable PPTP pass-through** - Point to Point Tunneling Protocol. This protocol enables the transfer of data packets of TCP / IP through a foreign network that is not based on these protocols (by marking the packet with an address suited to the foreign network)
  - **Enable L2TP pass-through** - Layer 2 Tunneling Protocol, an open standard with mutlivendor interoperability and acceptance.

## 6.5 MAC Filter

You can block access to the Internet from clients on the local network by MAC addresses. In the MAC Filter page you set MAC addresses to be filtered out by the security system. You can add addresses to the filtered group or delete them, and also enable or disable filtering at different times.



| Select. | MAC | Enabled |
|---|---|---|
| □ | __ : __ : __ : __ : __ : __ | ☑ |
| □ | __ : __ : __ : __ : __ : __ | ☑ |

**Figure 6-4: Advance - MAC Filter**

The following configuration parameters are available:

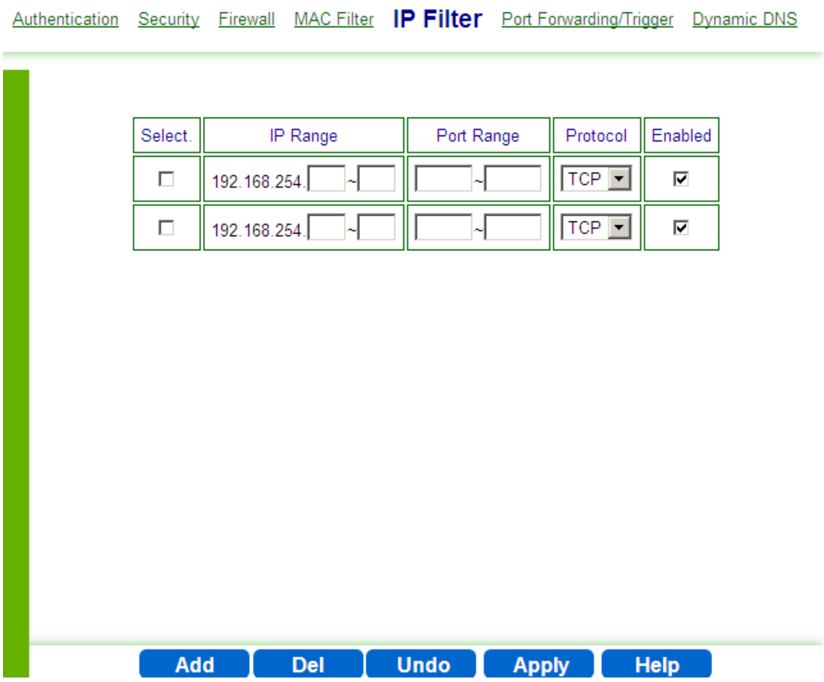
- **Select** - Select this check-box to delete this entry.
- **MAC** - Enter the MAC address to be filtered.
- **Enabled** - Select this check-box to enable/disable filter for the specific MAC address.

Use the **Add** or **Del** buttons to add the address to the filtered group or clear it from the group. Click **Apply** to activate your changes.

# 6.6 IP Filter

You can block access to the Internet from clients on the local network by specifying IP addresses and TCP/UDP port numbers. You can configure up to five IP filters on the unit.

In the IP Filter page you set IP addresses to be filtered out by the security system. You can add addresses to the filtered group or delete them. You can also enable or disable filtering at different times.



| Select. | IP Range | Port Range | Protocol | Enabled |
|---|---|---|---|---|
| □ | 192.168.254.[ ]~[ ] | [ ]~[ ] | TCP | ☑ |
| □ | 192.168.254.[ ]~[ ] | [ ]~[ ] | TCP | ☑ |

**Figure 6-5: Advance - IP Filter**

The following configuration parameters are available:

- **Select** - Select this check-box to delete this entry.
- **IP Range** - Specify an IP address or range on the local network. (Range: 192.168.254.1 to 192.168.254.254)
- **Port Range** - Enter the port range to be filtered
- **Protocol** - set the protocol to be filtered: TCP (default) or UDP.
- **Enabled** - Select this check-box to enable (default) or disable filtering for the specific table entry.

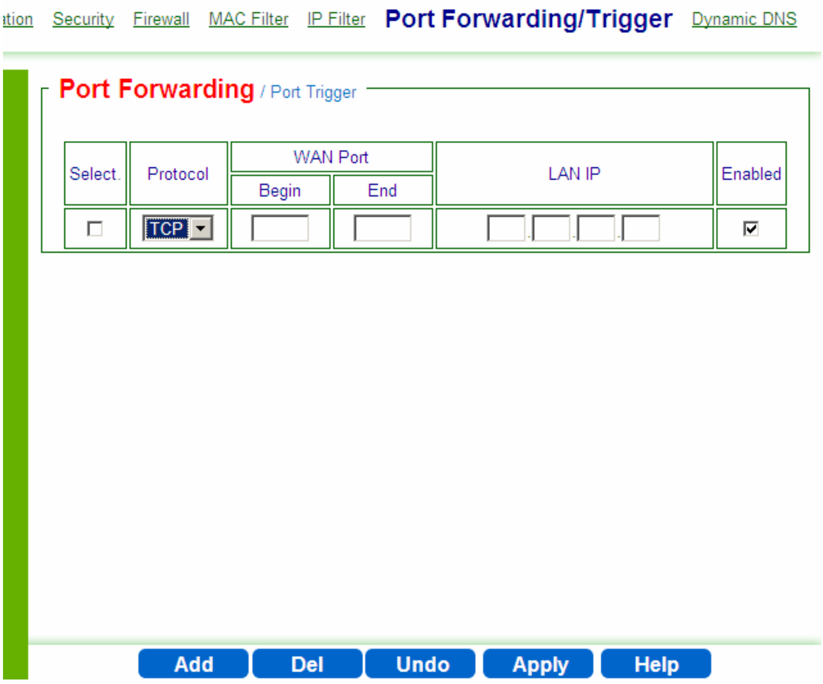
Use the **Add** or **Del** buttons to add the address to the filtered group or clear it from the group. Click **Apply** to activate your changes.

# 6.7 Port Forwarding/Trigger

## 6.7.1 Port Forwarding

Port Forwarding instructs the router to which computer on the local area network to send data. According to the port forwarding rules or setup, the router sends the data from the external IP address: port number to an internal IP address: port number. Port Forwarding rules are created per port.

The Port Forwarding page enables managing and setup of the rules for Port Forwarding.



| Select | Protocol | WAN Port | | LAN IP | Enabled |
|---|---|---|---|---|---|
| | | Begin | End | | |
| ☐ | TCP | | | . . . | ☑ |

**Figure 6-6: Advance - Port Forwarding**

The following configuration parameters are available:

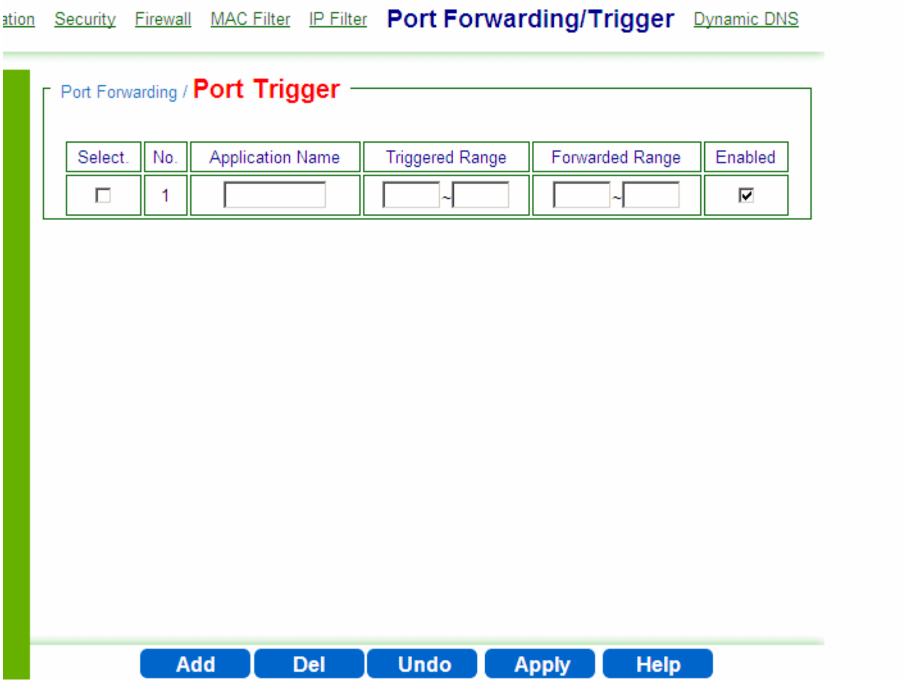
- **Select** - Select this check-box to delete this entry.
- **Protocol** - Set the protocol for port forwarding: TCP or UDP.
- **WAN Port** - Enter the range (begin and end ports) for the WAN.
- **LAN IP** - Enter the IP address of the computer from LAN network for which you open ports in “Port forwarding”.
- **Enabled** - Select this check-box to enable/disable port forwarding for the specific IP

Use the **Add** or **Del** buttons to add a rule to the port forwarding group or clear it from the group. Click **Apply** to activate your changes.

## 6.7.2 Port Trigger

Port forwarding redirects incoming network traffic from a pre-defined WAN port range to a pre-defined LAN IP Address and LAN port range. Port triggering is a way to automate port forwarding: outbound traffic on predefined ports ('triggering ports') causes inbound traffic to specific incoming ports to be dynamically forwarded to the initiating host, while the outbound ports are in use. This allows computers behind a NAT-enabled router on a local network to provide services that would normally require the computer to have a fixed address on the local network. Port triggering triggers can open an incoming port when a client on the local network makes an outgoing connection on a predetermined port or range of ports.

In the Port Trigger page you can specify up to 15 rules with parameters for Port Triggering.



| Select. | No. | Application Name | Triggered Range | Forwarded Range | Enabled |
|---|---|---|---|---|---|
| □ | 1 | | ~ | ~ | ☑ |

Figure 6-7: Advance - Port Trigger

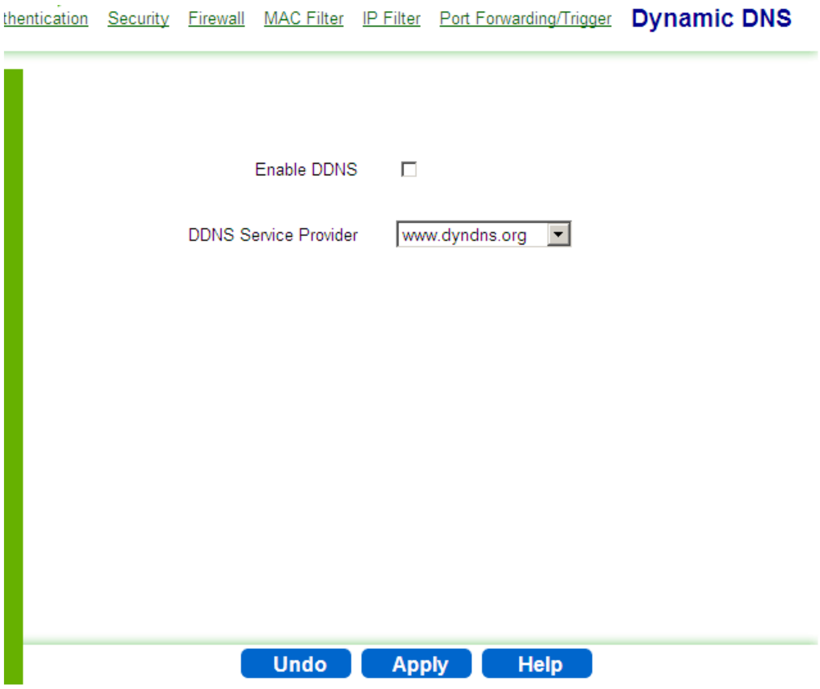
The following configuration parameters are available:

- **Select** - Select this check-box to delete this entry.
- **No**. - Display the number of the port trigger rule
- **Application Name** - Enter a name for identifying this port trigger protocol.
- **Triggered Range** - Enter the trigger range (1~65535)
- **Forwarded Range** - Enter the forwarded range (1~65535)
- **Enabled** - Select this check-box to enable/disable port trigger for the specific application

Use the **Add** or **Del** buttons to add a rule to the port triggering group or clear it from the group. Click **Apply** to activate your changes.

# 6.8 Dynamic DNS

Dynamic Domain Name System (DNS) is a mechanism used for translating host names for network nodes into IP addresses in real-time. This page allows enabling the Dynamic DNS and selecting the service provider.



Enable DDNS □

DDNS Service Provider www.dyndns.org

Figure 6-8: Advanced - Dynamic DNS

The Dynamic DNS page includes the following parameters:

- **Enable DDNS** - Select this check-box if the unit has a non-static IP address to keep the domain name associated with an ever-changing IP address.

  When DDNS is enabled, configure the following parameters:

  - DDNS User Name
  - DDNS Password
  - DDNS Host Name

- **DDNS Service Provider** - Select the DDNS service provider from the drop-down list (Default: www.dyndns.org).

# Chapter 7 - Displaying Status Details

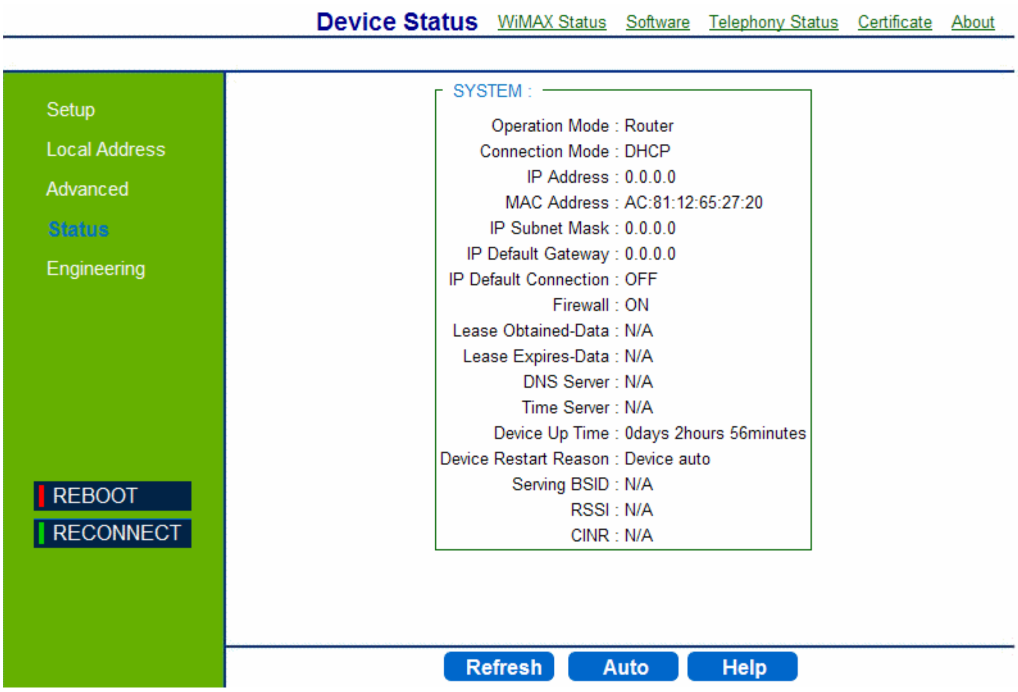
## In this chapter

# 7.1 Introduction

This chapter describes how to view and understand the various parameters that are currently set on your unit. The Status menu item includes pages containing information on all the features of the device, such as the device currently used software, the Telephony status, WiMAX parameters, certification information, etc.

