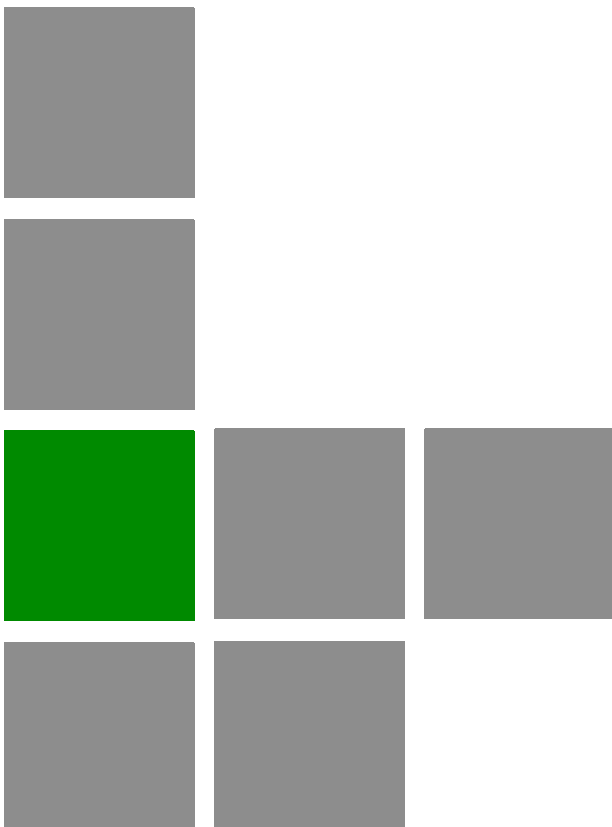




# BreezeMAX<sup>®</sup> Si 4000 CPE



## User Manual

Software Version: 2.0  
December 2010  
P/N 215801

## Document History

Topic	Description	Date Issued
BreezeMAX Si 4000 CPE Manual	This is the document's first release.	March 2010
General	<ul style="list-style-type: none"> <li>■ For changes that require device reset, the device will automatically initiate reset after clicking the Apply button.</li> <li>■ "Internet" menu item changed to "WiFi" in the Main menu</li> <li>■ Username and password are for all user levels (admin, admin)</li> </ul>	Ver.1.0M August 2010
<a href="#">"Wireless Security" on page 58</a>	<ul style="list-style-type: none"> <li>■ Added information on authentication options</li> </ul>	Ver.1.0M August 2010
Help	New <b>Help</b> button was added to initiate online help	Ver.1.0M August 2010
<a href="#">Table 3-1</a>	Added default information	Ver.1.0M August 2010
Setup > Basic > Connection Mode	Added a note: Static IP is not supported by 4Motion equipment	Ver.1.0M August 2010
"Advance" menu item	Changed to "Advanced"	Ver.1.0M August 2010
<a href="#">Chapter 5 Title</a>	Changed to "Configuring WiFi Parameters"	Ver.1.0M August 2010
WiFi > Wireless Settings	<ul style="list-style-type: none"> <li>■ Network Name (SSID) – Default: WiMAXCPE</li> <li>■ SSID Suppress – Default: Disable</li> </ul>	Ver.1.0M August 2010
<a href="#">"Wireless Security" on page 58</a>	Authentication - Default: Open System	Ver.1.0M August 2010
Authentication, Security and Dynamic DNS	Moved from Internet menu to the Advanced menu.	Ver.1.0M August 2010
Advanced > Security	Added a note: To access from WAN, use <a href="https://CPE_WAN_IP_Address:8080">https://CPE_WAN_IP_Address:8080</a> .	Ver.1.0M August 2010
Telephony	Added chapter	Ver.1.0M August 2010
VoIP parameters: <ul style="list-style-type: none"> <li>■ Call Waiting enable /disable</li> <li>■ Call waiting timeout specification</li> <li>■ Call Block Specification table (per line)</li> </ul>	Moved these items from the Engineering menu to the Telephony menu	Ver.1.0M August 2010

Topic	Description	Date Issued
Service Line	Moved from the Advanced Menu to Engineering	Ver.1.0M August 2010
General	<ul style="list-style-type: none"> <li>■ New CPE model - BreezeMAX 4000 Si Premium</li> <li>■ New 3.3-3.4 GHz band</li> </ul>	Ver. 2.0 October 2010
<a href="#">“Setting Basic Parameters” on page 44</a>	Added Bridge-IPCS and Bridge-ETHCS support description	Ver.2.0 November 2010
<a href="#">“DHCP Server” on page 65</a>	DHCP Ending IP Address default is 192.168.254.5	Ver.2.0 November 2010

## Legal Rights

© Copyright 2011 Alvarion Ltd. All rights reserved.

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<sup>®</sup>, BreezeCOM<sup>®</sup>, WALKair<sup>®</sup>, WALKnet<sup>®</sup>, BreezeNET<sup>®</sup>, BreezeACCESS<sup>®</sup>, BreezeLINK<sup>®</sup>, BreezeMAX<sup>®</sup>, BreezeLITE<sup>®</sup>, BreezePHONE<sup>®</sup>, 4MOTION<sup>®</sup> 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's 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).

## Safety Information

### Electronic Emission Notices

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

### FCC Radiation Hazard Warning

To comply with FCC RF exposure requirements in Section 1.1307 and 2.1091 of FCC Rules, the antenna used for this transmitter must be kept at a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

### Radio Frequency Interference Statement

The BreezeMAX Si 4000 CPE has been tested and found to comply with the limits for a class B digital device, pursuant to part 15 of the FCC rules and to EN 301 489-1 rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential environment notwithstanding use in commercial, business and industrial environments. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

### R&TTE Compliance Statement

This equipment complies with the appropriate essential requirements of Article 3 of the R&TTE Directive 1999/5/EC.

### Caution

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

### Line Voltage

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

## Radio

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

## UL Warning Statement

**IMPORTANT SAFETY INSTRUCTIONS** - When using your telephone equipment, basic safety precautions should always be followed to reduce the risk of fire, electric shock and injury to persons, including the following:

- Do not use this product near water (for example: near a bathtub, washbowl, kitchen sink or laundry tub, in a wet basement or near a swimming pool.)
- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
- Do not use the telephone to report a gas leak in the vicinity of the leak.
- Use only the power cord and batteries indicated in this manual. Do not dispose of batteries in a fire. They may explode. Check with local codes for possible special disposal instructions.
- **CAUTION:** To reduce the risk of fire, use only No. 26 AWG or larger (e.g., 24 AWG) UL Listed or CSA Certified Telecommunication Line Cord.
- **CAUTION:** To prevent an electric shock hazard, Do NOT connect telephone ports to public telephone system or equivalent.

## 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 <sup>6+</sup> )	(多溴联苯)	(多溴二苯乙醚)
含锡线材	x	o	o	o	o	o
连接器	x	o	o	o	o	o
变压器	x	o	o	o	o	o
陶瓷电容	x	o	o	o	o	o
高温锡材	x	o	o	o	o	o

o : 表示此附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。  
x : 表示此附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 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.

Some of the equipment provided by Alvarion and specified in this manual, is manufactured and warranted by third parties. All such equipment must be installed and handled in full compliance with the instructions provided by such manufacturers as attached to this manual or provided thereafter by Alvarion or

the manufacturers. Non-compliance with such instructions may result in serious damage and/or bodily harm and/or void the user's authority to operate the equipment and/or revoke the warranty provided by such manufacturer.

# About This Manual

This manual describes the BreezeMAX Si 4000 CPE and details how to install, operate and manage it.

This manual contains the following chapters and appendices:

- **Chapter 1 - [Product Description](#)** - Describes the BreezeMAX Si 4000 CPE unit and its functionality.
- **Chapter 2 - [CPE Installation](#)** - Describes how to install the BreezeMAX Si 4000 CPE and how to connect to subscriber's equipment.
- **Chapter 3 - [Commissioning](#)** - Describes how to initially configure the BreezeMAX Si 4000 CPE in order to test basic link operation.
- **Chapter 4 - [Configuring Setup Parameters](#)** - Describes how to configure general parameters of the BreezeMAX Si 4000 CPE.
- **Chapter 5 - [Configuring WiFi Parameters](#)** - Describes how to configure authentication, security and WiFi parameters.
- **Chapter 6 - [Configuring Local Address Parameters](#)** - Describes how to configure DHCP server and leasing parameters.
- **Chapter 7 - [Setting Advanced Parameters](#)** - Describes how to configure advanced parameters, such as: Authentication, security, Firewall, filters, and port forwarding/triggering parameters.
- **Chapter 8 - [Displaying Status Details](#)** - Describes how to view and understand the device status parameters.
- **Chapter 9 - [Configuring Telephony Parameters](#)** - Describes how to configure VoIP parameters
- **Chapter 10 - [Troubleshooting](#)** - Describes identifying and solving problems.
- **Glossary** - Terms used in this manual.

# Contents

About This Manual .....	xii
Contents .....	xiii
Chapter 1 - Product Description.....	1
<b>1.1 Introducing the BreezeMAX Si 4000 .....</b>	<b>3</b>
1.1.1 Product Features.....	5
<b>1.2 Safety Information .....</b>	<b>7</b>
<b>1.3 Specifications .....</b>	<b>8</b>
1.3.1 General .....	8
1.3.2 WiMAX Radio.....	8
1.3.3 WiFi Radio.....	10
1.3.4 VoIP Specifications .....	11
1.3.5 Configuration and Management.....	12
1.3.6 Mechanical .....	12
1.3.7 Electrical.....	13
1.3.8 Environmental .....	13
1.3.9 Standards Compliance.....	13
Chapter 2 - CPE Installation.....	15
<b>2.1 Installation Requirements .....</b>	<b>17</b>
2.1.1 Package Content.....	17
<b>2.2 Installation Procedure .....</b>	<b>18</b>
2.2.1 Guidelines for Positioning the Unit.....	18
2.2.2 Installing the Unit.....	18
<b>2.3 BreezeMAX Si 4000 Hardware Description .....</b>	<b>21</b>

2.3.1	Front Panel.....	21
2.3.2	Rear Panel .....	24
2.3.3	Reset Button .....	27
2.3.4	WiMAX Antennas .....	27
2.3.5	BreezeMAX Si 4000Cables.....	27
2.3.6	BreezeMAX Si 4000 Wi-Fi Option.....	28
<b>Chapter 3 - Commissioning .....</b>		<b>29</b>
<b>3.1</b>	<b>Introduction .....</b>	<b>31</b>
<b>3.2</b>	<b>Configuring the CPE Using the Web Management Interface .....</b>	<b>33</b>
3.2.1	Accessing the Web Management Interface .....	33
3.2.2	Applying Changes and Using Help .....	34
<b>3.3</b>	<b>Configuring the CPE Using the WiMAX Modem Application CD .....</b>	<b>36</b>
<b>3.4</b>	<b>Operation Verification .....</b>	<b>40</b>
<b>Chapter 4 - Configuring Setup Parameters.....</b>		<b>41</b>
<b>4.1</b>	<b>Introduction .....</b>	<b>43</b>
<b>4.2</b>	<b>Setting Basic Parameters .....</b>	<b>44</b>
<b>4.3</b>	<b>Setting Password .....</b>	<b>47</b>
<b>4.4</b>	<b>Setting Device Time Zone .....</b>	<b>48</b>
<b>4.5</b>	<b>Setting Device Name .....</b>	<b>50</b>
<b>4.6</b>	<b>Restore to Factory Default Configuration .....</b>	<b>51</b>
<b>Chapter 5 - Configuring WiFi Parameters .....</b>		<b>52</b>
<b>5.1</b>	<b>Introduction .....</b>	<b>54</b>
<b>5.2</b>	<b>WiFi Configuration .....</b>	<b>55</b>
5.2.1	Wireless Settings .....	55
5.2.2	Wireless Security .....	58
5.2.3	ACL (Access Control List) Settings .....	61