## 7.2 Device Status

This page displays the status of the unit such as system uptime and WAN information.



SYSTEM :

Operation Mode : Router
Connection Mode : DHCP
IP Address : 0.0.0.0
MAC Address : AC:81:12:65:27:20
IP Subnet Mask : 0.0.0.0
IP Default Gateway : 0.0.0.0
IP Default Connection : OFF
Firewall : ON
Lease Obtained-Data : N/A
Lease Expires-Data : N/A
DNS Server : N/A
Time Server : N/A
Device Up Time : 0days 2hours 56minutes
Device Restart Reason : Device auto
Serving BSID : N/A
RSSI : N/A
CINR : N/A

**Figure 7-1: Status - Device Status**

- Click **Refresh** to display the current device status.
- Click **Auto** to update the status information periodically.
- The following information is displayed:

**Table 7-1: Device Status Parameters**

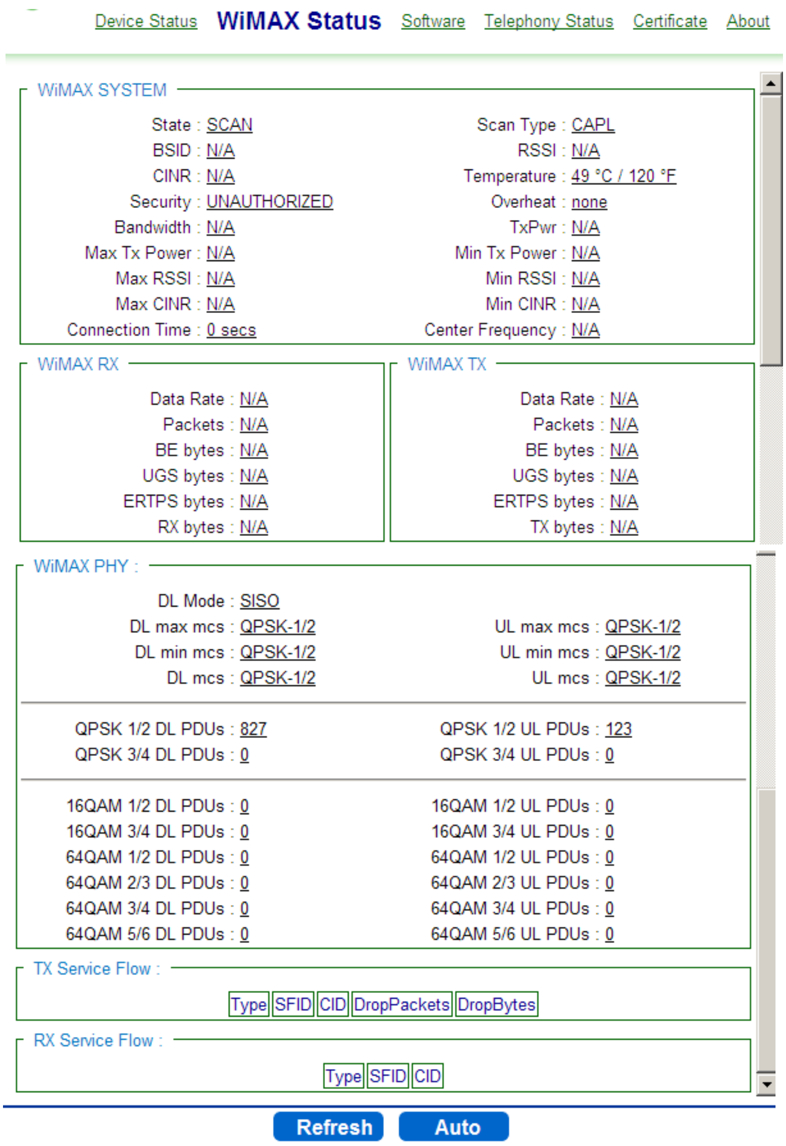
| Item | Description |
|---|---|
| Operation Mode | The mode for forwarding data packets from the service provider's WiMAX network to the local network, as defined in "Setting Basic Parameters" on page 37. Available option: Router. |
| Connection Mode | Connection type for the unit, as defined in "Setting Basic Parameters" on page 37. Available options: DHCP, Static |
| IP Address | WAN IP address, if the Static connection mode was selected, as defined in "Setting Basic Parameters" on page 37. For DHCP mode - IP address acquired on the WAN interface is displayed. Otherwise it is 0.0.0.0 |
| MAC | WAN MAC Address for data interface |

Table 7-1: Device Status Parameters (Continued)

| Item | Description |
|---|---|
| IP Subnet Mask | The IP subnet mask, if the Static connection mode was selected, as defined in "Setting Basic Parameters" on page 37, For DHCP mode - IP Subnet Mask acquired on the WAN interface is displayed. Otherwise it is 0.0.0.0 |
| IP Default Gateway | The IP Default Gateway, if the Static connection mode was selected, as defined in "Setting Basic Parameters" on page 37. For DHCP mode - IP Default Gateway acquired on the WAN interface is displayed. Otherwise it is 0.0.0.0 |
| IP Default Connection | IP is connected to the network (On/Off) |
| Firewall | Firewall enabled or disabled (on/off), as set in "Firewall" on page 55. |
| Lease Obtained-Data | Date of obtaining the device leasing. |
| Lease Expires-Data | Date of device leasing expiration. |
| DNS Server | The Domain Name Server address |
| Time Server | The NTP (Network Time Protocol) server address |
| Device Up Time | Duration of device function (xdays yhours zminutes) |
| Device Restart Reason | The reason for last device reboot (e.g. Software Upgrade) |
| Serving BSID | Base Station ID number (e.g. 00:01:21:00:03:5A) |
| RSSI | Currently received signal strength indication (e.g. -70 dBm) |
| CINR | Carrier to Interference-plus-Noise Ratio [in decibels (dB)] (e.g. 13 dB). This value should be maximized for best signal quality. |

## 7.3 WiMAX Status

The WiMAX Status displays a summary of the WiMAX network connection parameters.



WiMAX SYSTEM

State : SCAN
Scan Type : CAPL
BSID : N/A
RSSI : N/A
CINR : N/A
Temperature : 49 °C / 120 °F
Security : UNAUTHORIZED
Overheat : none
Bandwidth : N/A
TxPwr : N/A
Max Tx Power : N/A
Min Tx Power : N/A
Max RSSI : N/A
Min RSSI : N/A
Max CINR : N/A
Min CINR : N/A
Connection Time : 0 secs
Center Frequency : N/A

WiMAX RX

Data Rate : N/A
Packets : N/A
BE bytes : N/A
UGS bytes : N/A
ERTPS bytes : N/A
RX bytes : N/A

WiMAX TX

Data Rate : N/A
Packets : N/A
BE bytes : N/A
UGS bytes : N/A
ERTPS bytes : N/A
TX bytes : N/A

WiMAX PHY :

DL Mode : SISO
DL max mcs : QPSK-1/2
UL max mcs : QPSK-1/2
DL min mcs : QPSK-1/2
UL min mcs : QPSK-1/2
DL mcs : QPSK-1/2
UL mcs : QPSK-1/2

QPSK 1/2 DL PDUs : 827
QPSK 1/2 UL PDUs : 123
QPSK 3/4 DL PDUs : 0
QPSK 3/4 UL PDUs : 0

16QAM 1/2 DL PDUs : 0
16QAM 1/2 UL PDUs : 0
16QAM 3/4 DL PDUs : 0
16QAM 3/4 UL PDUs : 0
64QAM 1/2 DL PDUs : 0
64QAM 1/2 UL PDUs : 0
64QAM 2/3 DL PDUs : 0
64QAM 2/3 UL PDUs : 0
64QAM 3/4 DL PDUs : 0
64QAM 3/4 UL PDUs : 0
64QAM 5/6 DL PDUs : 0
64QAM 5/6 UL PDUs : 0

TX Service Flow :

| Type | SFID | CID | DropPackets | DropBytes |
|---|---|---|---|---|

RX Service Flow :

| Type | SFID | CID |
|---|---|---|

**Figure 7-2: Status - WiMAX Status**

- Click **Refresh** to display the current WiMAX connection status.
- Click **Auto** to update the status information periodically (every 3 seconds)

The following table describes the WiMAX Status parameters:

**Table 7-2: WiMAX System Parameters**

| Parameter | Description | Possible values |
|---|---|---|
| **WiMAX System** | | |
| State | The status of WiMAX connection. | ■ Network Entry - the unit has just been connected to the network<br>■ Operational - the unit is functional<br>■ Scan - the unit scans the network<br>■ Idle - the unit is de-registered from the network, however will continue to scan the network and keep track of its location |
| BSID | The Base Station ID | Depends on the BS to which the unit is connected |
| CINR | Carrier to Interference-plus-Noise Ratio [in decibels (dB)] - a measurement of signal effectiveness. A greater value will improve the connection speed. | 0-35 dB |
| Security | The network security technologies and protocols status | ■ Authorized - has authentication settings<br>■ Unauthorized - without authentication setting. Unauthorized also appears for units set with authentication, when they are not linked to a BS and successfully authenticated. |
| Bandwidth | Device operation bandwidth | Depending on unit model: 5000, 7000, or 10000 KHz |
| Max Tx Power | The maximum uplink transmit power | |
| Max RSSI | The maximum signal strength indication value used since the last reboot | -35 to -100 dBm |
| Max CINR | The maximum Carrier to Interference-plus-Noise Ratio value used since the last reboot | |
| Connection Time | Time (in seconds) during which the unit is connected to the BS | |

Table 7-2: WiMAX System Parameters (Continued)

| Parameter | Description | Possible values |
|---|---|---|
| Scan Type | The method by which the network is scanned | - Fullband - The system will try to scan the whole frequency band.<br>- CAPL - Channel Allocation Priority Level. The system allocates priority to channels for scanning order.<br>- Neighbor - The system will try to scan the neighbor BS to the previous BS defined in "Last good BS". The neighbor BS details will appear in the table of this section.<br>- History - The system will try to scan with the previous good BS to speed up the scan duration. A "good BS" is defined as one with which the unit can get an IP address. |
| RSSI | Currently received signal strength indication | -35 to -100 dBm |
| Temperature | Unit's temperature | |
| Overheat | Indication of temperature higher than 40° | |
| TxPwr | Current uplink transmit power | |
| Min Tx Power | Minimum uplink transmit power | |
| Min RSSI | The minimum signal strength indication value used since the last reboot | |
| Min CINR | Minimum Carrier to Interference-plus-Noise Ratio value used since the last reboot | |
| Center Frequency | The middle frequency of the bandwidth of a channel. The unit is synchronised on this frequency. | |
| **WiMAX TX Uplink Statistics** | | |
| Data Rate | Shows the current throughput in uplink direction. The level of available data throughput that can actually be provided to an end-user. | |
| Packets | The number of carried blocks of data | |

Table 7-2: WiMAX System Parameters (Continued)

| Parameter | Description | Possible values |
|---|---|---|
| BE bytes | Total number of bytes sent on Best Effort connection | |
| UGS bytes | Total number of bytes sent on Unsolicited Grant Service connection | |
| ERTPS bytes | Total number of bytes sent on ERTPS - Extended Real-time Polling Service data packets. | |
| TX bytes | Total of uplink transmitted bytes | |
| **WiMAX RX Downlink Statistic** | | |
| Data Rate | Shows the current throughput in downlink direction. The level of available data throughput that can actually be provided to an end-user. | |
| Packets | Number of carried blocks of data | |
| BE bytes | Total number of bytes sent on Best Effort data packets | |
| UGS bytes | Total number of bytes sent on Unsolicited Grant Service data packets | |
| ERTPS bytes | Total number of bytes sent on Extended Real-time Polling Service data packets | |
| RX bytes | Total of downlink transmitted bytes | |
| **WiMAX PHY** | | |
| DL Mode | Downlink connection mode | SISO, MIMO, MiMO A, MIMO B |
| DL max mcs | The maximum modulation reached | |
| DL min mcs | The minimum modulation reached | |
| DL mcs | Current modulation | |
| UL max mcs | The maximum modulation reached | |
| UL min mcs | The minimum modulation reached | |
| UL mcs | The current modulation | |

Table 7-2: WiMAX System Parameters (Continued)

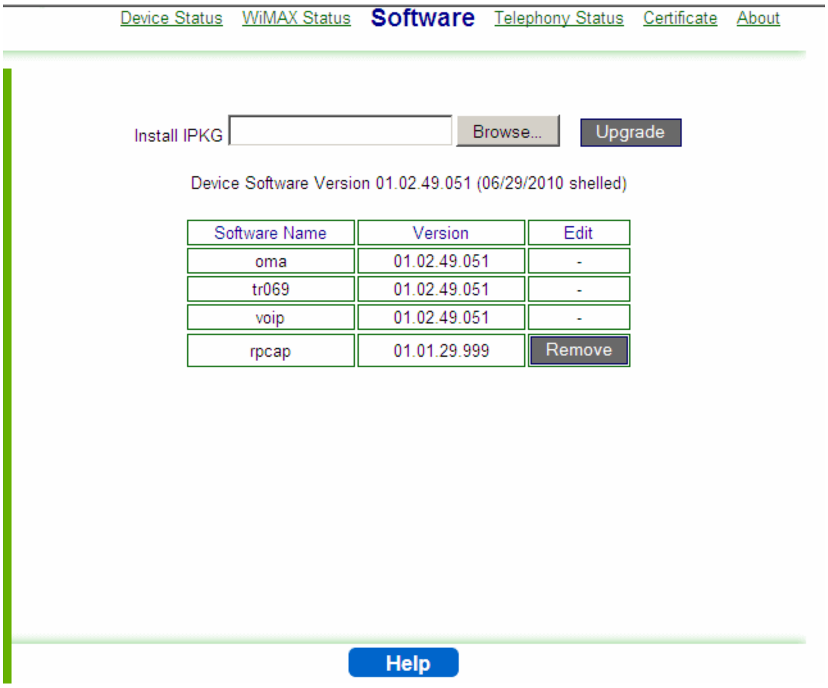
| Parameter | Description | Possible values |
|---|---|---|
| List of various modulations:<br>■ QPSK DL/UL PDUs<br>■ 16QAM DL/UL PDUs<br>■ 64QAM DL/UL PDUs | Number of packets in this modulation | |
| **TX Service Flow / Rx Service Flow** | | |
| Type | The service flow type | Best effort, ERT, NRT, UGS |
| SFID | Service flow ID | |
| CID | Connection ID | |
| DropPackets (Tx only) | Number of packets that were dropped | |
| DropBytes (Tx only) | Number of bytes that were dropped | |

# 7.4 Software Status

The Software page enables installing or removing IPKGs (Itsy Package Management System) - lightweight package management systems that allows for dynamic installation/removal of packages on a running system.