**Chapter 6 - Configuring Local Address Parameters ..... 62**

- 6.1 Introduction .....64**
- 6.2 DHCP Server .....65**
- 6.3 Lease Status .....66**
- 6.4 Lease Reservation .....67**

**Chapter 7 - Setting Advanced Parameters ..... 68**

- 7.1 Introduction .....70**
- 7.2 Authentication ... 71**
- 7.3 Security ... 73**
- 7.4 Firewall ....75**
- 7.5 MAC Filter .....78**
- 7.6 IP Filter .....79**
- 7.7 Port Forwarding/Trigger .....81**
  - 7.7.1 Port Forwarding.....81
  - 7.7.2 Port Trigger .....82
- 7.8 Dynamic DNS .....84**

**Chapter 8 - Displaying Status Details ..... 85**

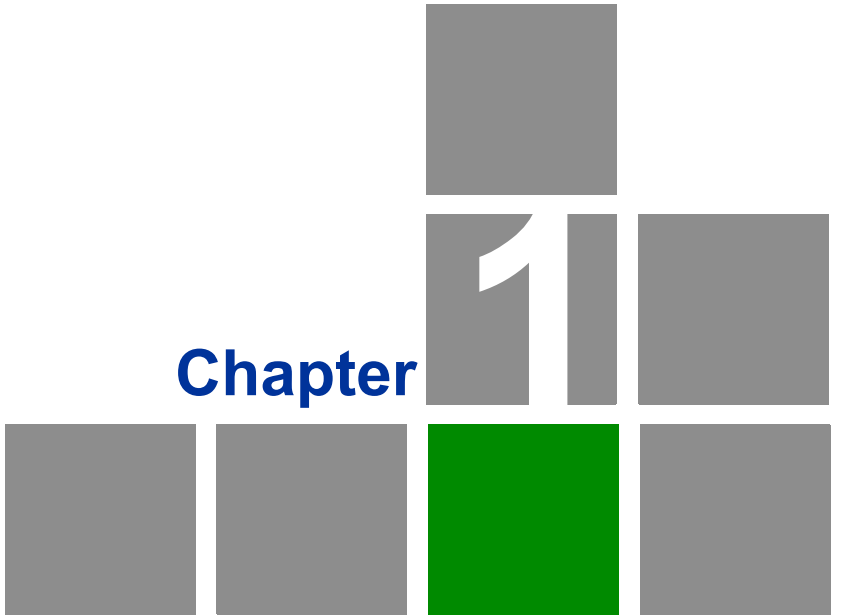
- 8.1 Introduction .....87**
- 8.2 Device Status .....88**
- 8.3 WiMAX Status .....90**
- 8.4 Software Status .....95**
- 8.5 Telephony Status .....96**
- 8.6 Certificate Status .....97**
- 8.7 About .....99**

**Chapter 9 - Configuring Telephony Parameters ..... 100**

- VoIP Parameters .....102**

Chapter 10 - Troubleshooting..... 105  
Glossary ..... 110





**Product Description**

## In This Chapter:

- “Introducing the BreezeMAX Si 4000” on page 3
- “Safety Information” on page 7
- “Specifications” on page 8

## 1.1 Introducing the BreezeMAX Si 4000

The BreezeMAX Si 4000 is a family of high capacity residential gateways and WiMAX Wireless Broadband Access subscriber stations, for a home or small office. The system provides network connections that are always on, supporting immediate access to the Internet and other IP services at high data rates. The unit provides a gateway function between a WiMAX service provider and a local Ethernet LAN. The device enables service providers to deliver last mile broadband wireless access as an alternative to wired DSL or cable modems.

The BreezeMAX Si 4000 solution enables the delivery of powerful wireless broadband services to the subscriber. The BreezeMAX Si 4000 is an out-of-the-box solution with immediate available local stock enabling virtually instant network expansion and simplified deployment. BreezeMAX Si 4000 provides a wireless solution for the subscriber to connect to the internet.

BreezeMAX Si 4000 enables service providers to wirelessly extend their services to customers in areas where the cost of cabling is prohibitive to deployment. Remote residential areas can now benefit from high-speed wireless Internet access, Web browsing and e-mail, and advanced applications such as multimedia services.

The BreezeMAX Si 4000 is a plug-and-play indoor unit (IDU) that is available in two WiMAX licensed frequency bands: 2.5 GHz and 3.5 GHz (See [“Product Features” on page 5](#)). The model you use depends on the frequency band of your service provider’s WiMAX service.

The BreezeMAX Si 4000 offers a user-friendly web-based management interface for the configuration of all the unit’s features. Any PC directly attached to the unit can access the management interface using a web browser, such as Internet Explorer (version 6.0 or above) or Firefox (version 1.5 or above).

Depending on models, the BreezeMAX Si 4000 includes one or two RJ-45 Ethernet switch ports 10/100 auto-sensing, auto-MDX for LAN connection and one or two RJ-11 Voice over IP (VoIP) phone ports. An 802.11b/g Wi-Fi module is included for providing a local WiFi access point service. The BreezeMAX Si 4000 unit also includes built-in WiMAX or two fold-out antennas for WiMAX communication.

The following table lists the available BreezeMAX Si 4000 models:

**Table 1-1: BreezeMAX Si 4000 Models**

Frequency Band	Model Number	Ports
<b>2.5 GHz</b>	4M-CPE4000-Si-1D-1V-2.5	<ul style="list-style-type: none"> <li>■ 1 data port (RJ-45)</li> <li>■ 1 VoIP phone port (RJ-11)</li> </ul>
	4M-CPE4000-Si-2D-2V-WiFi-2.5 (Premium model)	<ul style="list-style-type: none"> <li>■ 2 data port (RJ-45)</li> <li>■ 2 VoIP phone port (RJ-11)</li> <li>■ WiFi (802.11b/g)</li> </ul>
<b>3.3-3.6 GHz</b>	4M-CPE4000-Si-1D-1V-3.5	<ul style="list-style-type: none"> <li>■ 1 data port (RJ-45)</li> <li>■ 1 VoIP phone port (RJ-11)</li> </ul>
	4M-CPE4000-Si-1D-1V-WiFi-3.5	<ul style="list-style-type: none"> <li>■ 1 data port (RJ-45)</li> <li>■ 1 VoIP phone port (RJ-11)</li> <li>■ WiFi (802.11b/g)</li> </ul>

4M-CPE4000-Si-1D-1V-2.5

4M-CPE4000-Si-1D-1V-3.5

4M-CPE4000-Si-1D-1V-WiFi-3.5

The PREMIUM Model:

4M-CPE4000-Si-2D-2V-WiFi-2.5



**Figure 1-1: The BreezeMAX Si 4000 CPE**

## 1.1.1 Product Features

The BreezeMAX Si 4000 supports the following features:

- WiMAX 802.16-2005 Wave2 Standard Compliant Air Interface
- WiFi (for specific models)
- Dynamic Host Configuration Protocol (DHCP)
- Built-in web server for web-based configuration
- Dual image firmware crash protection
- Password protected access and configuration

- Auto-provisioning with remote firmware upgrade
- IEEE 802.3, IEEE 802.3u
- Gateway mode
- Bridge mode for Management and VoIP
- IP-CS Bridge mode
- ETH-CS Bridge mode
- Voice over IP
- VPN pass-through

## 1.2 Safety Information

### CAUTION



Failure to observe the following may result in personnel injury or device damage

- Avoid device exposure to high temperature or humidity. Always keep the device dry.
- Do not spill food or liquids on the device. Do not clean the device with wet cloth or with any liquids like water, harsh chemicals, cleaning solvents or strong detergents. Never operate the device in a wet environment. If the unit gets wet turn off the AC Power and contact Customer Support center.
- Do not push any objects into the openings of the device. Doing so may result in electric shock or fire by shorting out internal electronic circuit boards.
- Always use dry cloth to clean the device.
- Do not use or store the device in dusty or dirty environment.
- Do not attempt to open the enclosure. There are no user serviceable parts in the device. In case the device does not function properly please contact customer support center.
- Do not drop, knock or shake the device. Rough handling may break internal electronic boards.
- Do not use the device in areas where the local regulations prohibit its use.
- This device is a wireless RF device. RF Energy may affect operation of medical devices such as personal pace makers, patient monitoring systems etc. Do not use the devices in hospitals, health care centers, etc.
- Do not keep the device close to sensitive electronic equipment like TV, Radio, Microwave ovens, etc.
- Do not keep the device near strong magnetic field generators.

## 1.3 Specifications

### 1.3.1 General

**Table 1-2: General Specifications**

Feature	Description
Flash ROM	32MB
Ethernet LAN port	2.5 Ghz - One or two RJ-45 ports (depending on model) 3.5 Ghz - One RJ-45 port 10/100 auto-sensing, auto-MDX
Channel Step Size	In 250 kHz steps
POTS	One RJ-11
Power supply	Input: Universal range 100~240VAC Output: 12V/2A DC Frequency: 50Hz to 60Hz Current: 0.8A
WiFi SoC (3.5 GHz only)	RT2070 / 2.4GHz RF signal chip
VoiP Slic	Si3215
WiMAX SoC	BCS5200 and Dual Core 300MHz
RF IC	BCSR-200 / Dual Band 1T/2R RFIC
RAM	2.5 Ghz - 32MB 3.5 GHz - 64MB
Reset/Reboot button	Recessed switch, rear panel

### 1.3.2 WiMAX Radio

**Table 1-3: WiMAX Radio Specifications**

Item	Description
Radio Type	IEEE 802.16e 2005 WAVE 2
Frequency Band	<ul style="list-style-type: none"> <li>■ 2.5 GHz - 2485~2690 MHz</li> <li>■ 3.5 GHz - 3300~3600MHz</li> </ul>



**Table 1-3: WiMAX Radio Specifications**

Item	Description
<b>Antenna Type</b>	Two WiMAX antennas or high gain widebeam antenna, depending on model
<b>Channel Bandwidth</b>	2.5GHz - 5.00 and 10.00 MHz 3.5GHz - 5.00, 7.00, and 10.00 MHz
<b>Modulation Technique</b>	<ul style="list-style-type: none"> <li>■ Scalable OFDMA employing Time-Division Duplex (TDD) mechanism</li> <li>■ PRBS subcarrier randomization</li> <li>■ Contains pilot, preamble, and ranging modulation</li> </ul>
<b>FEC Coding Rates</b>	<ul style="list-style-type: none"> <li>■ Up Link and Down Link: QPSK, 16 QAM, 64 QAM</li> <li>■ QPSK and 16QAM - 1/2 and 3/4</li> <li>■ 64QAM - 1/2, 2/3, 3/4, 5/6</li> </ul>
<b>TPL (Transmit Power Level)</b>	27 dBm typical (maximum)
<b>Transmit Power Dynamic Range</b>	45 dB
<b>Channel Step Size</b>	In 250 kHz steps
<b>Synchronization</b>	Referenced to the WiMAX BTS Timing Module
<b>Frequency Accuracy</b>	MRCT Compliant
<b>Air Interface</b>	IEEE 802.16e Wireless MAN-OFDMA
<b>TDD Duty Cycle (Tx/Rx)</b>	Rx up to 75% , Tx up to 50%
<b>SISO or MIMO</b>	MIMO (1TX, 2RX)
<b>Regulatory Compliance</b>	FCC parts 15, 25, 27
<b>Frame Duration</b>	5 msec.
<b>RF Transmitter Specifications</b>	
<b>RF dynamic range</b>	45dB minimum
<b>Transmit Power Control Relative Accuracy</b>	mRCT compliant
<b>Transmit and Receive Switching Gap</b>	50 $\mu$ S
<b>RF Receiver Specifications</b>	
<b>Impedance</b>	50 ohms nominal
<b>Input return loss</b>	10dBi

**Table 1-3: WiMAX Radio Specifications**

Item	Description
<b>RX Sensitivity</b>	Typical 3dB better than mRCT in SISO mode, and 6 dB better in MRC or MIMO mode. -94.5 dBm maximum.
<b>Adjacent Channel Rejection</b>	4 dB min. Receive signal 64QAM-3/4, 3dB above sensitivity level.
<b>Non-Adjacent Channel Rejection</b>	23 dB min Receive signal 64QAM-3/4, 3dB above sensitivity level.
<b>Antenna Specifications</b>	
<b>Antenna Gain</b>	Typical 5dBi, Premium model: 7dBi
<b>Antenna Connectors</b>	None. Embedded IPEX

### 1.3.3 WiFi Radio



#### NOTE

This section only applies to the 4M-CPE4000-Si-2D-2V-WiFi-2.5 and 4M-CPE4000-Si-1D-1V-WiFi-3.5 models.

**Table 1-4: WiFi Radio Specifications**

Item	Description
<b>Radio Access Point modes</b>	IEEE 802.11b, IEEE 802.11g
<b>Frequency Range (center frequency)</b>	2412 MHz - 2484 MHz (channels 1- 14)
<b>Channel Bandwidth</b>	22 MHz
<b>Output Power@11g/54Mbps</b>	15±1 dBm
<b>Security</b>	802.1x, Shared Key, WPA, WPA2, WPA-WPA2-Mixed, WPA PSK, WPA2 PSK, WPA-WPA2-Mixed PSK
<b>Radio Technology</b>	Orthogonal Frequency Divisional Multiplexing (OFDM)

## 1.3.4 VoIP Specifications

**Table 1-5: VoIP Specifications**

Item	Description
<b>Voice Signalling Protocol</b>	<ul style="list-style-type: none"><li>■ SIP v2 (RFC 3261)</li><li>■ SDP (RFC2327)</li><li>■ RTP/RTCP (RFC 1889/RFC 1890)</li></ul>
<b>Voice Codecs</b>	<ul style="list-style-type: none"><li>■ g711 (a-law and u-law)</li><li>■ g729a/b</li><li>■ g723</li><li>■ ILBC</li></ul>
<b>Voice Quality</b>	<ul style="list-style-type: none"><li>■ VAD (Voice Activity Detection)</li><li>■ Echo cancellation (G.168)</li><li>■ Adaptive jitter buffer</li><li>■ DTMF tone detection and generation</li></ul>

**Table 1-5: VoIP Specifications**

Item	Description
<b>Call Features</b>	<ul style="list-style-type: none"> <li>■ Call ID</li> <li>■ Outgoing caller ID block</li> <li>■ Call transfer (blind/consultive)</li> <li>■ Call waiting/hold/retrieve</li> <li>■ Call waiting cancelation</li> <li>■ Anonymous incoming call blocking</li> <li>■ T.38 fax relay</li> <li>■ Dial plan</li> <li>■ Call forwarding: No Answer/Busy/All</li> <li>■ Do not disturb</li> <li>■ Redial/Redial on busy</li> <li>■ Automatic call return</li> <li>■ MWI and VMWI - message waiting indication</li> </ul>

### 1.3.5 Configuration and Management

**Table 1-6: Configuration and Management**

Item	Description
<b>Management options</b>	<ul style="list-style-type: none"> <li>■ Web-based (HTTP/HTTPS)</li> <li>■ TR-069</li> </ul>

### 1.3.6 Mechanical

**Table 1-7: Mechanical Specifications**

Item	Description
<b>Dimensions</b>	232(H)*142(W)*36(D) mm , Premium model: 253(H)*236(W)*165(D) mm
<b>Weight</b>	0.59 or 0.65 (depending on model) kg

**Table 1-7: Mechanical Specifications**

Item	Description
Mounting	Desktop

### 1.3.7 Electrical

**Table 1-8: Electrical Specifications**

Type	Details
AC Power Supply	Input: 100-240 VAC, 50-60 Hz, maximum current: 0.8A Output: 12 VDC, maximum current 2A

### 1.3.8 Environmental

**Table 1-9: Environmental Specifications**

Item	Details
Operating Temperature	0°C to 40°C
Storage Temperature	-20 to 55 °C
Humidity	Maximum 95%, non-condensing

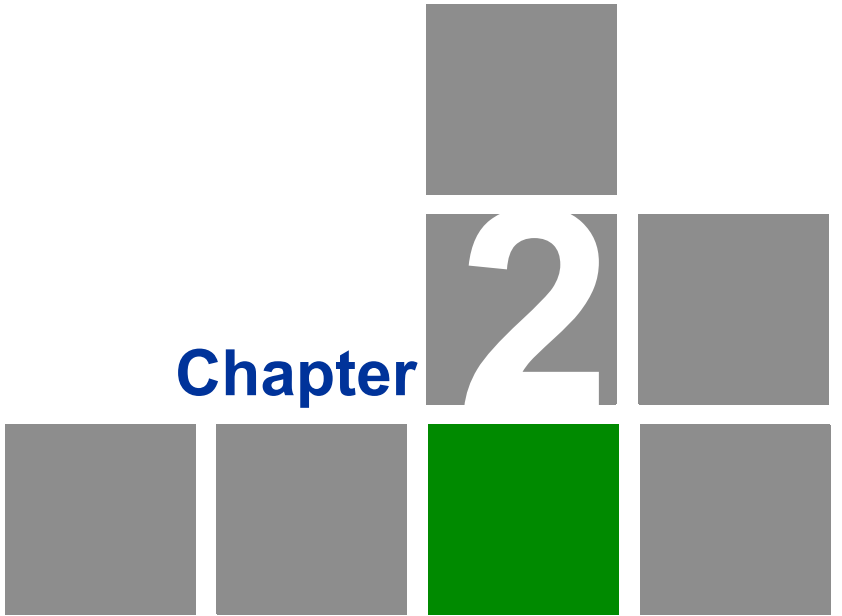
### 1.3.9 Standards Compliance

**Table 1-10: Standards Compliance**

Type	Standard
EMC	<ul style="list-style-type: none"> <li>■ FCC Part 15B</li> <li>■ ETSI EN 301 489</li> </ul>
Safety	<ul style="list-style-type: none"> <li>■ UL 60950-1</li> <li>■ IEC 60950-1</li> <li>■ EN 60950-1</li> </ul>
Radio	<ul style="list-style-type: none"> <li>■ ETSI EN 302 623</li> <li>■ ETSI EN 300 328</li> <li>■ FCC 04-135, Part 15, 25, 27</li> <li>■ EN 302 544</li> </ul>

**Table 1-10: Standards Compliance**

Type	Standard
<b>Standards</b>	<ul style="list-style-type: none"><li data-bbox="528 376 874 405">■ IEEE 802.16e-2005 WAVE 2</li><li data-bbox="528 443 1070 472">■ IEEE 802.3-2005 10BASE-T and 100BASE-TX</li><li data-bbox="528 510 703 539">■ IEEE 802.3u</li><li data-bbox="528 577 852 607">■ IEEE 802.11b and 802.11g</li></ul>



**Chapter**

**2**

**CPE Installation**

## In This Chapter:

- [“Installation Requirements” on page 17](#)
- [“Installation Procedure” on page 18](#)
- [“BreezeMAX Si 4000 Hardware Description” on page 21](#)



## 2.1 Installation Requirements

This section describes how to install and connect the BreezeMAX Si 4000.

### 2.1.1 Package Content

The BreezeMAX Si 4000 package includes the following components:

- BreezeMAX Si 4000 unit
- RJ-45 Category 5 network cable (1.5m)
- AC power adapter
- Quick Installation Guide

## 2.2 Installation Procedure



### CAUTION

The BreezeMAX Si 4000 is an indoor unit and must not be installed outdoors.

Before installing the BreezeMAX Si 4000, verify that you have all the items listed in the package checklist above. If any of the items are missing or damaged, contact your local WiMAX provider.

### 2.2.1 Guidelines for Positioning the Unit

The BreezeMAX Si 4000 can be installed indoors on any horizontal surface, such as a desktop or shelf. Be sure to select a suitable location for the device. Consider these points:

- Select a cool, dry place. To improve overall performance, choose an upper floor location near a window or outside wall.
- Leave adequate space (approximately 2"/5 cm) on all sides for proper air flow.
- Locate the unit near an AC power outlet that provides 100V to 240V.
- Avoid metal objects such as furniture, file cabinets or metal film anti-glare windows within 5 feet/1.5m of the modem.
- Position the unit at least 5 feet/1.5m away from any wireless device, such as WiFi enabled laptop or computer, WiFi router, wireless mouse or keyboard, or any cordless phone equipment. Other wireless devices may also cause interference, such as baby monitors, security systems, Bluetooth devices, etc.


### 2.2.2 Installing the Unit

The BreezeMAX Si 4000 is a plug-and-play device, so once it has been connected to your PC and powered up, it is fully operable.

- 1 Place the unit on a flat horizontal surface indoors. For the standing device, use the rotating base to stabilize the device. For the Premium unit, open up both antennas to upright position.
- 2 Connect the power cable to the power jack located on the rear panel of the unit. Connect the other end of the power cord to the AC outlet. The unit will take 1-2 minutes to boot up and find a nearby base station signal.

**CAUTION**

To avoid damage to the product, use ONLY the power adapter supplied with the unit.

- 3 Observe the Indicator LEDs. When you power on the BreezeMAX Si 4000, verify that the Power LED turns on and that the other LED indicators start functioning as described in [Table 2-1](#), [Table 2-2](#), and [Table 2-3](#).
- 4 Do one or both of the following:
  - » Connect your PC - Connect a Category 5 or better Ethernet cable to the BreezeMAX Si 4000's LAN port and the other end to the network port of your PC. Alternatively, you can connect the LAN port to an Ethernet switch or other devices. Make sure the length of each cable does not exceed 100 meters (328 ft).
  - » Connect your PC using WiFi(if available) - Click the WiFi icon  (lower right corner of PC); Click Find WLAN. Click the name of WiFi network and click Connect.

If your PC is powered on, the RJ-45 LAN port LEDs on the BreezeMAX Si 4000 turn on to indicate valid Ethernet links.

- 5 Align the unit or the fold-out antennas so that you receive the strongest signal by monitoring the WiMAX LEDs on the front panel of the unit.

Functioning as a gateway, the unit routes traffic between a WiMAX service provider's base station and the PCs or notebooks in the local network.

**NOTE**

If the BreezeMAX Si 4000 displays a weak WiMAX receive signal, try moving it to another location, or position it differently.

- 6 Connect a standard (analog) telephone set to the BreezeMAX Si 4000's VoIP port using standard telephone cable with RJ-11 plugs.

The BreezeMAX Si 4000 enables VoIP calls to be made through the unit using a standard (analog) telephone set connected to a VoIP port. Standard Session Initiation Protocol (SIP) technology is used to make VoIP calls. You must access the web interface and configure settings for your SIP service provider before you can make VoIP calls. The VoIP service may be configured remotely or locally by web.

- 7 If your unit is supplied with a CDROM, insert it to the CDROM drive, run the *CPEAutoConfigTool.exe* program and follow the procedure described in [“Configuring the CPE Using the WiMAX Modem Application CD” on page 36.](#)
- 8 Use your PC’s web browser to access the unit’s management interface and make any configuration changes. For more information, see [“Commissioning” on page 29.](#)

## 2.3 BreezeMAX Si 4000 Hardware Description

### 2.3.1 Front Panel

The front side of the BreezeMAX Si 4000 provides an array of system status indicators that simplifies installation and WiMAX network troubleshooting. The figure below shows the BreezeMAX Si 4000's LED locations. The LEDs functionality is described in [Table 2-1](#), [Table 2-2](#) and [Table 2-3](#).

Optimize the performance by placing the BreezeMAX Si 4000 where the greatest number of WiMAX signal strength lights are on. Try positioning the unit in different places to maximize signal strength.