**INFORMATION**

Use this page only upon instructions from Alvarion.



Device Software Version 01.02.49.051 (06/29/2010 shelled)

| Software Name | Version | Edit |
|---|---|---|
| oma | 01.02.49.051 | - |
| tr069 | 01.02.49.051 | - |
| voip | 01.02.49.051 | - |
| rpcap | 01.01.29.999 | Remove |

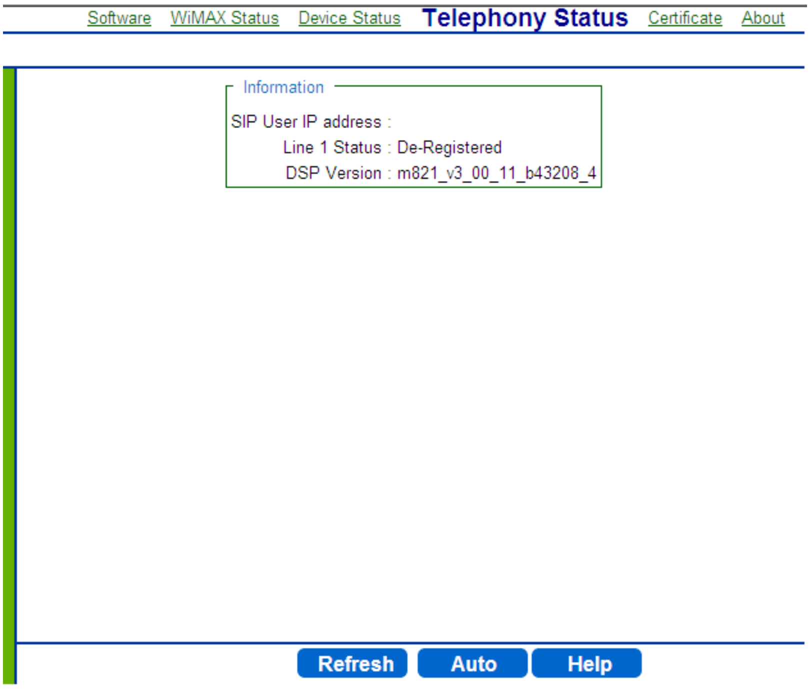
**Figure 7-3: Status - Software**

- To install an IPKG - Click **Browse** to load and install an Itsy Package Management System and click **Upgrade**.
- To remove an IPKG - Click **Remove** next to the component to be deleted.

The page also displays the current software items installed by the operator on the device. These are read-only items that cannot be edited/removed

# 7.5 Telephony Status

This page displays information on the telephone line status.



SIP User IP address :
Line 1 Status : De-Registered
DSP Version : m821_v3_00_11_b43208_4

**Figure 7-4: Status - Telephony Status**

The information displayed in this window is:

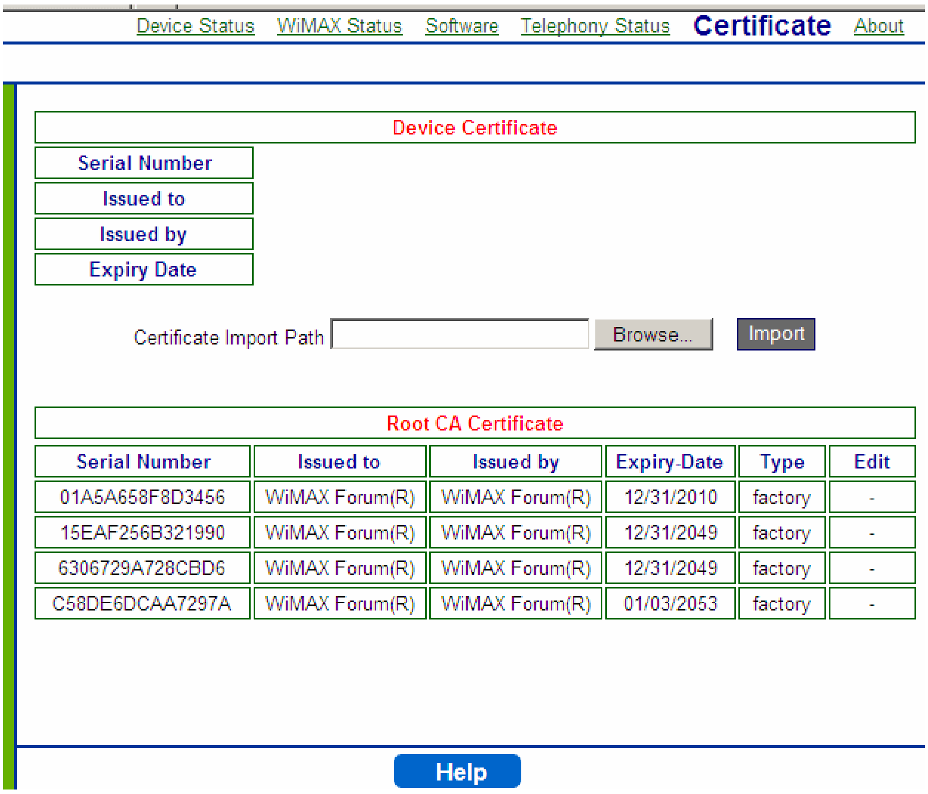
- **SIP User IP address** - IP address of the Session Initiation Protocol, an application-layer control protocol that can establish, modify, and terminate multimedia sessions such as Internet telephony calls (VOIP).
- **Line 1 Status** - Registered or De-registered in the SIP server.
- **DSP Version** - current version of the voice chip in the Data Signal Processor (DSP).
- Click **Refresh** to display the current telephony status.
- Click **Auto** to update the status information periodically (every 3 seconds).

# 7.6 Certificate Status

The Certificate page displays available certificates information, such as serial number, issuer of certificate, type and expiration date. Root CA certificates can be added or deleted using this page.

NOTE!

Do not change parameters in this page unless specifically instructed by your service provider.



Device Certificate

| | |
|---|---|
| Serial Number | |
| Issued to | |
| Issued by | |
| Expiry Date | |

Certificate Import Path

Root CA Certificate

| Serial Number | Issued to | Issued by | Expiry-Date | Type | Edit |
|---|---|---|---|---|---|
| 01A5A658F8D3456 | WiMAX Forum(R) | WiMAX Forum(R) | 12/31/2010 | factory | - |
| 15EAF256B321990 | WiMAX Forum(R) | WiMAX Forum(R) | 12/31/2049 | factory | - |
| 6306729A728CBD6 | WiMAX Forum(R) | WiMAX Forum(R) | 12/31/2049 | factory | - |
| C58DE6DCAA7297A | WiMAX Forum(R) | WiMAX Forum(R) | 01/03/2053 | factory | - |

**Figure 7-5: Status - Certificate**

The page displays the following information in a table:

- Certificate Serial Number
- Issued to
- Issued by
- Expiry Date - the date for certificate expiration. The format is mm/dd/yyyy.
- Certificate type
- Edit - option to remove a certificate from the list (only if the Remove option appears in this column)

**INFORMATION**

The table displays only part of the information (e.g. part of the serial number). To view the entire string, hover the mouse over the cell to display a tool-tip with the entire string.

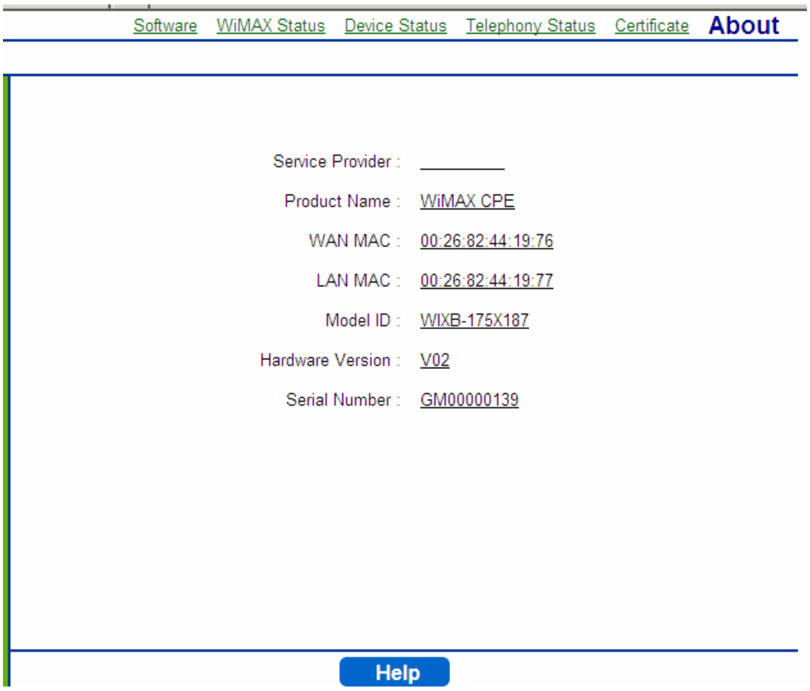
- To add a certificate, click **Browse** and select the file to load. Click **Import** to add the certificate to the list.
- To remove an editable certificate, click **Remove** next to the certificate to be deleted. Some certificates are read-only and cannot be deleted.

# 7.7 About

This page displays the current information about the unit. The information is set by the manufacturer as the factory defaults.

The information includes:

- Service Provider
- Product Name
- WAN MAC
- LAN MAC
- Model ID
- Hardware Version
- Serial Number



Service Provider : ________

Product Name : WiMAX CPE

WAN MAC : 00:26:82:44:19:76

LAN MAC : 00:26:82:44:19:77

Model ID : WIXB-175X187

Hardware Version : V02

Serial Number : GM00000139

**Figure 7-6: Status - About**

# Chapter 8 - Configuring Telephony Parameters

## In this chapter

# 8.1 Introduction

This chapter describes how to configure VoIP parameters.

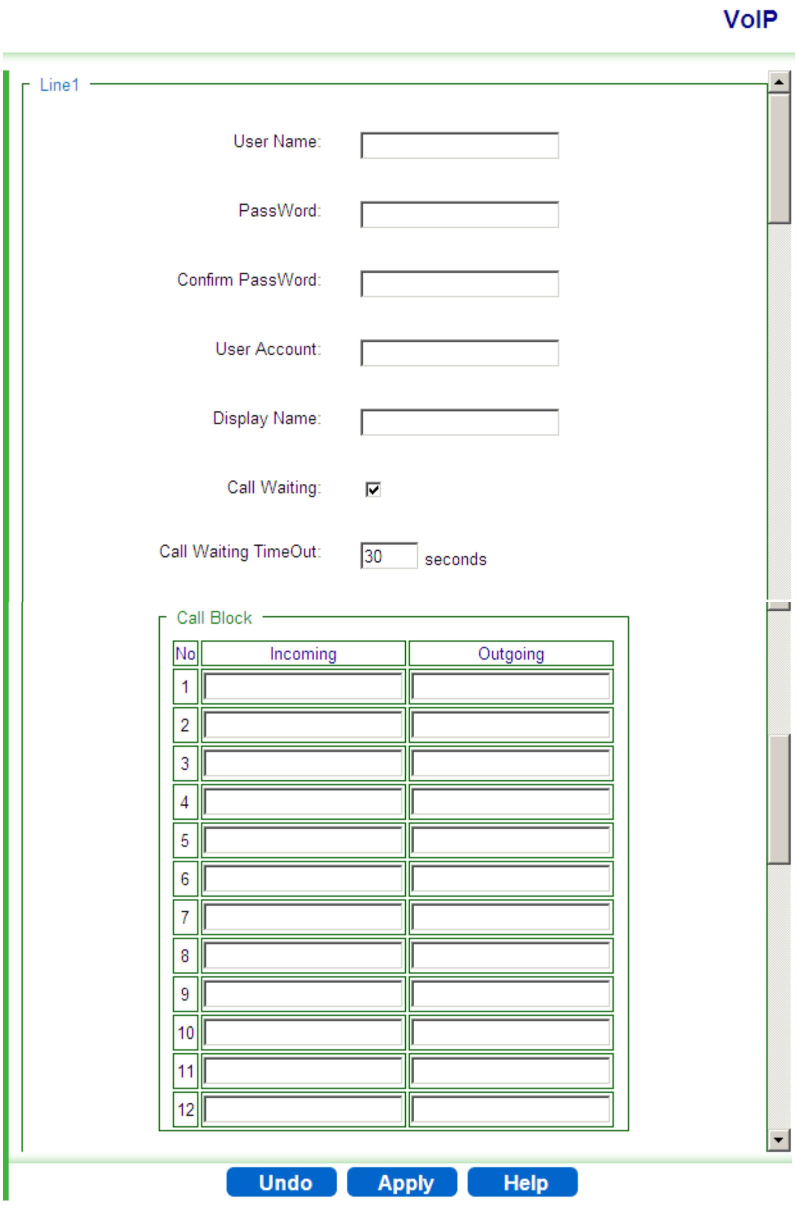
Voice over Internet Protocol (VoIP) technology is a way of using the Internet to make phone calls. You can make VoIP calls by connecting a regular phone to one of the unit's Phone ports.

Before using the VoIP Phone ports on the unit, you must have an account with a SIP service provider that includes one voice line. Setup of the modem is automatic and you will not need to make any changes to this page to have your voice service enabled, however you may want to change some of the features that are listed below. The modem allows the Phone port to be configured separately with different settings.