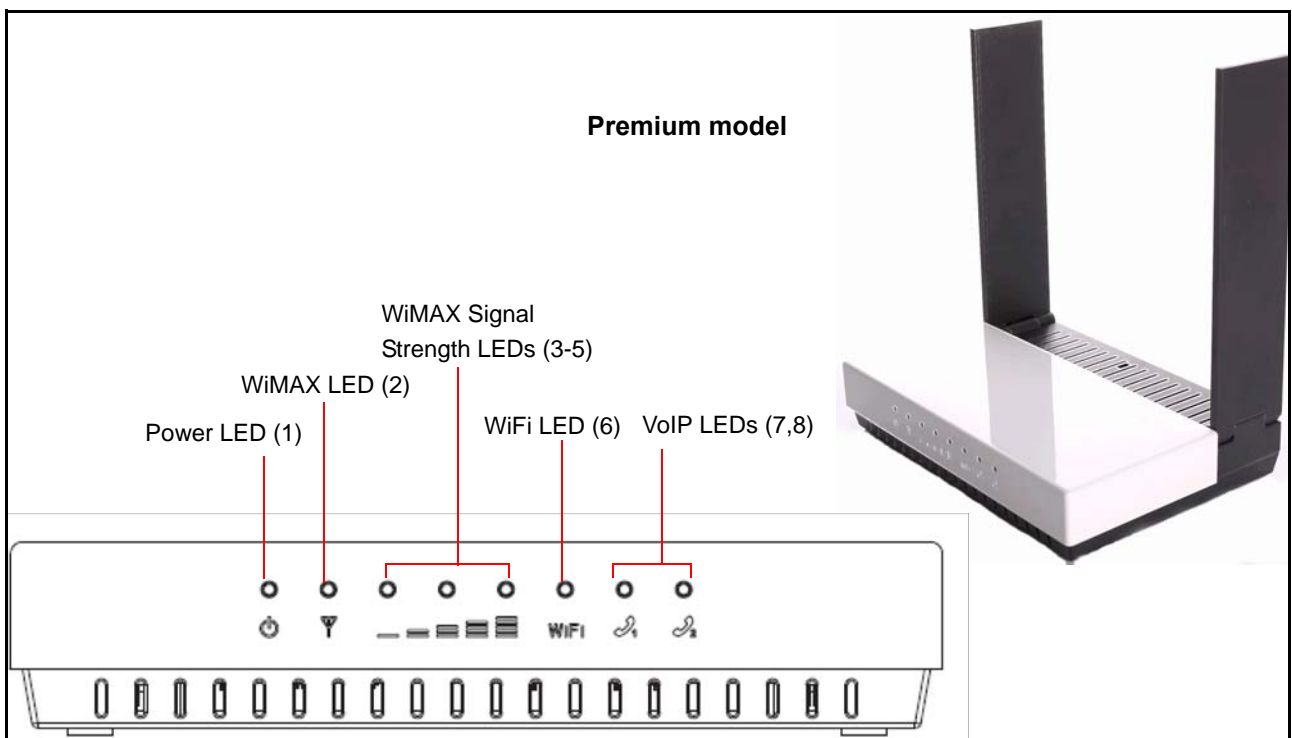
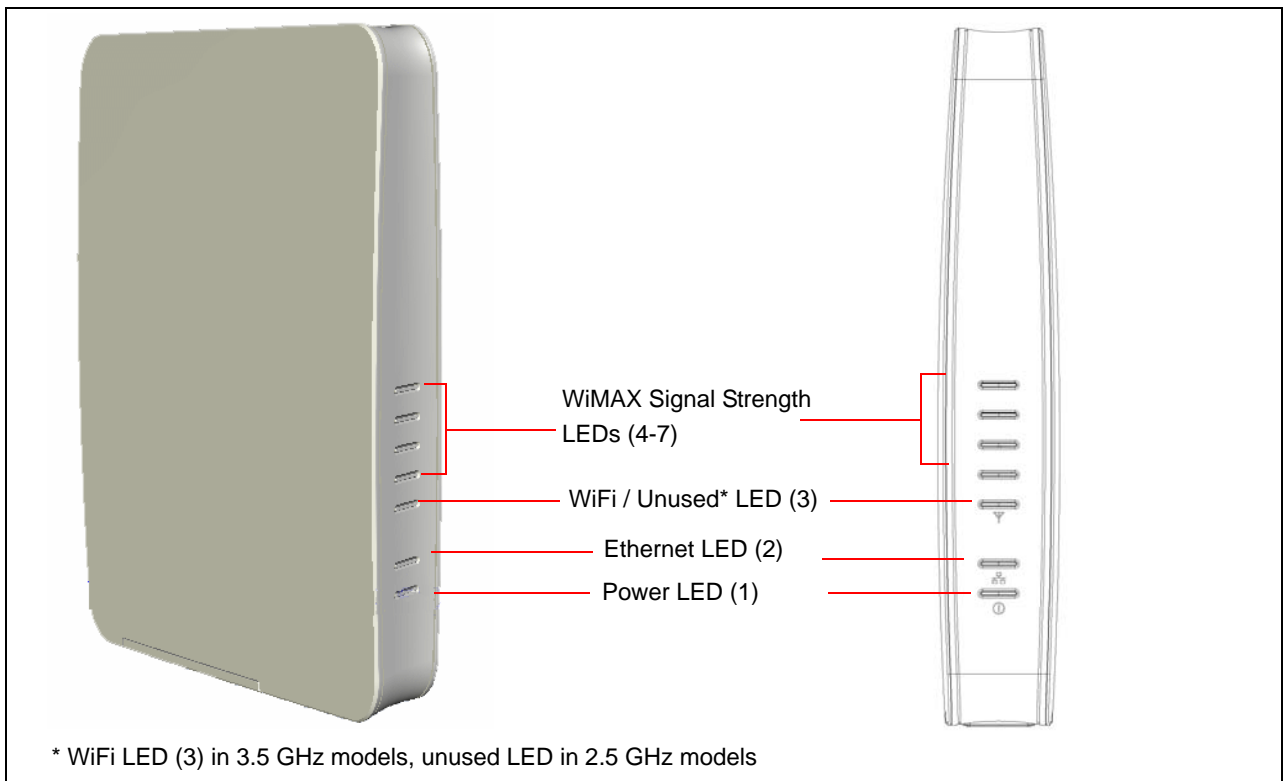


Figure 2-1: BreezeMAX Si 4000 and BreezeMAX Si 4000 Premium Front Panel

**Table 2-1: LEDs Status Indications - 2.5 GHz Models**

LED	Color	Status	Description
Power (1)	Blue	Off	Power off
		On	Power on
Ethernet (2)	Green	Off	LAN device is disconnected
		On	LAN device is connected
		Blinking	Data packet transmission
Unused LED (3)	Green	N/A	N/A
WiMAX Link Status (4)	Green	On	CPE is connected to a base station
		Off	CPE is not connected to a base station
WiMAX Link Status (5)	Green	On	The greater the number of WiMAX link status lights are on, the better the performance.
WiMAX Link Status (6)	Green	On	
WiMAX Link Status (7)	Green	On	

**Table 2-2: LEDs Status Indications - 3.5 GHz Units**

LED	Color	Status	Description
Power (1)	Blue	Off	Power off
		On	Power on
Ethernet (2)	Green	Off	LAN device is disconnected
		On	LAN device is connected
		Blinking	Data packet transmission
Wi-Fi (3)	Green	Off	Wi-Fi disabled
		On	Wi-Fi enabled
WiMAX Link Status (4)	Green	On	CPE is connected to a base station
		Off	CPE is not connected to a base station
WiMAX Link Status (5)	Green	On	The greater the number of WiMAX link status lights are on, the better the performance.
WiMAX Link Status (6)		On	
WiMAX Link Status (7)		On	

**Table 2-3: BreezeMAX Si Premium Model LEDs Status Indications**

LED	Color	Status	Description
Power (1)	Blue	Off	AC input not active or power failure
		On	Power on
		Blinking	<ul style="list-style-type: none"> <li>■ The modem is booting (blinking ~25 seconds).</li> <li>■ The modem is not functional or is being remotely managed (e.g., software is being upgraded, or application is loaded)</li> <li>■ Stops blinking when scanning begins. Radio is operational.</li> </ul>
WiMAX (2)	Blue	Off	The modem is not connected to base station
		On	The modem is connected to base station
LED 3 - WiMAX Signal	Blue	On	The greater the number of WiMAX signal strength lights are on, the better the performance.
LED 4 - WiMAX Signal	Blue	On	
LED 5 - WiMAX Signal	Blue	On	
Wi-Fi (6)	Blue	On	Wi-Fi enabled
		Off	Wi-Fi disabled
VoIP (7,8)	Blue	Off	<ul style="list-style-type: none"> <li>■ VoIP (voice) is not configured</li> <li>■ The modem is not connected to the network</li> <li>■ SIP registration time expired</li> <li>■ SIP registration in process</li> </ul>
		On	VoIP (voice) is configured and available after successful registration to the SIP server
		Blinking	Voicemail waiting

### 2.3.2 Rear Panel

The BreezeMAX Si 4000 includes one LAN port for 10/100 Mbps Ethernet connection, one RJ-11 Voice over IP (VoIP) phone port, and an AC power jack.

The BreezeMAX Si 4000 Premium model includes two LAN ports for 10/100 Mbps Ethernet connection, two RJ-11 Voice over IP (VoIP) phone ports, and an AC power jack.

The following table summarizes the BreezeMAX Si 4000 rear panel elements:



**Table 2-4: BreezeMAX Si 4000 Connectors**

Item	Connector	Description
Ethernet network port	10BASE-T/100BASE-TX RJ-45 port	Connects directly to the PC can also be connected to an Ethernet switch or hub to support more users and provide a data link to the local network.
VoIP port	RJ-11 telephone ports	Connects directly to a standard (analog) telephone set to allow a regular telephone to be used for making VoIP calls over the Internet.
Power adapter	Power socket	Connection to 100-240 VAC at 50-60 Hz

The following figures show the rear of BreezeMAX Si 4000 and the location of the ports.