**NOTE!**

Modifying the user name, password, or user account settings is not required. These attributes are automatically populated when the modem is configured after connection. If you are having trouble with your voice service, contact Customer Service for support. Do not make changes to these items in an attempt to restore your service.

# 8.2 VoIP Parameters



VoIP

Line1

User Name:

PassWord:

Confirm PassWord:

User Account:

Display Name:

Call Waiting: ☑

Call Waiting TimeOut: 30 seconds

Call Block

| No | Incoming | Outgoing |
|---|---|---|
| 1 | | |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |
| 6 | | |
| 7 | | |
| 8 | | |
| 9 | | |
| 10 | | |
| 11 | | |
| 12 | | |

**Figure 8-1: Telephony - VoIP Parameters**

The VoIP page includes the following parameters:

- **User Name** - The SIP (Session Initiation Protocol) User name. Its format depends on the Sip Server
- **Password** and **Confirm Password** - The SIP user Password
- **User Account** - The SIP Account. Its format depends on the Sip Server.
- **Display Name** - Enter a name that will be displayed on the Caller ID Display Name of the receiving party (if supported by the network)

- **Call Waiting** - Select this check-box to enable/disable suspending the current telephone call and switch to a new incoming call (Default: Disabled).
- **Call Waiting Timeout** - enter a number of seconds after which the call waiting is timed out (Default: 30 seconds).
- **Call Block** list - set up the numbers as follows:
  - » Incoming - blocks incoming calls from the listed numbers (up to 50 digits).
  - » Outcoming - blocks outgoing calls from the listed numbers (up to 50 digits).

# Chapter 9 - Engineering

## In this chapter:

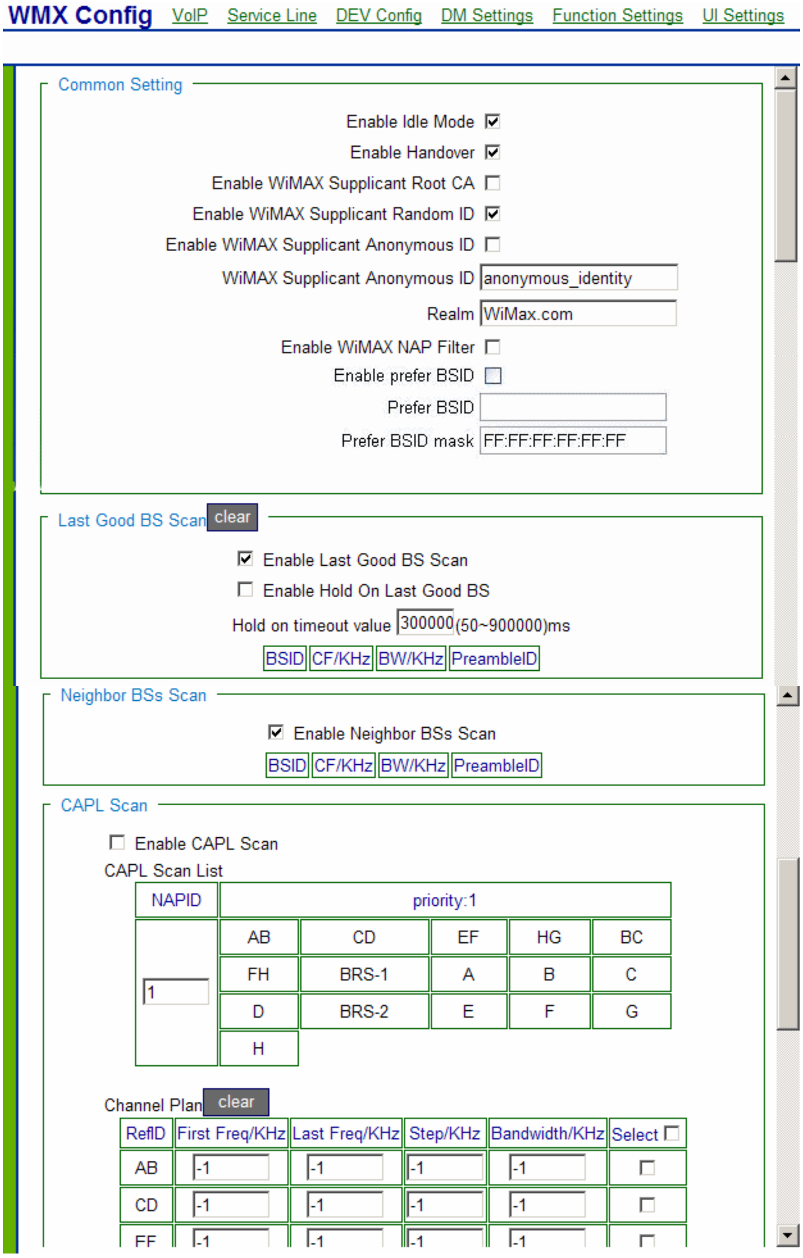
# 9.1 Introduction

The Engineering menu item is accessible to the Operator only and provides advanced CPE configuration parameters. The Engineering mode is available in a software package that is uploaded from the Status page; See "WiMAX Status" on page 67).

For detailed description of terms and abbreviations, refer to the "Glossary" on page 109.

# 9.2 WiMAX Configuration

In this page the operator defines WiMAX parameters for the CPE WiMAX connection functionality.



Common Setting

Enable Idle Mode ☑
Enable Handover ☑
Enable WiMAX Supplicant Root CA □
Enable WiMAX Supplicant Random ID ☑
Enable WiMAX Supplicant Anonymous ID □
WiMAX Supplicant Anonymous ID anonymous_identity
Realm WiMax.com
Enable WiMAX NAP Filter □
Enable prefer BSID □
Prefer BSID
Prefer BSID mask FF:FF:FF:FF:FF:FF

Last Good BS Scan clear

☑ Enable Last Good BS Scan
□ Enable Hold On Last Good BS
Hold on timeout value 300000(50~900000)ms

| BSID | CF/KHz | BW/KHz | PreambleID |
|---|---|---|---|

Neighbor BSs Scan

☑ Enable Neighbor BSs Scan

| BSID | CF/KHz | BW/KHz | PreambleID |
|---|---|---|---|

CAPL Scan

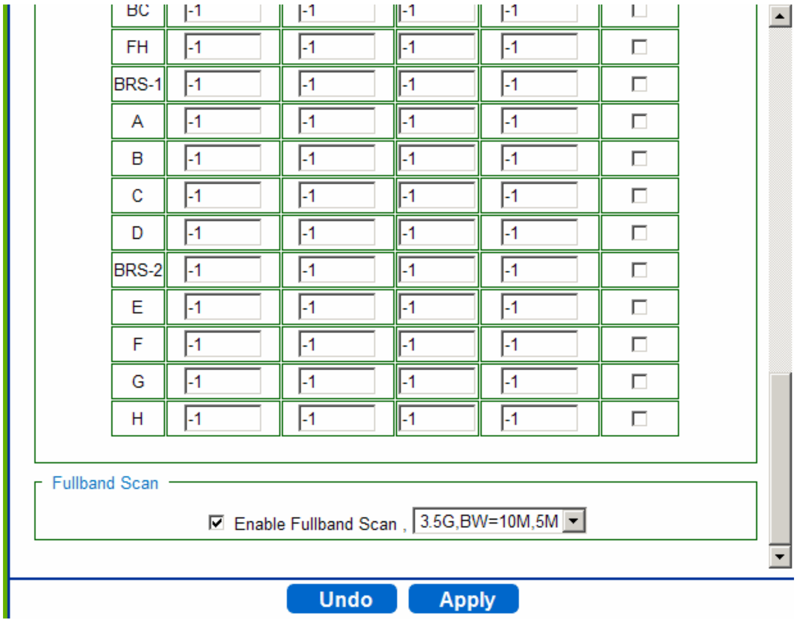
□ Enable CAPL Scan
CAPL Scan List

| NAPID | priority:1 | | | | |
|---|---|---|---|---|---|
| 1 | AB | CD | EF | HG | BC |
| | FH | BRS-1 | A | B | C |
| | D | BRS-2 | E | F | G |
| | H | | | | |

Channel Plan clear

| RefID | First Freq/KHz | Last Freq/KHz | Step/KHz | Bandwidth/KHz | Select □ |
|---|---|---|---|---|---|
| AB | -1 | -1 | -1 | -1 | □ |
| CD | -1 | -1 | -1 | -1 | □ |
| EF | -1 | -1 | -1 | -1 | □ |

**Figure 9-1: Engineering - WMAX Config.**



| | | | | | |
|---|---|---|---|---|---|
| BC | -1 | -1 | -1 | -1 | □ |
| FH | -1 | -1 | -1 | -1 | □ |
| BRS-1 | -1 | -1 | -1 | -1 | □ |
| A | -1 | -1 | -1 | -1 | □ |
| B | -1 | -1 | -1 | -1 | □ |
| C | -1 | -1 | -1 | -1 | □ |
| D | -1 | -1 | -1 | -1 | □ |
| BRS-2 | -1 | -1 | -1 | -1 | □ |
| E | -1 | -1 | -1 | -1 | □ |
| F | -1 | -1 | -1 | -1 | □ |
| G | -1 | -1 | -1 | -1 | □ |
| H | -1 | -1 | -1 | -1 | □ |

Fullband Scan

☑ Enable Fullband Scan , 3.5G,BW=10M,5M

**Figure 9-1: Engineering - WMAX Config. (Continued)**

The following table describes the WMAX Configuration parameters:

**Table 9-1: WMAX Config. Settings**

| Parameter | Description | Default | Possible Values |
|---|---|---|---|
| **Common Settings** | | | |
| Enable Idle Mode | Select this check-box to enable Idle Mode -the CPE is completely deregistered from the network, however will continue to scan the network and keep track of its location | Enable | Enable/disable |
| Enable Handover | Select this check-box to enable Handover - transfer to another BS during mobility | Enable | Enable/disable |
| Enable WiMAX Supplicant Root CA | IOT AAA root certificates are predefined in the CPE. Select this check-box to allow the CPE to verify BS's certification. | Disable | Enable/disable |
| Enable WiMAX Supplicant Random ID | Select this check-box to assign a random ID to the Supplicant. If disabled - the ID is the MAC_Address@realm. | Enable | Enable/disable |

Table 9-1: WMAX Config. Settings (Continued)

| Parameter | Description | Default | Possible Values |
|---|---|---|---|
| Enable WiMAX Supplicant Anonymous ID | If enabled, the unit will use "WiMAX Supplicant Anonymous ID" as anonymous identity, else the unit will use MAC_Address@realm instead. | Disable | Enable/disable |
| WiMAX Supplicant Anonymous ID | Enter the WiMAX Supplicant Anonymous ID to be used. | anonymous_identity | Up to 128 characters |
| Realm | The WiMAX domain | WiMax.com | |
| Enable WiMAX NAP Filter | Enables filtering Network Access Provider. If it is enabled - network provider ID will be checked for network entry. | Disable | Enable/disable |
| Enable Prefer BSID | When enabled, the CPE will connect to the preferred BS, whose details (ID and mask) are defined below. | Disable | Enable/disable |
| Prefer BSID | Enter an ID of the preferred base station. | N/A | |
| Prefer BSID mask | Enter a mask for the preferred base station. | N/A | |
| **Last Good BS Scan** | | | |
| Table of Last Good BSs | ■ BSID -Base Station ID<br>■ CF/KHz - Channel Frequency<br>■ BW/KHz - Bandwidth in KHz<br>■ PreambleID - The Preamble ID of the BS<br>Use the **Clear** button to delete a saved last good BS from the list. | N/A | N/A |
| Enable Last Good BSs Scan | The system will try to scan with the previous good BS to speed up the scan duration. A "good BS" is defined as one with which the CPE can get an IP address. | Enable | Enable/disable |
| Enable Hold On Last Good BS | The system will try to connect to the last good BS for the specified time defined below. | Enable | Enable/disable |

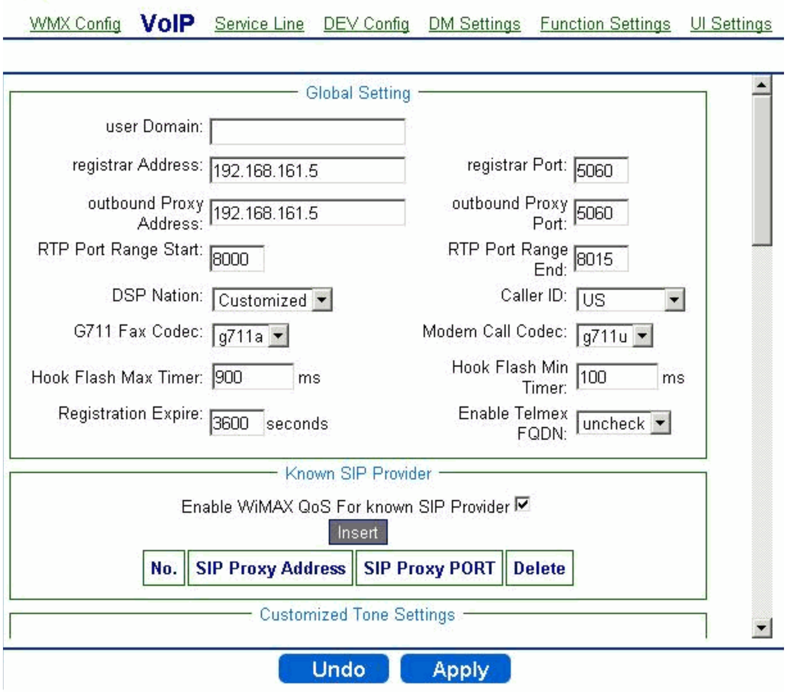
Table 9-1: WMAX Config. Settings (Continued)

| Parameter | Description | Default | Possible Values |
|---|---|---|---|
| Hold on timeout value | Enter the period of time (in milliseconds) to keep referring to this BS as the Last Good BS when connection is not optimal. | 300,000 | 50~900,000 ms |
| **Neighbor BS Scan** | | | |
| Enable Neighbor BS Scan | The system will try to scan the neighbor BS to the previous BS defined in "Last good BS". The neighbor BS details will appear in the table of this section. | Enable | Enable/disable |
| **CAPL BS Scan (Channel Allocation Priority Level)** | | | |
| NAPID | Sequential number of NAP | N/A | |
| Enable CAPL BS Scan | Channel Allocation Priority Level - The CAPL scan list is defined by the customer provisioned list. Priority is the customer defined priority scan order. Higher priority will be scanned first. | Disable | Enable/disable |
| Channel Plan | Define the channel plan by adding the Ref IDs, in order to map the IDs into a scan list. | N/A | |
| **Fullband Scan** | | | |
| Enable Fullband Scan | The system will try to scan the whole frequency band (250 kHz for the frequency step) with user specified bandwidth (5 MHz, 7 MHz, 10 MHz) | Enable | Enable/disable |

# 9.3 VoIP Configuration

The BreezeMAX PRO 6000 CPE uses Session Initiation Protocol (SIP) as the control mechanism that sets up, initiates, and terminates calls between a caller and a called party. The SIP messaging makes use of “Proxy,” “Redirect,” and “Registration” servers to process call requests and find the location of called parties across the Internet. When SIP has set up a call between two parties, the actual voice communication is a direct peer-to-peer connection using the standard Real-Time Protocol (RTP), which streams the encoded voice data across the network.

Before using the VoIP Phone port on the unit, the user must have an account with a SIP service provider and configure the required parameters through the web interface.



user Domain:

registrar Address: 192.168.161.5 registrar Port: 5060

outbound Proxy Address: 192.168.161.5 outbound Proxy Port: 5060

RTP Port Range Start: 8000 RTP Port Range End: 8015

DSP Nation: Customized Caller ID: US

G711 Fax Codec: g711a Modem Call Codec: g711u

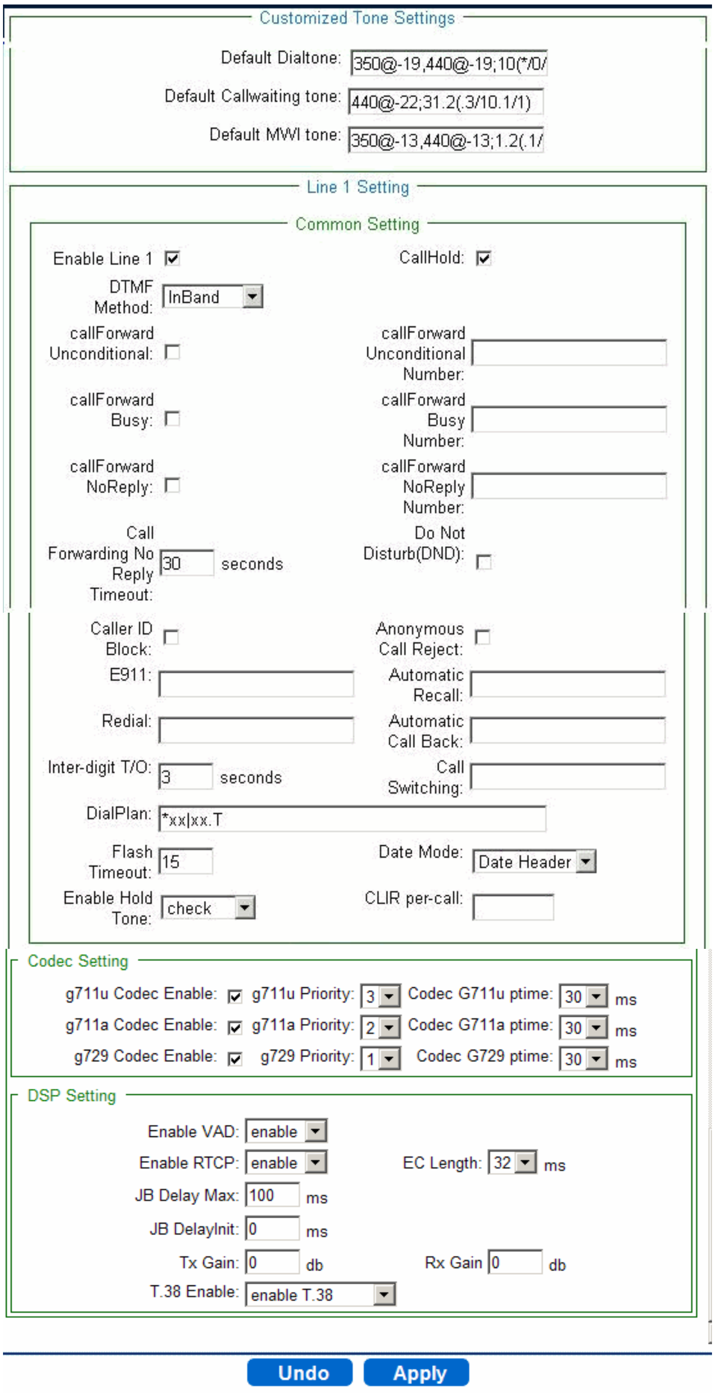
Hook Flash Max Timer: 900 ms Hook Flash Min Timer: 100 ms

Registration Expire: 3600 seconds Enable Telmex FQDN: uncheck

Enable WiMAX QoS For known SIP Provider ☑

| No. | SIP Proxy Address | SIP Proxy PORT | Delete |
|---|---|---|---|

Figure 9-2: Engineering - VoIP



Customized Tone Settings

Default Dialtone: 350@-19,440@-19;10(*/0/

Default Callwaiting tone: 440@-22;31.2(.3/10.1/1)

Default MWI tone: 350@-13,440@-13;1.2(.1/

Line 1 Setting

Common Setting

Enable Line 1 ☑

CallHold: ☑

DTMF Method: InBand

callForward Unconditional: □

callForward Unconditional Number:

callForward Busy: □

callForward Busy Number:

callForward NoReply: □

callForward NoReply Number:

Call Forwarding No Reply Timeout: 30 seconds

Do Not Disturb(DND): □

Caller ID Block: □

Anonymous Call Reject: □

E911:

Automatic Recall:

Redial:

Automatic Call Back:

Inter-digit T/O: 3 seconds

Call Switching:

DialPlan: *xx|xx.T

Flash Timeout: 15

Date Mode: Date Header

Enable Hold Tone: check

CLIR per-call:

Codec Setting

g711u Codec Enable: ☑ g711u Priority: 3 Codec G711u ptime: 30 ms

g711a Codec Enable: ☑ g711a Priority: 2 Codec G711a ptime: 30 ms

g729 Codec Enable: ☑ g729 Priority: 1 Codec G729 ptime: 30 ms

DSP Setting

Enable VAD: enable

Enable RTCP: enable

EC Length: 32 ms

JB Delay Max: 100 ms

JB DelayInit: 0 ms

Tx Gain: 0 db

Rx Gain 0 db

T.38 Enable: enable T.38

Figure 9-3: Engineering - VoIP (continued)

The following table describes the VoIP Settings parameters:

**Table 9-2: VoIP Settings**

| Parameter | Description | Default | Possible Values |
|---|---|---|---|
| **Global Settings** | | | |
| user Domain | The host portion of the SIP Uniform Resource Identifiers (URIs) that are assigned to users in a network. The SIP domain name can sometimes be different from the internal network domain name. | N/A | Up to 256 characters |
| registrar Address | The IP address of the SIP registrar server. A registrar is a server that accepts SIP register requests and places the information it receives in those requests into the location service for the domain it handles. | N/A | Up to 256 characters |
| registrar Port | The TCP port number used by the VoIP service provider’s register server. | 5060 | Range: 1030 to 65535 |
| outbound Proxy Address | Address of the VoIP service provider SIP proxy server. | N/A | Up to 256 characters |
| outbound Proxy Port | The TCP port number used by the VoIP service provider’s SIP proxy server. | 5060 | Range: 1030 to 65535 |
| RTP Port Range Start | Enter the port Start and End to define the range that Real-time Transport Protocol will use | 8000 | Range: 1030 to 65535 |
| RTP Port Range End | | 8015 | |
| DSP Nation | National protocol definition | Customized | |
| Caller ID | ■ Select the standard by which the caller is identified:<br>■ British TelecomDual-tone multi-frequency signaling standard | US | |
| G711 Fax Codec | Select the codec to convert fax signals into digital data to be transmitted over the Internet. | g711a | g711u<br>g711a |
| Modem Call Codec | Select the codec to be used for modem calls; when a modem call is detected, this codec will be used | g711u | g711u<br>g711a |

Table 9-2: VoIP Settings (Continued)

| Parameter | Description | Default | Possible Values |
|---|---|---|---|
| Hook Flash Max/Min. Timer | Enter a value (in milliseconds) to define how long should the hook be pressed as to be considered as flash (hook should be pressed for a time between min. and max. values) | Max: 0.9 ms<br>Min: 0.1 ms | 100 - 1550 ms |
| Registration Expire | Enter a value (in seconds) to define the time by which the CPE has to renew its subscription to the SIP server | 3600 seconds | 1 - 99999 seconds |
| Enable Telmex FQDN | Enable Request for Comments (RFC) 3263 "Locating SIP Servers" functionality. The Session Initiation Protocol (SIP) uses DNS procedures to allow a client to resolve a SIP Uniform Resource Identifier (URI) into the IP address, port, and transport protocol of the next hop to contact. It also uses DNS to allow a server to send a response to a backup client if the primary client has failed. This procedure uses the Fully-qualified domain name (FQDN). | Uncheck | Check/Uncheck |
| **Customized Tone Settings** | | | |
| Default Dial Tone | Defines the tone that will be heard during dialing. The string refers to tone, frequency, and cadence. | 350@-19,440@-19;10(*/0/1+2) | Set by the operator |
| Default Callwaiting Tone | Defines the tone that will be heard during call waiting. The string refers to tone, frequency, and cadence. | 440@-22;31.2(.3/10.1/1) | |
| Default MWI Tone | Defines a message-waiting indicator tone. The string refers to tone, frequency, and cadence. | 350@-13,440@-13;1.2(.1/.1/1+2);*(*/0/1+2) | |
| **Known SIP Provider** | | | |
| Enable WiMAX QoS For known SIP Provider | This check-box enables the CPE to select the quality of service level from a known SIP. This feature is used for MS initial service -flow. | Enabled | Enable/disable |
| List of SIP providers | Click **Insert** to add a known SIP provider to the list and specify the SIP Proxy address and Proxy port. To remove from the list, click **Del**. | N/A | |

**Table 9-2: VoIP Settings (Continued)**

| Parameter | Description | Default | Possible Values |
|---|---|---|---|
| **Line 1 Settings - Common Settings** | | | |
| Enable Line 1 | To enable voice feature | Disabled | Enable/disable |
| DTMF Method | Enable the sending of dual-tone multi-frequency (touch tone) phone signals over the VoIP connection:<br>■ InBand - The DTMF signals are sent over the RTP voice stream.<br>■ RFC2833 - Relay the DTMF signals over the RTP voice stream without any distortion<br>■ RFC2833+InBand - Uses the best method depending on the called party.<br>■ SIPInfo - Uses the data from SIP | RFC2833+ InBand | InBand, RFC2833, RFC2833+InBand, SIPInfo |
| callForward Unconditional | Forwards an incoming call to another number for all calls. | Disabled | Enable/disable |
| callForward Unconditional Number | Enter the number to which to forward all incoming calls. | N/A | Up to 256 characters |
| callForward Busy | Forwards an incoming call to another number when the current line is busy. | Disabled | Enable/disable |
| callForward Busy Number | Enter the number to which to forward incoming calls when the current line is busy. | N/A | |
| callForward NoReply | Incoming calls are forwarded to another phone number only if there is no answer after a pre-configured timeout. | Disabled | Enable/disable |
| Call Forwarding No Reply Timeout | The time (in seconds) a call waits for an answer before being forwarded to the number specified in callForward NoReply | 30 seconds | N/A |
| callForward NoReply Number | Enter the number to which to forward incoming calls when there is no reply from current line. | N/A | |
| Caller ID Block | Select this check-box to hide your name and number when calling another number. | Enable | Enable/disable |
| Anonymous Call Reject | Select this check-box to block calls from an unidentified number. | Disabled | Enable/disable |

Table 9-2: VoIP Settings (Continued)

| Parameter | Description | Default | Possible Values |
|---|---|---|---|
| E911 | Emergency call: Enter a number that will be referred to as the emergency call. When dialing “911” this call will be routed to the emergency service. | N/A | |
| Automatic Recall | Return call: Enables calling back the number whose call you missed. Enter a special number (e.g. *42). Dialing this number will recall the number that was missed in last incoming call. Empty field means Automatic Return Call is disabled | N/A | |
| Redial | Enter a shortcut (e.g. *53) to define redialing to the last number | N/A | |
| Automatic Call Back | Repeat dial if busy: automatically redial the number time and again. Define a special number (e.g.*52). Dialing this number after the busy tone received, will automatically redial the number until the recipient's line is free. Then your phone will ring back when you are being connected. Empty field means Automatic Return Call is disabled. | N/A | |
| Inter-digit T/O | Delay in call establishment (timeout in seconds) | 5 sec. | |
| Call Switching | Set a shortcut (e.g. *66) to enable switching from one phone to another without hanging up. Switching is done by pressing the flash button and dialing the shortcut number. | N/A | |
| DialPlan | Establish the expected number and pattern of digits for a telephone number | N/A | |
| Flash Timeout | When pressing Flash you have the time interval defined by this value to dial other numbers (e.g. for a conference call). If you do not dial a number within the specified time, you return to the initial call. | 15 seconds | Any number |
| Date Mode | Use date information from the Date header in the SIP message/NTP server | Date Header | Date Header/NTP |
| Enable Hold Tone | Select whether to play hold tone when put in hold. | Check | Check/Uncheck |

Table 9-2: VoIP Settings (Continued)

| Parameter | Description | Default | Possible Values |
|---|---|---|---|
| CLIR per-call | Enter a dialing prefix for Calling Line Identification Restriction (CLIR) per call, for example: *45 | N/A | Any number |
| CallHold | Enables holding the line while speaking with one participant in a conversation. | Disabled | Enable/disable |
| Do Not Disturb(DND) | Select this check-box to reject any incoming calls. The call will result in Busy tone. | Disabled | Enable/disable |
| **Codec Setting** | | | |
| g711u Codec Enable | The ITU-T G.711 with mu-law standard codec that uses Pulse Code Modulation (PCM) to produce a 64 Kbps high-quality voice data stream. This standard is used in North America and Japan. | Enable | Enable/disable |
| g711u Priority | The priority of codec by which the unit will attempt to use for best voice quality | Third priority | |
| g711u ptime | Set the time (in milliseconds) for the unit to attempt to use the codec highest priority in the list before trying the next lower one. | 30 ms | |
| g711a Codec Enable | (G711.aLaw): The ITU-T G.711 with A-law standard codec that uses Pulse Code Modulation (PCM) to produce a 64 Kbps high-quality voice data stream. This standard is used in Europe and most other countries around the world. | Enabled | Enable/disable |
| g711a Priority | The priority of codec by which the unit will attempt to use for best voice quality | Second priority | |
| g711a ptime | Set the time (in milliseconds) for the unit to attempt to use the codec highest priority in the list before trying the next lower one. | 30 ms | |
| g729 Codec Enable | The ITU-T G.729ab standard codec that uses Conjugate Structure Algebraic-Code Excited Linear Prediction (CS-ACELP) with silence suppression to produce a low-bandwidth data stream of 8 Kbps. Note that DTMF and fax tones do not transport reliably with this codec, it is better to use G.711 for these signals. | Enabled | Enable/disable |