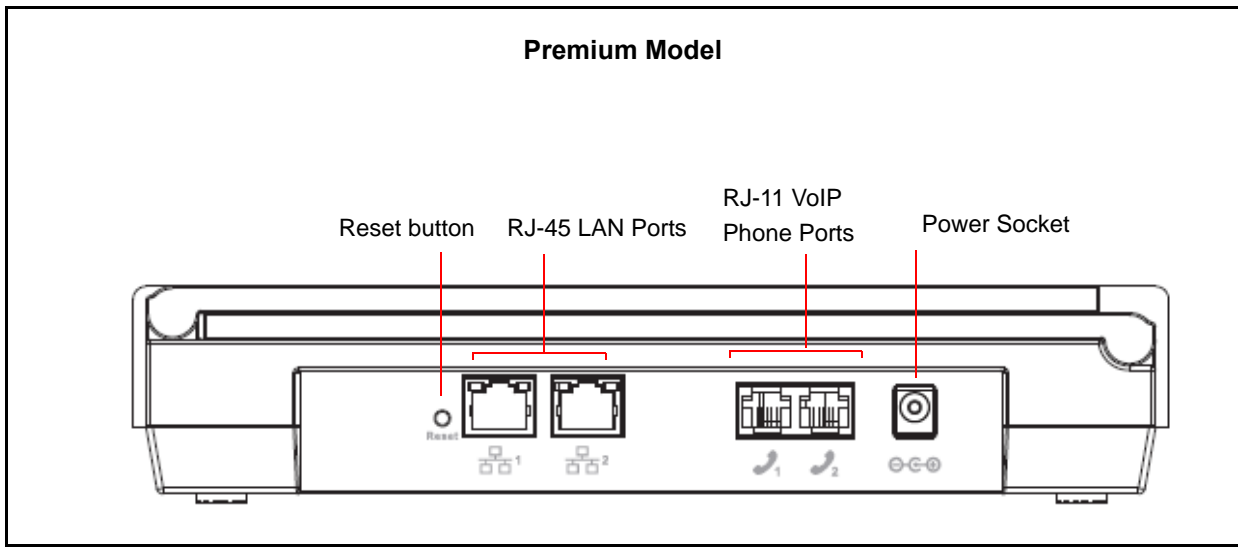
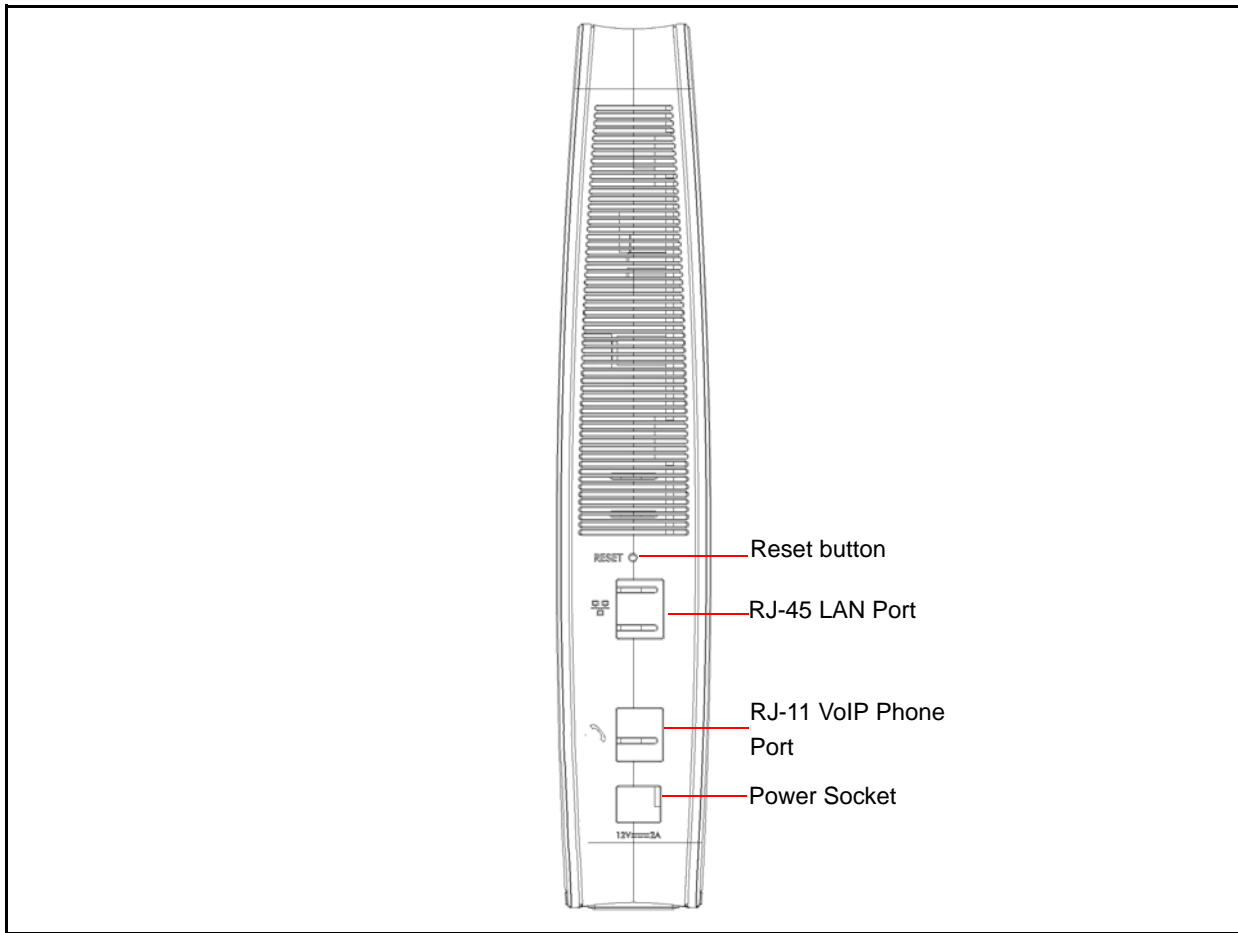


Figure 2-2: BreezeMAX Si 4000 and BreezeMAX Si 4000 Premium Rear Panel

### 2.3.3 Reset Button

The recessed button is used to reset the BreezeMAX Si 4000 or to restore the unit to factory default configuration.

- Do not perform reset to factory default unless specifically instructed by customer support.
- To perform a hardware reset, press the button for approximately 1 second.
- To restore the device to the factory default settings, press and hold the button for 5 seconds or more; any configuration changes you made are removed and the factory default configuration is restored to the unit.
- Some user-configured parameters will be lost and must be reconfigured.

### 2.3.4 WiMAX Antennas

Two WiMAX antennas are included with the BreezeMAX Si 4000 for WiMAX communications. The BreezeMAX Si 4000 antennas are embedded in the unit. In the Premium model, the antennas are external and fold out.

### 2.3.5 BreezeMAX Si 4000 Cables



#### NOTE

The length of the Ethernet cable connecting the BreezeMAX Si 4000 to the data equipment, must not exceed 100 meters.

Use only Category 5E Ethernet cables from either Alvarion or any of the approved manufacturers, listed in [Table 2-5](#). Consult with Alvarion's specialists on the suitability of other cables.

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

Manufacturer	Part Number
Superior Cables Ltd. <a href="http://www.superior-cables.com">www.superior-cables.com</a>	612098
HES Cabling Systems <a href="http://www.hescs.com">www.hescs.com</a>	H5E-00481


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

Manufacturer	Part Number
Teldor <a href="http://www.teldor.com">www.teldor.com</a>	8393204101
Southbay Holdings Limited 11th Fl., 15, Lane 347, Jong Jeng Rd. Shin Juang City, Taipei County Taiwan, R.O.C. Attn: Eva Lin Tel. 886-2-2832 3339 Fax. 886-2-2206 0081 E-mail: <a href="mailto:eva@south-bay.com.tw">eva@south-bay.com.tw</a>	TSM2404A0D
GU-Tech., LLC . - A Member of OVIS Group Tel/Fax : 732 918 8221 Mobile: 718 909 4093 <a href="http://www.OVIS.COM.TW">www.OVIS.COM.TW</a> <a href="http://www.GU-TECH.COM">www.GU-TECH.COM</a>	

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.

### 2.3.6 BreezeMAX Si 4000 Wi-Fi Option

The BreezeMAX Si 4000 3.5 GHz model includes the 802.11b/g Wi-Fi option. This unit includes internal antennas for local wireless connections to PCs.

To connect your PC using WiFi, click the WiFi icon  (lower right corner of PC); Click **Find WLAN** and select the name of WiFi network Click **Connect**.



## In This Chapter:

- [“Introduction” on page 31](#)
- [“Configuring the CPE Using the Web Management Interface” on page 33](#)
- [“Configuring the CPE Using the WiMAX Modem Application CD” on page 36](#)
- [“Operation Verification” on page 40](#)

## 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 BreezeMAX Si 4000:

- The web-based management interface - accessed using a PC/Notebook with a web browser (see [“Configuring the CPE Using the Web Management Interface” on page 33](#)).
- An automatic configuration tool provided on a CDROM for the subscribers (see [“Configuring the CPE Using the WiMAX Modem Application CD” on page 36](#)).
- Upgrading the CPE using an auto-configuration file, or IPKG (in \*.ipk format) (see [“Operation Verification” on page 40](#)).

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 (also Eng > WiMAX Config > Realm)	
Frequency	Full Scan	Should be supplied by system administrator.

**Table 3-1: Basic Parameters**

<b>Item</b>	<b>Default Value</b>	<b>Comment</b>
Telephony - SIP Server, phone number, authentication, enable the phone	Disabled	Optional VoIP is disabled by default and should be enabled by the operator
WiFi	Enabled	Enabled by default



## 3.2 Configuring the CPE Using the Web Management Interface

### 3.2.1 Accessing the Web Management Interface

By default, the BreezeMAX Si 4000 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 parameters:

IP address: 192.168.254.x ( $1 \leq x \leq 253$ , excluding 251)

Netmask: 255.255.255.0

Gateway: 192.168.254.251



#### To log in:

- 1 Open a web browser and enter the default IP address: <http://192.168.254.251>. The web browser displays the login page.

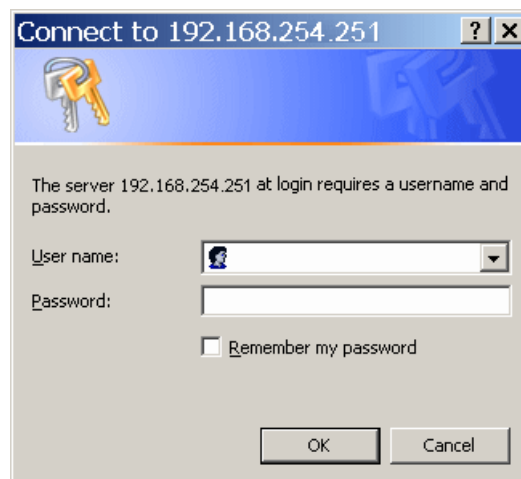
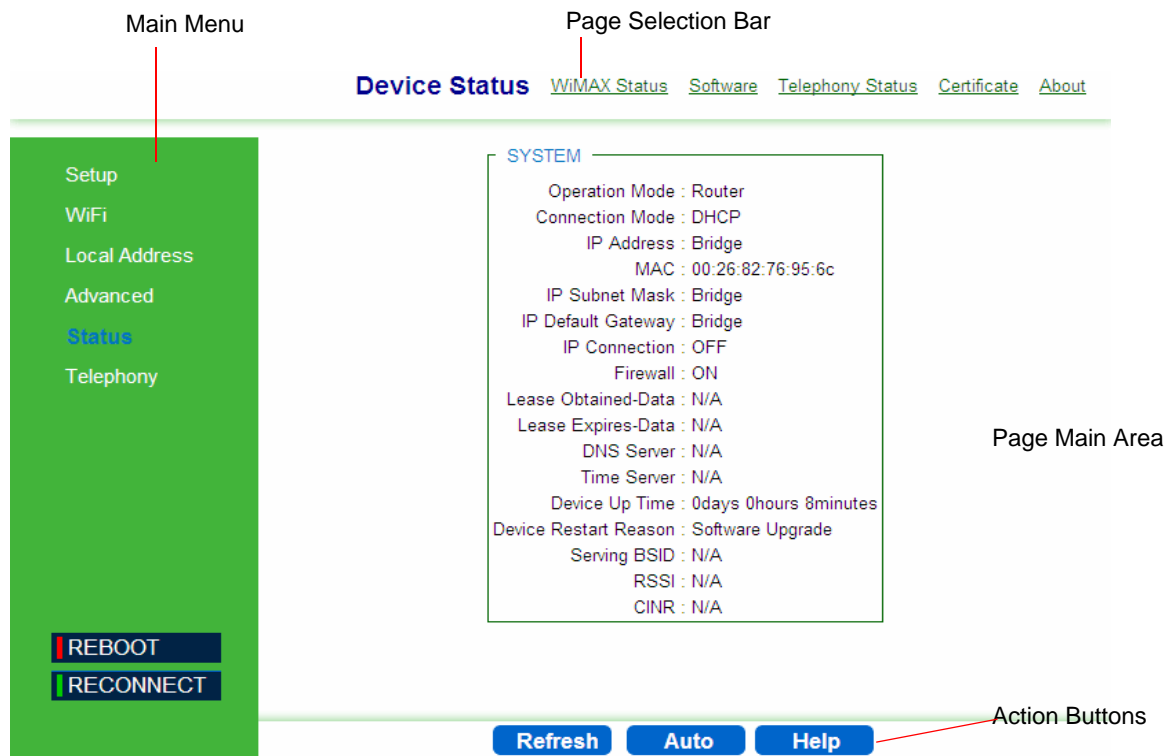


Figure 3-1: Login Window

- 2 Enter the user name and password, and click **Login**. The default credentials are:
  - » Username: admin
  - » Password: admin

The Status - Device Status page is displayed.



**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.

### 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.

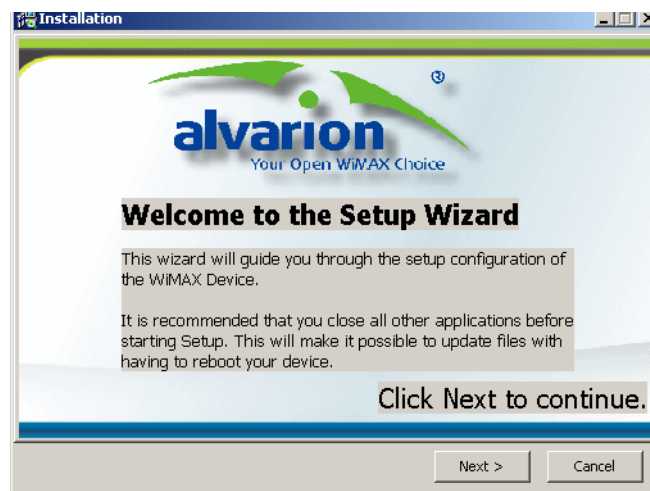
## 3.3 Configuring the CPE Using the WiMAX Modem Application CD

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.



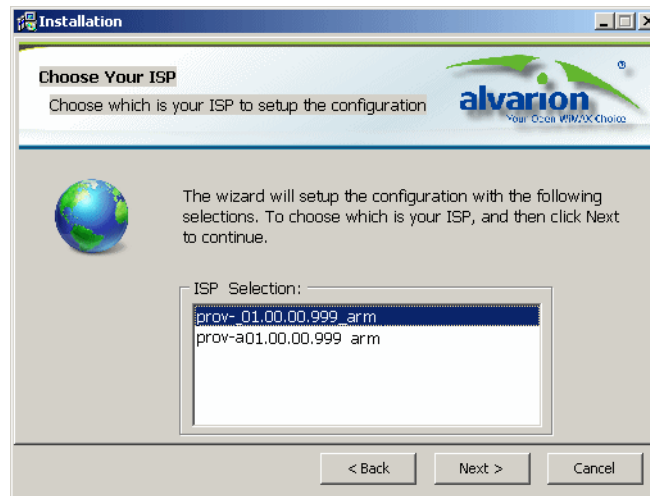
**To configure the unit using the Auto-Configuration tool:**

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



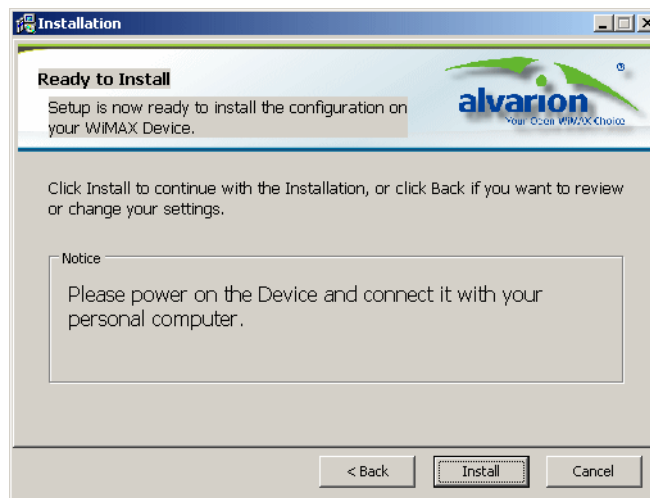
**Figure 3-3: Installation Setup Wizard Window**

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



**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.



**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.

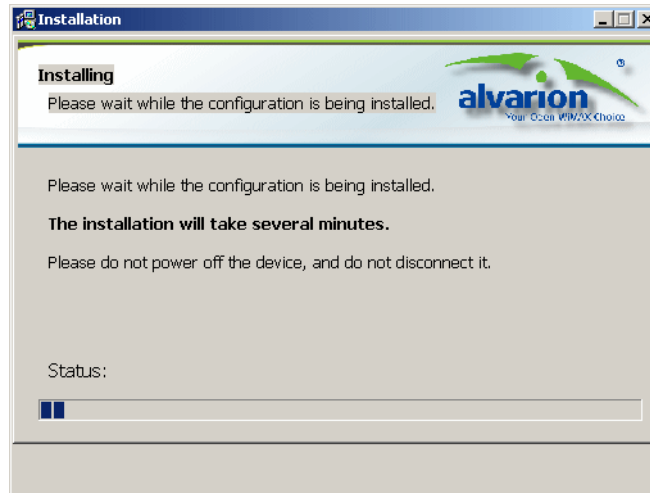


Figure 3-6: Installing Window

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

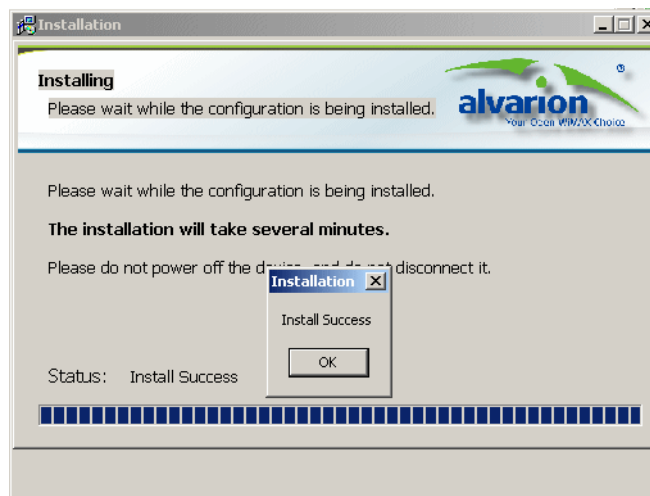


Figure 3-7: Installation Succeeded

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

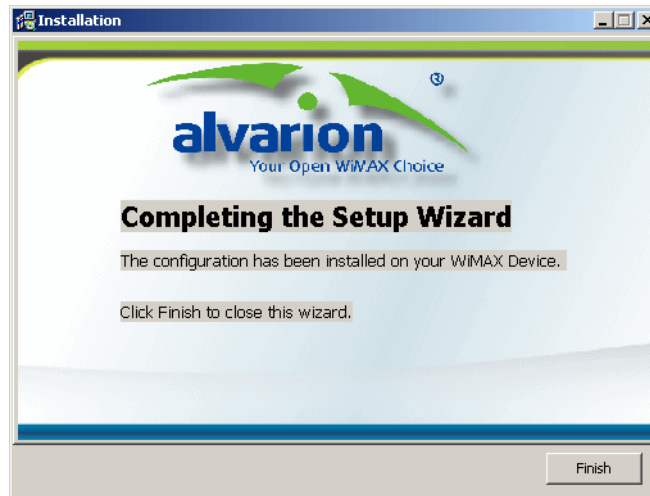


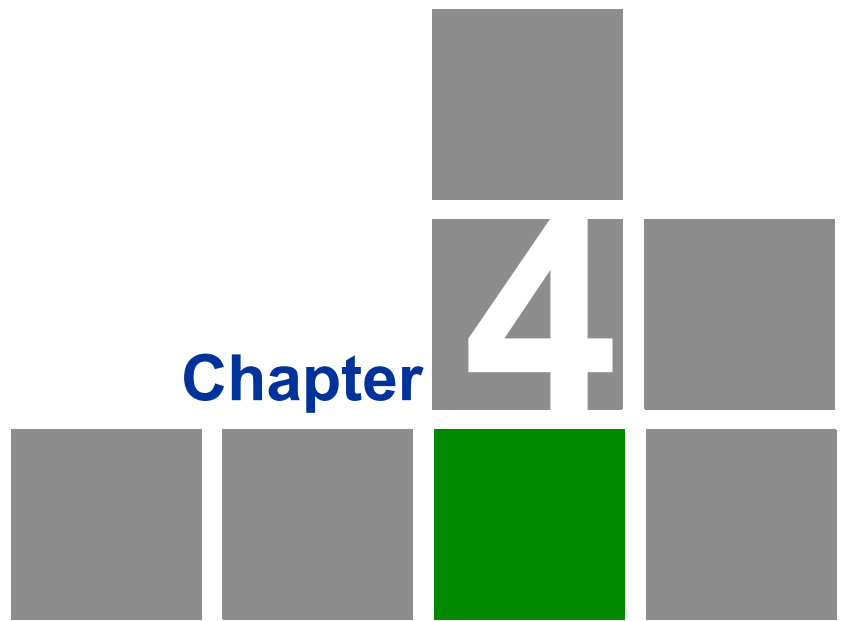
Figure 3-8: Installation Complete

## 3.4 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 [www.Alvarion.com](http://www.Alvarion.com). This site can be reached by clicking the Alvarion logo on any page in the GUI.





# Configuring Setup Parameters

## In This Chapter:

- [“Introduction” on page 43](#)
- [“Setting Basic Parameters” on page 44](#)
- [“Setting Password” on page 47](#)
- [“Setting Device Time Zone” on page 48](#)
- [“Setting Device Name” on page 50](#)
- [“Restore to Factory Default Configuration” on page 51](#)

## 4.1 Introduction

The BreezeMAX Si 4000'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.



### NOTE

You can use the web browser interface to access the WAN IP address only if the BreezeMAX Si 4000 already has an IP address that is reachable through your network.

The default IP address of the BreezeMAX Si 4000 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 Rebooting message and the 60 seconds countdown are displayed.

## 4.2 Setting Basic Parameters

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

### IMPORTANT



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.

**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			

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

Parameter	Description	Default	Possible Values
Operation Mode	Specifies the mode for forwarding data packets from the service provider's WiMAX network to the local network.	Router	<ul style="list-style-type: none"> <li>■ Router (the only option, unless differently configured by Alvarion)</li> <li>■ Bridge IPCS</li> <li>■ Bridge ETHCS</li> </ul>
<b>Internal Management/VoIP Connection Mode</b>			
Management Connection Mode	<p>Sets the forwarding mode for sending management packets to the WiMAX network:</p> <ul style="list-style-type: none"> <li>■ 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.</li> <li>■ Router mode - forwards packets based on Layer 3 IP addresses.</li> </ul>	Router	<ul style="list-style-type: none"> <li>■ Bridge</li> <li>■ Router</li> </ul>
VoIP Connection Mode	<p>Sets the forwarding mode for sending VoIP packets to the WiMAX network:</p> <ul style="list-style-type: none"> <li>■ 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.</li> <li>■ Router mode forwards packets based on Layer 3 IP addresses.</li> <li>■ None - No forwarding</li> </ul>	Router	<ul style="list-style-type: none"> <li>■ Bridge</li> <li>■ Router</li> <li>■ None</li> </ul>

Table 4-1: Basic Parameters (Continued)

Parameter	Description	Default	Possible Values
<b>Connection Mode</b>			
Connection Mode	<p>Sets the connection type for the unit:</p> <ul style="list-style-type: none"> <li>■ DHCP - The system will assign IP addresses to the unit on the local area network.</li> <li>■ Static - The IP address is predefined and fixed. When you select this option, new menu items are displayed for configuration: <ul style="list-style-type: none"> <li>» WAN IP Address</li> <li>» WAN Subnet Mask</li> <li>» WAN Gateway Address</li> <li>» DNS1- Domain Name System</li> <li>» DNS2</li> </ul> </li> </ul>	DHCP	<ul style="list-style-type: none"> <li>■ DHCP</li> <li>■ Static</li> </ul>
<b>WAN MTU</b>			
WAN MTU	<p>Sets the WAN maximum transmission unit (MTU) size in bytes</p> <ul style="list-style-type: none"> <li>■ Auto (1400) - transmission unit size is 1400 bytes</li> <li>■ Manual - enter the value for transmission unit size (Range: 576-1500)</li> </ul>	Auto (1400)	<ul style="list-style-type: none"> <li>■ Auto (1400)</li> <li>■ Manual</li> </ul>

**NOTE**

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).