Table 9-2: VoIP Settings (Continued)

| Parameter | Description | Default | Possible Values |
|---|---|---|---|
| g729 Priority | The priority of codec by which the unit will attempt to use for best voice quality | First priority | |
| g729 ptime | Set the time (in milliseconds) for the unit to attempt to use the codec highest priority in the list before trying the next lower one. | 30 ms | |
| **DSP Setting (Digital Signal Processing)** | | | |
| Enable VAD | Voice Activity Detection - detects the periods of silence in the audio stream so that it is not transmitted over the network. | Enabled | Enable/Disable |
| Enable RTCP | Select this check-box to enable Real-time Transport Control Protocol | Enable | Enable/Disable |
| EC Length | Echo Cancellation - Sets the delay time (in milliseconds) for voice echo cancellation. A voice echo can be created on some two-wire phone loops, which becomes increasingly louder and annoying when there is a long delay. If voice echo is a problem during a call, you can adjust this parameter to try and reduce or remove it. | 32 | 16, 32, 48 |
| JB Delay Max | Jitter Buffer control: JB delays the arriving packets so that the end user experiences a clear connection with very little sound distortion.<br>Set the maximum jitter buffer delay time (in milliseconds) | 100 ms | |
| JB DelayInit | The initial delay of the jitter buffer in milliseconds. The system holds the 1st received packet for the time defined in DelayInit before sending it out. | 0 ms | |
| Tx Gain | Enter a value (in db) to control the voice transmission quality | 0 | -5 to +5 |
| Rx Gain | Enter a value (in db) to control the voice receiving quality | 0 | -5 to +5 |

Table 9-2: VoIP Settings (Continued)

| Parameter | Description | Default | Possible Values |
|---|---|---|---|
| T.38 Enable | Select one of the options to send fax messages over the VoIP network from a fax machine connected to one of the RJ-11 Phone ports on the unit.<br>T.38 is a standard for sending FAX across IP networks in a real-time mode. | Enable T.38 | Enable T.38<br>Disable T.38<br>Enable T.38+WA (T.38 with Asterisk) |

# 9.4 Service Line

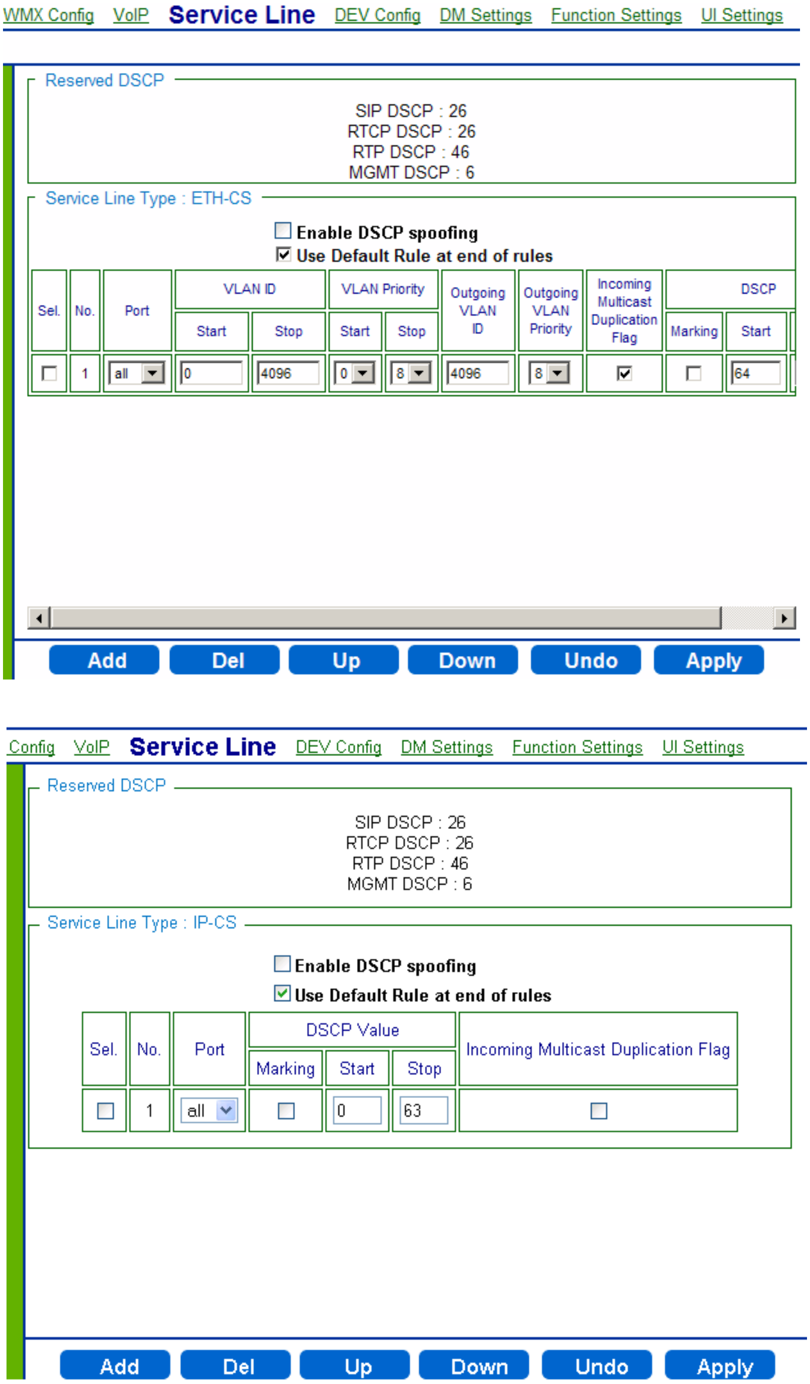
In the Service Line page you set the rules for data traffic. If the Marking check-box is not activated (marking disabled), then you can configure a range of DSCPs (Differentiated Services Code Point) as a rule. For uplink traffic, if the packets have the DSCP in the specified interval of a rule and are coming from the configured port, then a match is found and traffic is forwarded towards WAN. For downlink traffic, if the packets have the DSCP in the specified interval of a rule and the destination is on the configured port then the packets are forwarded towards LAN.

A rule with Marking enabled must have the same value for the start and stop DSCP. For uplink traffic, when a rule with marking enabled is encountered then the traffic is marked with the corresponding DSCP value, regardless of the existing DSCP value. For downlink traffic, packets coming from WAN are forwarded to the configured LAN port only if they have the configured DSCP value. The value of the DSCP field of the first incoming packet from the specified LAN port will be used to mark all the reply packets towards LAN.

For example, if the first coming packet from Ethernet LAN has the DSCP value 3, the second 5 and so on, and the Service Line rule is configured to mark the Ethernet LAN packets with 10 - all the reply packets coming from WAN with the DSCP 10 will be forwarded to LAN with DSCP 3.

Any combination of VLAN ID, VLAN Priority and DSCP Value parameters must be unique over all the configured service lines. Otherwise the service line configuration is rejected. The set of rules are verified one by one until a match is found. If a match is found the other rules are not checked anymore. The default rule permits all the traffic (DSCP value between 0 and 63.

For IP-CS, Bridge-IPCS (IP Conversion Sublayer) and Bridge-ETHCS (Ethernet Conversion Sublayer) service line types are available depending on the function settings defined by the operator (see "Function Settings" on page 106).



Reserved DSCP

SIP DSCP : 26
RTCP DSCP : 26
RTP DSCP : 46
MGMT DSCP : 6

Service Line Type : ETH-CS

□ Enable DSCP spoofing
☑ Use Default Rule at end of rules

| Sel. | No. | Port | VLAN ID | | VLAN Priority | | Outgoing VLAN ID | Outgoing VLAN Priority | Incoming Multicast Duplication Flag | DSCP | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Start | Stop | Start | Stop | | | | Marking | Start |
| □ | 1 | all | 0 | 4096 | 0 | 8 | 4096 | 8 | ☑ | □ | 64 |

Reserved DSCP

SIP DSCP : 26
RTCP DSCP : 26
RTP DSCP : 46
MGMT DSCP : 6

Service Line Type : IP-CS

□ Enable DSCP spoofing
☑ Use Default Rule at end of rules

| Sel. | No. | Port | DSCP Value | | | Incoming Multicast Duplication Flag |
|---|---|---|---|---|---|---|
| | | | Marking | Start | Stop | |
| □ | 1 | all | □ | 0 | 63 | □ |

**Figure 9-4: Engineering - Service Line (ETHCS and IP-CS)**

The following information is displayed:

**Reserved DSCP** - When DSCP spoofing is enabled, you cannot configure a rule with a range of DSCPs that contains one of the DSCPs reserved for SIP, RTP/RTCP, or MGMT. For example, if the values for SIP, RTP/RTCP, MGMT are 26/46/6, you cannot configure a rule that contains one of these values (DSCP start

4, DSCP stop 7 or DSCP start 20, DSCP stop 50). Also you cannot configure a rule to mark packets with one of these values. (See also "Function Settings" on page 106).

The following configuration parameters are available:

**Table 9-3: Service Line Parameters**

| Parameter | Description |
|---|---|
| Use Default Rule at end of rules | The default rule permits all the traffic (DSCP value between 0 and 63).If the default rule is enabled and none of the configured rules can be applied to the traffic, the default rule is applied. If the default rule is disabled and none of the rules matches the packets, then the packets are discarded. |
| Enable DSCP spoofing | When selected, packets containing Management or Voice DSCP value will be handled as follows:<br>■ coming from the LAN side - dropped<br>■ coming from the WAN side - routed to internal Management and Voice applications<br>When not selected, packets containing Management or Voice DSCP value will be handled as follows:<br>■ coming from the LAN side - passed through<br>■ coming from the WAN side - routed to internal Management and Voice applications according to the destination IP address and Port range, or forwarded to LAN according to the destination IP.<br>The default is not selected (DSCP spoofing disabled) |
| Sel. | Select this check-box to delete this row |
| No. | Display the number of this rule |
| Port | Set the port for IP-CS/ETHCS: eth (Ethernet) |
| VLAN ID | VLAN Identification of the data flow in LAN. Range: 1-4096 (4096 = Untagged) |
| VLAN Priority | VLAN Priority of the data flow in LAN. Range: 1-8 (8=No priority) |
| DSCP Value | ■ Marking - Select this check-box to tag packets in this line for classification. If you select this option, the Start and Stop values should be the same (Start=Stop)<br>■ Start /Stop - When Marking is disabled, enter a range of values, excluding the Internal Management, internal VoIP SIP and RTP DSCP reserved values. If the reserved values are in the range between start and stop, outgoing packets with these values will be dropped.<br>Default: start=0, stop=63. Range: 0-63. |

Table 9-3: Service Line Parameters (Continued)

| Parameter | Description |
|---|---|
| Incoming Multicast Duplication Flag | Select this check-box to enable duplication of multicast (VoIP, Data) packets. |

- Use the **Add** or **Del** buttons to add a rule to the group or clear it from the group.
- Use the **Up** or **Down** buttons to change the rules priority.
- Click **Apply** to activate your changes.

# 9.5 Device Configuration

In the Dev Config page you save and export all the parameters currently set on the device, packed in a file, to your PC. This file will be used as a configuration template in order to apply the same settings to other CPEs. The format of the exported file is *.tar, which will have to be converted into an *.ipk file format using the Auto-configuration tool (see "Configuring the Unit Using the WiMAX Modem Application CD" on page 26).

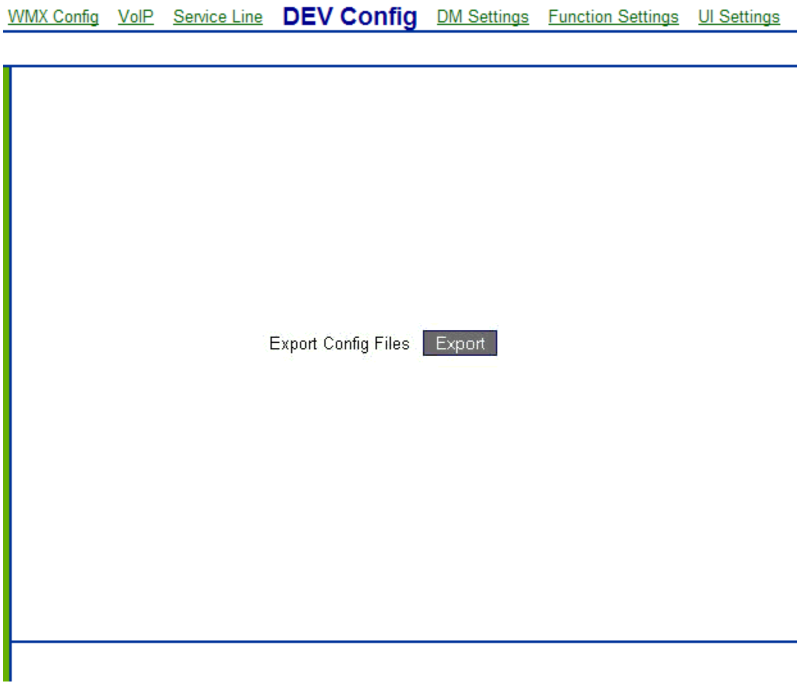


Figure 9-5: Engineering - DEV Config.