### NOTE

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.

Basic **Password** Device Time Device Name Restore To Factory

Setup  
WiFi  
Local Address  
Advanced  
Status  
Telephony

REBOOT  
RECONNECT

New Login Password

Confirm New Login Password

Undo Apply Help

Figure 4-2: Setup - Password

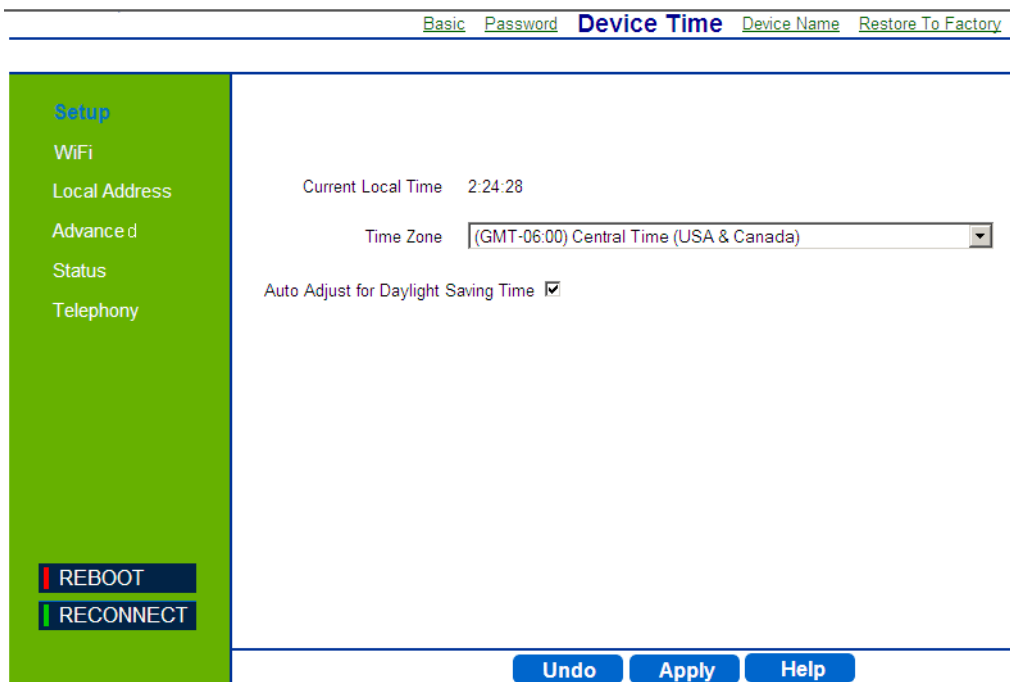


To change the login password:

- 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 Si 4000 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.



**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-06.00, 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.*).

The screenshot shows the 'Device Name' configuration page. At the top, there are navigation tabs: 'Basic', 'Password', 'Device Time', 'Device Name' (which is highlighted), and 'Restore To Factory'. On the left side, there is a green sidebar menu with the following items: 'Setup' (highlighted), 'WiFi', 'Local Address', 'Advanced', 'Status', and 'Telephony'. At the bottom of the sidebar are two buttons: 'REBOOT' and 'RECONNECT'. The main content area displays 'Current Device Name' as 'WiMaxCPE' and 'New Device Name' with an empty text input field. At the bottom of the main area, there are three buttons: 'Undo', 'Apply', and 'Help'.

**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: WiMAXCPE)
- **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 and WiFi settings. 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. However, you will not be able to make and receive calls until the voice line LED is lit on the front panel. You will need to manually restore any parameter changes, such as WiFi SSID and security settings, and voice settings that you made, since these settings will not exist after the unit reboots following the default restoration.

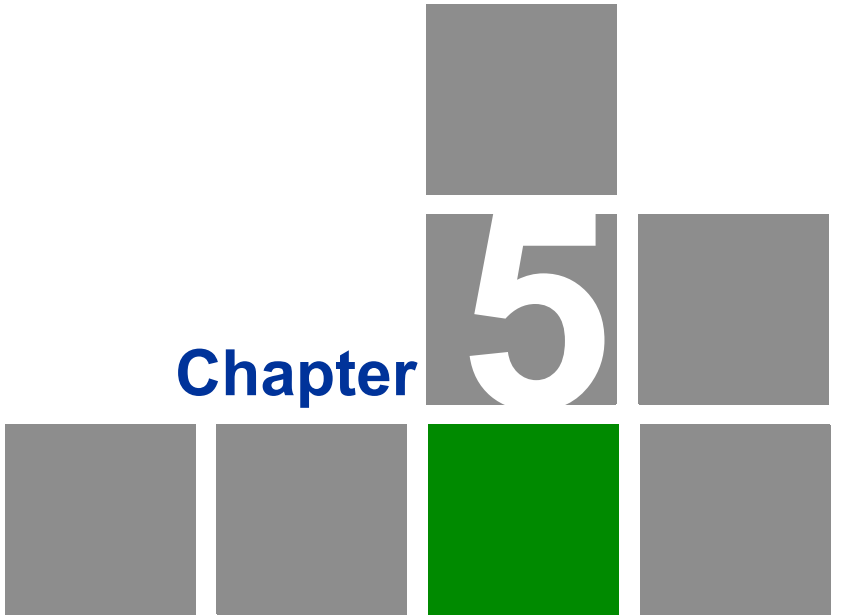
### IMPORTANT

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.



# Configuring WiFi Parameters

## In this chapter:

- [“Introduction” on page 54](#)
- [“WiFi Configuration” on page 55](#)

## 5.1 Introduction

The BreezeMAX Si 4000 model for 3.5 GHz WiMAX band and the BreezeMAX Si 4000 premium model include an IEEE 802.11g and IEEE 802.11b radio interface for local Wi-Fi communications. The Wi-Fi setup pages include configuration options for the radio signal characteristics and Wi-Fi security.

## 5.2 WiFi Configuration

Some BreezeMAX Si 4000 models include IEEE 802.11b/g radio interfaces for local Wi-Fi communications. The Wi-Fi set up pages include configuration options for the radio signal characteristics and Wi-Fi security.

Figure 5-1: WiFi Configuration

### 5.2.1 Wireless Settings

The Wireless Settings page includes the following parameters:

- **Enable WiFi Interface** - Enables/disables the Wi-Fi radio
- **Country Code** -The parameter set (list of parameters per country regulations) by which various parameters are defined (Read-only). Default WiFi Country Code for EU P/N is ETSI.

- **Network Name (SSID)** – The Service Set ID (SSID) that identifies the Wi-Fi network. The SSID is case sensitive and can consist of up to 32 alphanumeric characters. (Default: WiMAXCPE)
- **Radio Channel** – The radio channel used by the unit and its clients to communicate with each other. This channel must be the same on the unit and all of its wireless clients. The available channel settings are limited by local regulations. (Default: 1; Range: 1-14, Auto; Default for EU P/N: Auto).

**NOTE**

If you experience poor performance, you may be encountering interference from another wireless device. Try changing the channel, as this may eliminate interference and increase performance. \_

- **Working mode** - The 802.1x authentication is an addition to the WLAN security methods. It provides a method to protect the network behind the access point from intruders as well as provide dynamic keys and strengthen WLAN encryption. (Range: 802.11b, 802.11g, 802.11b/g, Default:802.11b/g)
- **Transmit Power** – The power of the radio signals transmitted from the unit. The higher the transmission power, the farther the transmission range. Only Full power is available.
- **RTS Threshold** – Sets the packet size threshold at which a Request to Send (RTS) signal must be sent to a receiving station prior to sending the data frame. The unit sends RTS frames to a receiving station to negotiate the sending of a data frame. After receiving an RTS frame, the station sends a CTS (clear to send) frame to notify the unit that it can start sending data. If a packet size equals or exceeds the RTS threshold, the RTS/CTS (Request to Send/Clear to Send) mechanism will be enabled. Units contending for the medium may not be aware of each other, and the RTS/CTS mechanism can solve this “Hidden Node Problem.” (Range: 256-2432 bytes: Default: 2432 bytes).
- **CTS Protect Mode** – When 802.11g and 802.11b clients operate together in the same Wi-Fi network, there needs to be a mechanism that prevents 802.11b clients from interfering with 802.11g transmissions. This is achieved by sending 802.11b-compatible CTS (Clear to Send) or RTS/CTS (Request to Send / Clear to Send) frames before each transmission. This mechanism



decreases the performance of 802.11g clients, but ensures that 802.11b clients can communicate with the BreezeMAX Si 4000. (Default: Auto)

- » **Always off:** If there are no 802.11b clients in the network, the protection mode can be disabled.
  - » **Always on:** The transmitting client sends a CTS frame to prevent others from accessing the medium. This mechanism is effective for most networks with mixed 802.11g and 802.11b clients.
  - » **Auto:** Both RTS and CTS frames must be exchanged before a client can send data. There may be 802.11b clients in some networks that do not detect the CTS frames from other stations. The full RTS/CTS exchange should solve most connection problems, but it also has the greatest impact on network performance.
- **Preamble Length** – All IEEE 802.11 frames begin with an alternating pattern of 1s and 0s called the preamble, which tells receiving stations that a frame is arriving. This provides time for the receiving station to synchronize to the incoming data stream. This parameter sets the length of the signal preamble that is used at the start of a data transmission. Using a short preamble instead of a long preamble can increase data throughput on the unit, but requires that all clients can support a short preamble. (Default: Short Preamble)
- » **Short:** Sets the preamble to short (96 microseconds) for increased throughput.
  - » **Long:** Sets the preamble to long (192 microseconds). Using a long preamble ensures the unit can support all 802.11b and 802.11g clients.
- **SSID Suppress** – The unit is configured by default as an “open system”, which broadcasts a beacon signal including the configured SSID. Wireless clients with a configured SSID of “ANY” can read the SSID from the beacon, and automatically set their SSID for immediate connection to the BreezeMAX Si 4000. When enabled, the unit does not include its SSID in beacon messages. This provides a basic level of security, since wireless clients must be configured with the SSID to connect to the BreezeMAX Si 4000. (Default: Disable)

## 5.2.2 Wireless Security

The BreezeMAX Si 4000 Wi-Fi interface is configured by default as an “open system”, which broadcasts a beacon signal including the configured SSID (Service Set ID). Wireless clients with a configured SSID of “ANY” can read the SSID from the beacon, and automatically set their SSID to allow immediate connection to the wireless network.

To implement wireless network security, you have to employ two main functions:

- **Authentication** – It must be verified that clients attempting to connect to the network are authorized users. Refer to the next sections for details on various authentication options (Default mode is Open System).
- **Encryption** – Data passing between the unit and clients must be protected from interception and eavesdropping. You can select one of the following, depending on your Authentication method:
  - » WEP (see [“Wired Equivalent Privacy \(WEP\)” on page 59](#))
  - » TKIP (see [“Temporal Key Integrity Protocol \(TKIP\)” on page 60](#))
  - » None (Default)

For a more secure network, the BreezeMAX Si 4000 can implement one of several security mechanisms. The security mechanism employed depends on the level of security required, the network and management resources available, and the software support provided on wireless clients.

The following security options are available. These options are described in the next sections:

- 802.1x
- WEP
  - » Open System
  - » Shared Key
- WPA
  - » WPA

- » WPA2
- » WPA-WPA2-Mixed
- » WPA PSK
- » WPA2 PSK
- » WPA-WPA2-Mixed PSK

When you select the security type from the list, the required settings are displayed. The option “Open System” together with encryption disabled is equivalent to no security, all clients will be able to immediately connect to the Wi-Fi network.