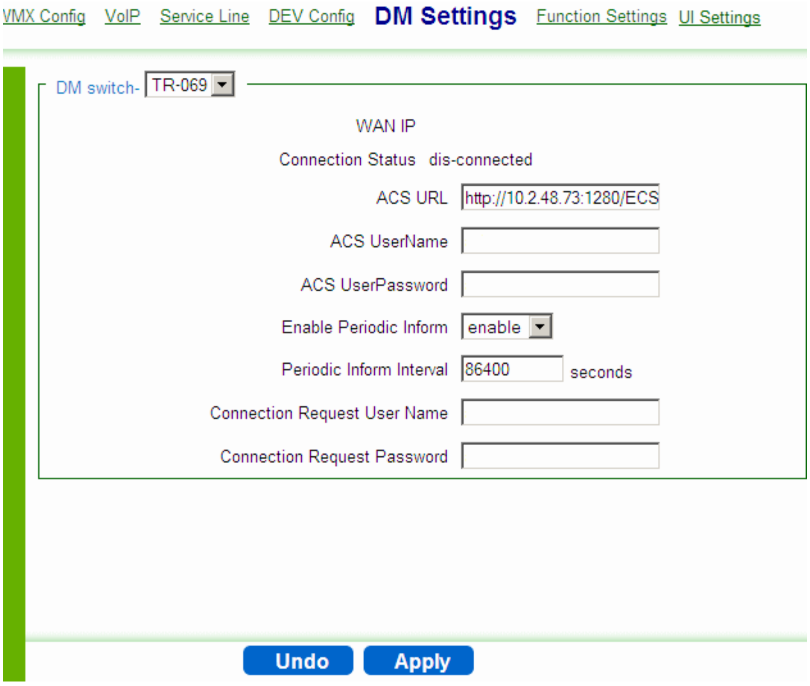
**To save and export the current device settings:**

1. Set the device parameters as required in each of the application pages. Be sure to click **Apply** to activate your changes.
2. In the Dev Config page click **Export** to save the current settings and export as a *.tar file.
3. Save the file (.*tar format) for mass CPE configuration (see "Creating a Default Configuration File" on page 31).

# 9.6 DM (Device Management) Settings

## 9.6.1 TR-069

In the DM Settings page you can set parameters for TR-069. TR-069 is a bidirectional SOAP/HTTP based protocol that provides the communication between CPE and Auto Configuration Servers (ACS). It includes both a safe auto configuration and the control of other CPE management functions within an integrated framework.



DM switch- TR-069

WAN IP

Connection Status dis-connected

ACS URL http://10.2.48.73:1280/ECS

ACS UserName

ACS UserPassword

Enable Periodic Inform enable

Periodic Inform Interval 86400 seconds

Connection Request User Name

Connection Request Password

**Figure 9-6: Engineering - DM Settings (TR-069)**

The following table describes the configurable TR-069 parameters:

**Table 9-4: DM Settings - TR-069**

| Parameter | Description | Default | Possible Values |
|---|---|---|---|
| WAN IP | Management IP of the device | N/A | N/A |
| Connection Status | Displays the CPE connection state | N/A | Connected/ disconnected |
| ACS URL | Enter the URL of the ACS server | N/A | N/A |
| ACS UserName | Enter the username for the ACS application | CPEmac@wimax.com | Up to 256 characters |

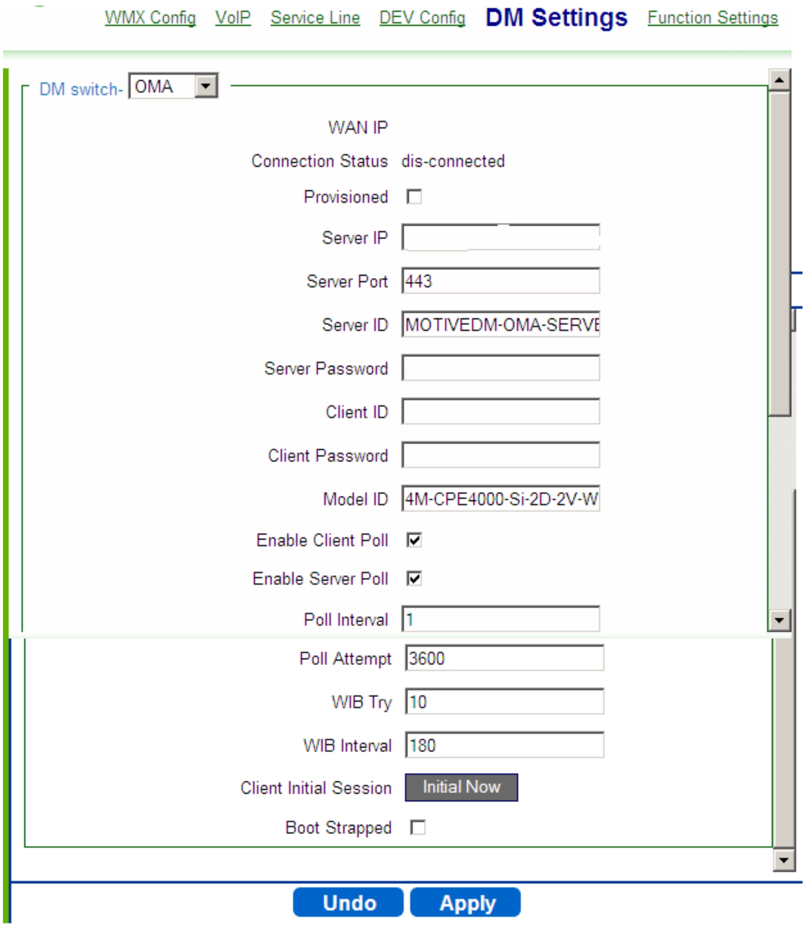
Table 9-4: DM Settings - TR-069

| Parameter | Description | Default | Possible Values |
|---|---|---|---|
| ACS UserPassword | Enter the password for the ACS application | quickynikynyoky | Up to 256 characters |
| Enable Periodic Inform | Select this check-box to enable the CPE to send periodical information messages to the ACS | Enable | Enable/disable |
| Periodic Inform Interval | Set the interval (in seconds) for sending messages from CPE to ACS | 3600 seconds | Less than defined in ACS |
| Connection Request User Name | Enter the CPE username for connecting with ACS. | CPEmac@wimax.com | Up to 256 characters |
| Connection Request Password | Enter the CPE password for connecting with ACS. | quickynikynyoky | Up to 256 characters |

## 9.6.2 OMA Device Management Parameters

OMA DM is a protocol specified by Open Mobile Alliance (OMA) for Device Management (DM) purposes, by the Device Management Working Group and the Data Synchronization (DS) Working Group.

The WiMax broadband modem can be remotely managed by a remote device management server using the OMA-DM protocol.



DM switch- OMA

| | |
|---|---|
| WAN IP | |
| Connection Status | dis-connected |
| Provisioned | □ |
| Server IP | |
| Server Port | 443 |
| Server ID | MOTIVEDM-OMA-SERVE |
| Server Password | |
| Client ID | |
| Client Password | |
| Model ID | 4M-CPE4000-Si-2D-2V-W |
| Enable Client Poll | ☑ |
| Enable Server Poll | ☑ |
| Poll Interval | 1 |
| Poll Attempt | 3600 |
| WIB Try | 10 |
| WIB Interval | 180 |
| Client Initial Session | Initial Now |
| Boot Strapped | □ |

**Figure 9-7: Engineering - DM Settings (OMA)**

The following table describes the configurable OMA parameters:

**Table 9-5: DM Settings - OMA**

| Parameter | Description | Default | Possible Values |
|---|---|---|---|
| WAN IP | Management IP of the device | N/A | N/A |
| Connection Status | Displays the CPE connection state | N/A | Connected/ disconnected |
| Provisioned | Select this check-box to allow checking if the device is activated or not. | Disable | Enable/disable |
| Debug | Select this check-box to allow debugging of the device. | Disable | Enable/disable |
| Server IP | IP address of the OMA server | | |
| Server Port | Port number of the OMA server | | |

**Table 9-5: DM Settings - OMA**

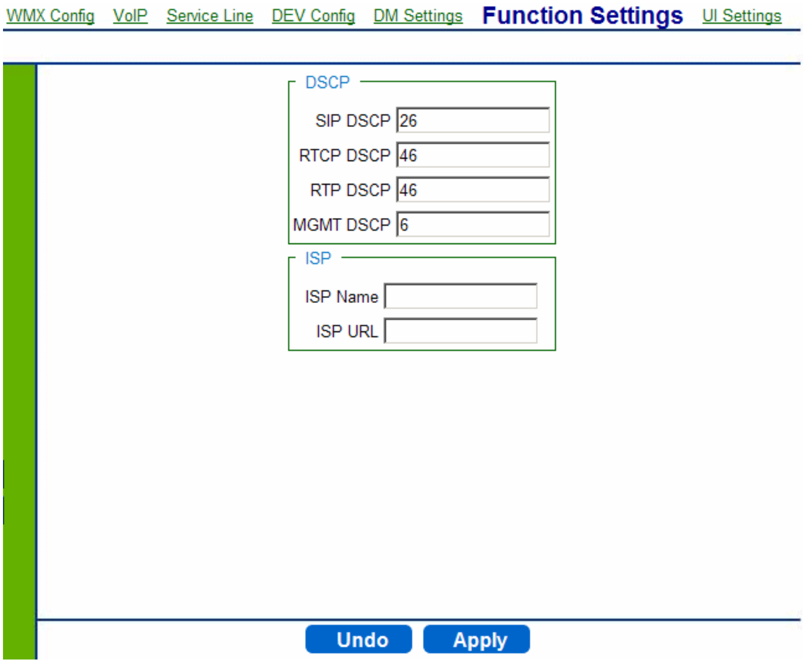
| Parameter | Description | Default | Possible Values |
|---|---|---|---|
| Server ID | The OMA server authentication user name | | |
| Server Password | Authentication password of the OMA server | | Up to 128 characters |
| Client ID | OMA client authentication user name | WiMAXCPE | Up to 128 characters |
| Client Password | OMA client authentication password | admin | Up to 128 characters |
| Model ID | The device model ID. OMA DM client uses this ID in communication sessions. The server uses this ID to identify the client. | 4M-CPE6000-PRO-1D_1V | |
| Enable Client Poll | Select this check-box to enable OMA DM client polling mechanism. | Enable | |
| Enable Server Poll | Select this check-box to enable an initial session between the server and client. | Enable | |
| Poll Interval | If the client polling mechanism is enabled, the client will follow this interval (in minutes) for polling. | 1 | |
| Poll Attempt | Enter the number of attempts for client polling | 2 | |
| WIB Try | The number of WIB (Wireless Initial Bootstrap) re-try that the client will try to do. | 0 | |
| WIB Interval | The interval (in seconds) between WIB actions. | 180 | |
| Network Entry Delay Time | | 0 | |

Table 9-5: DM Settings - OMA

| Parameter | Description | Default | Possible Values |
|---|---|---|---|
| Server Nonce | A string used only once for the first session until the ID and password are set. The server nonce is used in an OMA DM session when a device authenticates the server. For the device to connect to the server, the nonce that is stored in the device must be the same as the nonce that the server has. | 1234 | |
| Client Nonce | | 1234 | |
| Client Initial Session | Click **Initial Now** to start a contact and send a poll to the server. | N/A | |
| Boot Strapped | If client already has an OMA DM profile set with the parameters described above, this check-box is checked automatically. | Disable | Enable/Disable |

# 9.7 Function Settings

In this page you reserve DSCP (Differentiated Services Code Point) markings for classification settings and set the ISP details.



DSCP

SIP DSCP 26

RTCP DSCP 46

RTP DSCP 46

MGMT DSCP 6

ISP

ISP Name

ISP URL

**Figure 9-8: Engineering - Function Settings**

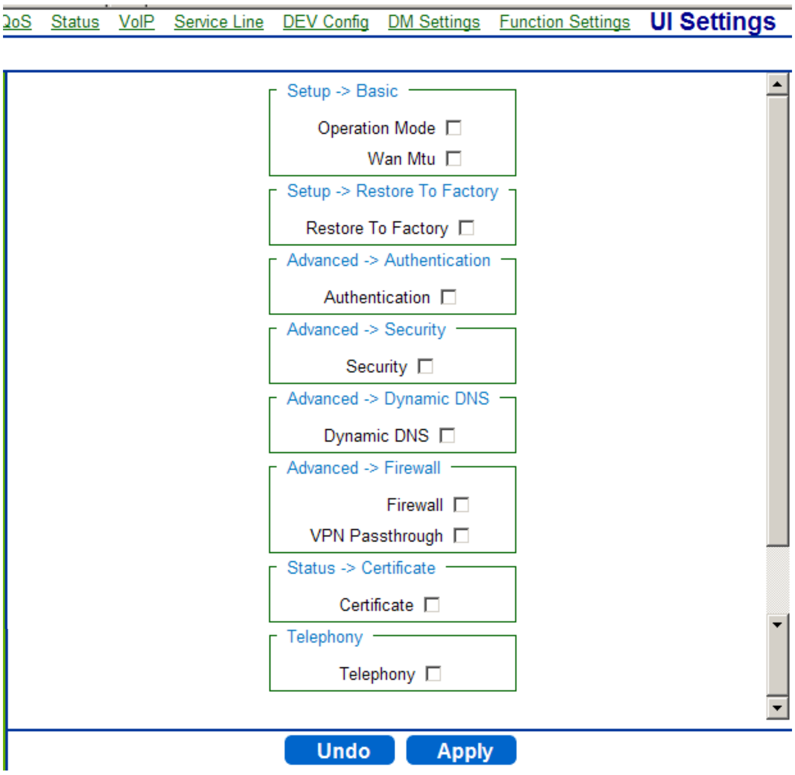
The following table describes the configurable Function Setting parameters:

**Table 9-6: Function Settings**

| Parameter | Description | Default | Possible Values |
|---|---|---|---|
| **DSCP (Differentiated Services Code Point)** | | | |
| SIP DSCP | Session Initiation Protocol | 26 | 0-63 |
| RTCP DSCP | Real Time Voice Control Protocol | 46 | 0-63 |
| RTP DSCP | Real Time Voice | 46 | 0-63 |
| MGMT DSCP | Management | 6 | 0-63 |
| **ISP (Internet Service Provider)** | | | |
| ISP Name | Name of the internet service provider | N/A | |
| ISP URL | URL of the internet service provider | N/A | |

# 9.8 UI Settings

This window enables controlling the User Interface of the subscriber. Selecting the features in this window disables the accessibility and availability of features for the end-user.



Setup -> Basic
Operation Mode ☐
Wan Mtu ☐

Setup -> Restore To Factory
Restore To Factory ☐

Advanced -> Authentication
Authentication ☐

Advanced -> Security
Security ☐

Advanced -> Dynamic DNS
Dynamic DNS ☐

Advanced -> Firewall
Firewall ☐
VPN Passthrough ☐

Status -> Certificate
Certificate ☐

Telephony
Telephony ☐

**Figure 9-9: Engineering - UI Settings**

The following table describes the configurable UI Setting parameters:

**Table 9-7: UI Settings Parameters**

| Parameter | Description | Comments |
|---|---|---|
| Setup > Basic | ■ Operation Mode - select this check-box to disable the option to modify the operation mode by the user.<br>■ Wan Mtu - select this check-box to disable the option to modify the WAN Mtu by the user. | Selecting both options makes the Setup > Basic page unavailable to the subscriber.<br>See also "Setting Basic Parameters" on page 37 |
| Setup > Restore To Factory | Restore To Factory - select this check-box to disable the option to restore parameters by the user. | Selecting this option makes the Setup > Restore To Factory page unavailable to the subscriber. |

Table 9-7: UI Settings Parameters (Continued)

| Parameter | Description | Comments |
|---|---|---|
| Advanced > Authentication | Authentication - select this check-box to disable the option to set Authentication parameters by the user. | See also "Setting Advanced Parameters" on page 49 |
| Advanced > Security | Security - select this check-box to disable the option to set Security parameters by the user. | |
| Advanced > Dynamic DNS | Dynamic DNS - select this check-box to disable the option to set DDNS parameters by the user. | Selecting this option makes the Advanced > Dynamic DNS page unavailable to the subscriber. |
| Advanced - Firewall | ■ Firewall - select this check-box to disable the option to set Firewall parameters by the user.<br>■ VPN Passthrough - select this check-box to disable the option to set VPN Passthrough parameters by the user. | See "Firewall" on page 55 |
| Status - Certificate | Certificate - select this check-box to disable the option to view and set the certificates by the user. | Selecting this option makes the Status > Certificate page unavailable to the subscriber<br>See "Certificate Status" on page 74 |
| Telephony | Telephony - select this check-box to disable the option to view the telephony parameters by the user. | Selecting this option makes the Telephony menu item unavailable to the subscriber<br>See "Configuring Telephony Parameters" on page 77 |

# Glossary

**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

**Advanced Encryption Standard (AES)**

An strong encryption algorithm that implements symmetric key cryptography.

**Access List (ACL)**

A list of MAC addresses which are allowed to access the device

**Automatic Gain Control (AGC)**

Automatic electronic regulation by recording devices of video and audio signals at a predetermined rate (by electronic control).

**Authentication**

The process to verify the identity of a client requesting network access. IEEE 802.11 specifies two forms of authentication: open system and shared key.

**Auto-negotiation**

Signalling 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.

**Best Effort (BE)**

One of the five QoS service types defined in the IEEE 802.16 WiMAX.

**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.

**Broadcast Key**

Broadcast keys are sent to stations using 802.1X dynamic keying. Dynamic broadcast key rotation is often used to allow the access point to generate a random group key and periodically update all key-management capable wireless clients.

**Channel Allocation Priority Level (CAPL)**

CAPL scan list is defined by the customer provisioned list. There are some parameters with CAPL scan: NAPID, priority and RefID.

NAPID is used to filter some BS if the NAPID is not matched.

Priority is the customer defined priority scan order. Higher priority will be scanned first.

RefID is a result of mapping from IDs into a scan list from the channel plan.

**CINR**

Carrier to Interference-plus-Noise Ratio (CINR), expressed in decibels (dBs), is a measurement of signal effectiveness. The carrier is the desired signal, and the interference can either be noise or co-channel interference or both. In order for the signal receiver to be able to decode the signal, the signal must fall into an acceptable CINR range, which differs with the technology used (i.e., CDMA, GSM, etc.).

**Clear to Send (CTS)**

Signal that gives a modem permission to send data.

**Calling Line Identification Restriction (CLIR)**
Controls the presentation of caller identity (via CLIP-Calling Line Identification Presentation) in GSM networks. If CLIR is enabled, the caller’s MSC (Mobile Switching Centre) indicates this restriction to the destination MSC. The identity is then not forwarded to the destination mobile station.

**Customer Premise Equipment (CPE)**
Customer Premise Equipment: Communications equipment that resides on the customer's premises.

**Dynamic Host Configuration Protocol (DHCP)**
A protocol used to assign IP addresses to computers on a Microsoft NT local area network

**Domain Name System (DNS)**
A mechanism used for translating host names for network nodes into IP addresses.

**Dynamic Domain Name System (DDNS)**
A method, protocol, or network service that provides the capability for a networked device to notify a domain name server to change the active DNS configuration of its configured hostnames, addresses or other information stored in DNS, in real-time.

**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.

**(“Demilitarized Zone”) DMZ**
A server that acts as "neutral zone" and separates an internal network from a public one (in order to prevent outside access to a company's private data.

**Data/Digital Signal Processor (DSP)**
A system that controls voice quality

**Differentiated Services Code Point (DSCP)**
A field in the header of IP packets for packet classification purposes.

**Dual Tone Multi Frequency (DTMF)**
Allocation of a unique tone to each button on an appliance (made up of two frequencies - high and low) that allows a computer to recognize the tone.

**Extended Real-time POLLING SERVICE (ertPS)**
One of the five QoS service types defined in the IEEE 802.16 WiMAX.

**Ethernet**
A popular local area data communications network, which accepts transmission from computers and terminals.

**Ethernet Conversion Sublayer (ETH CS)**
A mode in which transmitted packets contain an 802.3 header

**Encryption**
Data passing between the SU-A-EZ and clients can use encryption to protect from interception and evesdropping.

**Extended Service Set (ESS)**
Extended Service Set: More than one wireless cell can be configured with the same Service Set Identifier to allow mobile users can roam between different cells with the Extended Service Set.

**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

**EAP-Tunneled Transport Layer Security (EAP-TTLS)**

An EAP protocol that extends TLS. (see “Transport Layer Security (TLS)” on page 115)

**File Transfer Protocol (FTP)**

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

**Fully-qualified Domain Name (FQDN)**

A fully-qualified domain name (FQDN), sometimes referred to as an absolute domain name, is a domain name that specifies its exact location in the tree hierarchy of the Domain Name System (DNS). It specifies all domain levels, including the top-level domain, relative to the root domain. A fully-qualified domain name is distinguished by this absoluteness in the name space.

**Hypertext Transfer Protocol (HTTP)**

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

**IDENT**

An Internet protocol that helps identify the user of a particular TCP connection.

**IEEE 802.16e**

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

**Internet Low Bitrate Codec (iLBC)**

A free speech codec suitable for robust voice communication over IP. The codec is designed for narrow band speech and results in a payload bit rate of 13.33 kbit/s with an encoding frame length of 30 ms and 15.20 kbps with an encoding length of 20 ms. The iLBC codec enables graceful speech quality degradation in the case of lost frames, which occurs in connection with lost or delayed IP packets.

**IP Conversion Sublayer (IP-CS)**

A mode in which transmitted packets contain an 802.3 header

**Itsy Package Management System (IPKG, ipkg)**

Itsy Package Management System - a lightweight package management system designed for embedded devices.

**Internet Protocol Security (IPsec)**

A protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream.

**Jitter Buffer (JB)**

A shared data area where voice packets can be collected, stored, and sent to the voice processor in evenly spaced intervals. Variations in packet arrival time, called jitter, can occur because of network congestion, timing drift, or route changes. The jitter buffer, which is located at the receiving end of the voice connection, intentionally delays the arriving packets so that the end user experiences a clear connection with very little sound distortion.

**Local Area Network (LAN)**

Local Area Network: A group of interconnected computer and support devices.

**Layer 2 Tunneling Protocol (L2TP)**

A tunneling protocol used to support virtual private networks (VPNs).

**Media Access Control (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 6bytes long and are controlled by the IEEE.

**Maximum Transmission Unit (MTU)**

Largest size of a data packet or frame that can be sent in one complete unit over a packet-based computer network

**Multiple Input Multiple Output (MIMO)**

Using multiple antennas in a Wi-Fi device to improve performance and throughput.

**MSCHAPV2 (MS-CHAP. v2)**

Microsoft version of the Challenge-handshake authentication protocol, version 2. MS-CHAPv2 provides mutual authentication between peers by adding a peer challenge upon the Response packet and an authenticator response on the Success packet.

**Network Access Point (NAP)**

Network exchange point equipped with large-scale switching facilities and serving as a connection point between individual Internet Service Providers

**Network Address Translation (NAT)**

A system for reusing IP addresses - The process of modifying network address information in datagram packet headers, while in transit, across a router, in order to remap a given address space into another.

**Network Time Protocol (NTP)**

NTP is a protocol designed to synchronize the clocks of computers over a network. The time servers operate in a hierarchical-master-slave configuration in order to synchronize local clocks within the subnet and to national time standards via wire or radio.

**Open Mobile Alliance (OMA)**

OMA DM (device Management) is a protocol specified by Open Mobile Alliance (OMA) for Device Management purposes, by the Device Management Working Group and the Data Synchronization (DS) Working Group.

**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.

**Physical Layer Device (PHY)**

The term used for a transceiver in Fast Ethernet and Gigabit Ethernet systems.

**Plain Old Telephone Service (POTS)**

Standard analog telephone service, regular telephone line without extra enhancements

**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 the locating of Wi$^2$s and network devices, and significantly decreased installation costs.

**Point to Point Tunneling Protocol (PPTP)**

This protocol enables the transfer of data packets of TCP / IP through a foreign network that is not based on these protocols (by marking the packet with an address suited to the foreign network)

**Quadrature Phase Shift Keying (QPSK)**

A digital modulation scheme that conveys data by changing, or modulating, the phase of a reference signal (the carrier wave).

**Request for Comments (RFC)**

A memorandum published by the Internet Engineering Task Force (IETF) describing methods, behaviors, research, or innovations applicable to the working of the Internet and Internet-connected systems.

**Received signal strength indication (RSSI)**

A measurement of the power present in a received radio signal.

RSSI is generic radio receiver technology metric, which is usually invisible to the user of device containing the receiver, but is directly known to users of wireless networking of
IEEE 802.11 protocol family.

**Real-time Transport Protocol (RTP)**

The Real-time Transport Protocol (RTP) defines a standardized packet format for delivering audio and video over the Internet.

**Real-time Transport Control Protocol (RTCP)**

Real-time Transport Control Protocol (RTCP) is a sister protocol of the Real-time Transport Protocol (RTP).

RTCP provides out-of-band control information for an RTP flow. It partners RTP in the delivery and packaging of multimedia data, but does not transport any data itself. It is used periodically to transmit control packets to participants in a streaming multimedia session. The primary function of RTCP is to provide feedback on the quality of service being provided by RTP.

**RTS Threshold**

Transmitters contending for the medium may not be aware of each other. RTS/CTS mechanism can solve this “Hidden Node Problem”. If the packet size is smaller than the preset RTS Threshold size, the RTS/CTS mechanism will NOT be enabled.

**Service Set Identifier (SSID)**

An identifier that is attached to packets sent over the wireless LAN and functions as a password for joining a particular radio cell; i.e., Basic Service Set (BSS).

**Session Key**

Session keys are unique to each client, and are used to authenticate a client connection, and correlate traffic passing between a specific client and the AU-EZ.

**Shared Key**

A shared key can be used to authenticate each client attached to a wireless network. Shared Key authentication must be used along with the 802.11 Wireless Equivalent Privacy algorithm.

**Session Initiation Protocol (SIP)**

An application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. It can be used to create two-party, multiparty, or multicast sessions that include Internet telephone calls, multimedia distribution, and multimedia conferences.

**Simple Network Management Protocol (SNMP)**

Simple Network Management Protocol: The application protocol in the Internet suite of protocols which offers network management services.

**Simple Network Time Protocol (SNTP)**

SNTP allows a device to set its internal clock based on periodic updates from a Network Time Protocol (NTP) server. Updates can be requested from a specific NTP server, or can be received via broadcasts sent by NTP servers.

**Single Input Single Output (SISO)**

A form of antenna technology for wireless communications in which a single antenna at both the transmitter and at the destination (receiver) are used.

**Subscriber Station**

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

**Temporal Key Integrity Protocol (TKIP)**

Temporal Key Integrity Protocol - a security protocol used in Wi-Fi Protected Access (WPA). Unlike WEP, TKIP provides per-packet key mixing, a message integrity check and a rekeying mechanism. TKIP ensures that every data packet is sent with its own unique encryption key.

**TR-069 (Technical Report 069)**

A DSL Forum technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices.

It provides the communication between CPE and Auto Configuration Servers (ACS).

**Trivial File Transfer Protocol (TFTP)**

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

**Transport Layer Security (TLS)**

A cryptographic protocol that provides security for communications over networks such as the Internet. TLS  encrypts the segments of network connections at the Transport Layer end-to-end.

**Point to Point Tunneling Protocol (PPTP)**

protocol that enables the transfer of data packets of TCP / IP through a foreign network that is not based on these protocols (by marking the packet with an address suited to the foreign network)

**Unsolicited Grant Service  (UGS)**

One of the five QoS service types defined in the IEEE 802.16 WiMAX. It is designed to support real-time service flows that generate fixed-size data packets on a periodic basis, such as T1/E1 and Voice over IP without silence suppression.

**User Datagram Protocol (UDP))**

Protocol with no connection required between sender and receiver that allows sending of data packets on the Internet (thought unreliable because it cannot ensure the packets will arrive undamaged or in the correct order)

**Universal Plug and Play Internet Gateway Device (UPnP IGD)**

A set of networking protocols promulgated by the UPnP Forum. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home and in corporate environments for simplified installation of computer components.

**UTP**

Unshielded twisted-pair cable.

**VoicE Activity Detection (VAD**

Enables the detection of periods of silence in the audio stream so that it is not transmitted over the network.

**Wide Area Network (WAN)**

Communications network intended to connect between remote local area networks

**Wired Equivalent Privacy (WEP)**

Wired Equivalent Privacy: WEP is based on the use of security keys and the popular RC4 encryption algorithm. Wireless devices without a valid WEP key will be excluded from network traffic.

**Wireless Application Protocol (WAP)**

Wireless Application Protocol (WAP) is an open international standard for application-layer network communications in a wireless-communication environment. Most use of WAP involves accessing the mobile web from any mobile device  or phone.

**Wi-Fi Protected Access (WPA)**

Wi-Fi Protected Access (WPA and WPA2) is a certification program developed to indicate compliance with the security protocol to secure wireless computer networks. The WPA protocol implements the majority of the IEEE 802.11i standard. WPA2 implements the mandatory elements of the 802.11i standard.

**WiFi Protected Access, Pre-Shared Key (WPA PSK)**

WPA (see above) utilizes 128-bit encryption keys and dynamic session keys to ensure the wireless network's privacy and enterprise security.

There are two basic forms of WPA:

- WPA Enterprise (requires a Radius server)
- WPA Personal (also known as WPA-PSK)

**Virtual Private Network (VPN)**

A private communications network that is based on the public network and uses information security and channeling protocol in order to maintain security of information transferred over the general network.