### 5.2.2.1 802.1x Authentication

The 802.1x authentication is an addition to the WLAN security methods. It provides a method to protect the network behind the access point from intruders as well as provide for dynamic keys and strengthen WLAN encryption.

You can set the following:

- Rekey Interval - Time (in seconds) between renewals of authentication key (Default: 3600)
- RADIUS Server -Remote Authentication Dial-in User Service (RADIUS) authentication server
- RADIUS Port (Default: 1812)
- RADIUS Key (Default: radius\_key)

### 5.2.2.2 Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy (WEP) provides a basic level of security, preventing unauthorized access to the network and encrypting data transmitted between wireless clients and the BreezeMAX Si 4000.

Two methods of authentication can be used with WEP: Open System authentication and Shared Key authentication.

#### 5.2.2.2.1 Open System Authentication

Open System Authentication (OSA) is a process by which a computer can gain access to a wireless network that uses the Wired Equivalent Privacy (WEP) protocol. With OSA, a computer equipped with a wireless modem can access any

WEP network and receive files that are not encrypted. In Open System authentication, the WLAN client need not provide its credentials to the Access Point during authentication. Thus, any client, regardless of its WEP keys, can authenticate itself with the Access Point and then attempt to associate. In effect, no authentication (in the true sense of the term) occurs.

#### 5.2.2.2.2 Shared Key

WEP uses static shared keys (fixed-length hexadecimal or alphanumeric strings) that are manually distributed to all clients that want to use the network.

When enabled, you must configure at least one WEP key for the Wi-Fi interface and all its clients:

Default Key (1 ~ 4) – Sets WEP key values for authentication and encryption. The user must first choose between ASCII or Hexadecimal keys. At least one key must be specified. Each WEP key has an index number. The selected key is used for authentication and encryption on the Wi-Fi interface. Enter key values that match the key type and length settings. (Default: Hex, 128 bits, no preset value)

- » Key Type - Specifies keys as either ASCII or Hexadecimal values.
- » Key Length - WEP keys can be set as 64 or 128 bits in length.
- » Key - Depending on the selected key length, specify keys as either:
  - ◇ 5 or 13 alphanumeric characters, or
  - ◇ 10 or 26 hexadecimal digits

#### 5.2.2.3 Temporal Key Integrity Protocol (TKIP)

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

#### 5.2.2.4 WPA/WPA2 Security

WPA is a more powerful security technology for Wi-Fi networks than WEP. It provides strong data protection by using encryption as well as strong access controls and user authentication. WPA utilizes 128-bit encryption keys and dynamic session keys to ensure your 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 - WiFi Protected Access, Pre-Shared Key)

The *WPA* and *WPA2* modes use IEEE 802.1X as their basic framework for user authentication and dynamic key management. IEEE 802.1X access security uses Extensible Authentication Protocol (EAP) and requires a configured Remote Authentication Dial-in User Service (RADIUS) authentication server to be accessible in the enterprise network. If you select WPA or WPA2 mode, be sure to configure the RADIUS settings displayed on the page.

The *WPA-WPA2-Mixed* mode is a transitional mode of operation for networks moving from WPA security to WPA2. WPA-WPA2-Mixed mode allows both WPA and WPA2 clients to associate to a common Wi-Fi interface.

*WPA-PSK* is an authentication mechanism in which users provide credentials to verify that they should be allowed access to a network. This requires a single password entered into each WLAN node.

Encryption mechanisms used for WPA and WPA-PSK are the same, with one difference: in WPA-PSK, authentication is reduced to a simple common password, instead of user-specific credentials.

You can set the following for each mode:

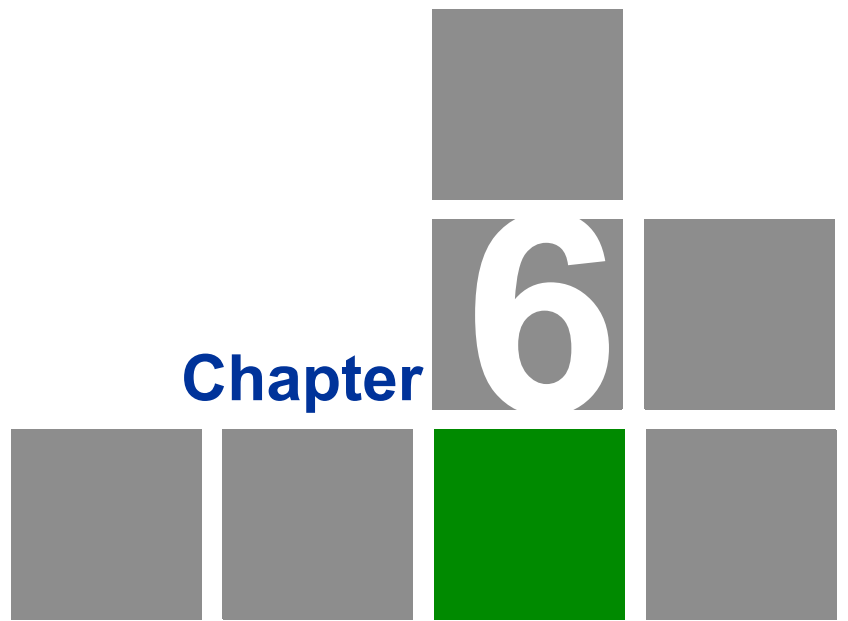
- Rekey Interval - Time (in seconds) between renewals of authentication key (Default: 3600)
- WPAPSK Type - ASCII (default) or HEX
- WPAPSK - Enter your security key

### 5.2.3 ACL (Access Control List) Settings

In this section you can add MAC addresses of clients which are allowed to access the system, or denied from accessing. The following are examples of a MAC address template that can be used:

- 00:11:22:33:44:55
- 001122334455

- 1 Select either **Disable**, **Allow** or **Deny**.
- 2 For the Allow and Deny lists, click **Insert** to add a MAC address to the list.



# Configuring Local Address Parameters

## In this chapter:

- [“Introduction” on page 64](#)
- [“DHCP Server” on page 65](#)
- [“Lease Status” on page 66](#)
- [“Lease Reservation” on page 67](#)

## 6.1 Introduction

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

### NOTE



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



## 6.2 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 and WiFi access point. In the DHCP Server page you set DHCP parameters for dynamic IP assignment.

The screenshot shows the DHCP Server configuration interface. On the left is a green sidebar with a menu: Setup, WiFi, Local Address (selected), Advanced, Status, and Telephony. Below the menu are REBOOT and RECONNECT buttons. The main area is titled 'DHCP Server' and has links for Lease Status and Lease Reservation. The configuration fields are: 'Enable DHCP Server' (checked), 'DHCP Server IP Address' (192.168.254.251), 'DHCP Starting IP Address' (192.168.254.1), 'DHCP Ending IP Address' (192.168.254.10), and 'DHCP Lease Time' (1 hour, 0 minutes, 0 seconds). At the bottom are Undo, Apply, and Help buttons.

Figure 6-1: 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: 1 hour.

## 6.3 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)

The screenshot shows the 'Lease Status' page in a web interface. The page has a navigation menu on the left with options: Setup, WiFi, Local Address, Advanced, Status, and Telephony. Below the menu are buttons for REBOOT and RECONNECT. The main content area displays a table with the following data:

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

At the bottom of the page, there are buttons for Refresh, Auto, and Help.

**Figure 6-2: Lease Status**

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

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

## 6.4 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 and WiFi access point. You can also add, delete, or modify the reservation settings.

Select	Host Name	MAC Address	IP Address	Enabled
<input type="checkbox"/>	<input type="text"/>	<input type="text" value="xx:xx:xx:xx:xx:xx"/>	<input type="text" value="x.x.x.x"/>	<input checked="" type="checkbox"/>

REBOOT  
RECONNECT

Add Del Undo Apply Help

Figure 6-3: 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.



# Setting Advanced Parameters

## In this chapter:

- [“Introduction” on page 70](#)
- [“Authentication” on page 71](#)
- [“Security” on page 73](#)
- [“Firewall” on page 75](#)
- [“MAC Filter” on page 78](#)
- [“IP Filter” on page 79](#)
- [“Port Forwarding/Trigger” on page 81](#)
- [“Dynamic DNS” on page 84](#)

## 7.1 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.

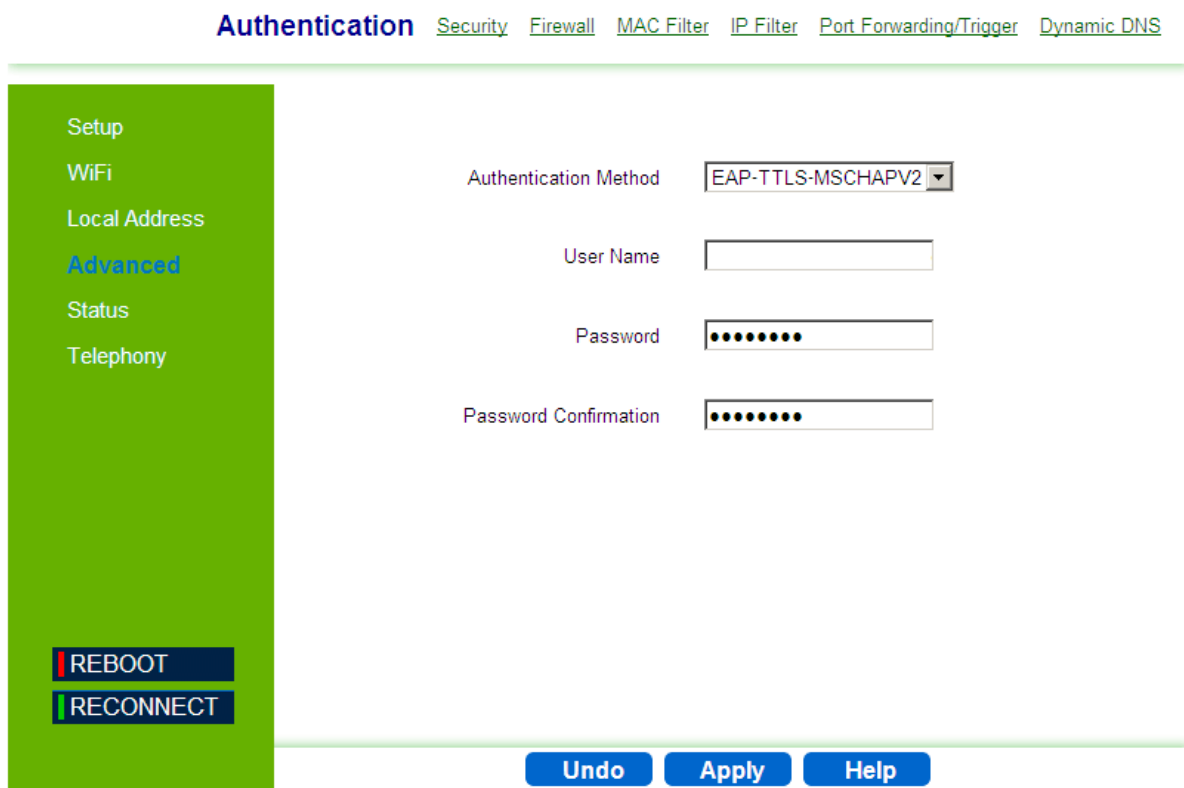
## 7.2 Authentication

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

**IMPORTANT**



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



**Figure 7-1: 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: wan mac address@WiMax.com, e.g. 0026824EE12C@WiMax.com).
- **Password** - Enter the user password supplied by the service provider). Default: quickynikyoky
- **Password Confirmation** - Re-enter the user password to confirm it.



## 7.3 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.

### IMPORTANT



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

**Figure 7-2: 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: Disabled)
- **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).

**NOTE**

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 net 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 from WAN, use [https://CPE\\_WAN\\_IP\\_Address:8080](https://CPE_WAN_IP_Address:8080).

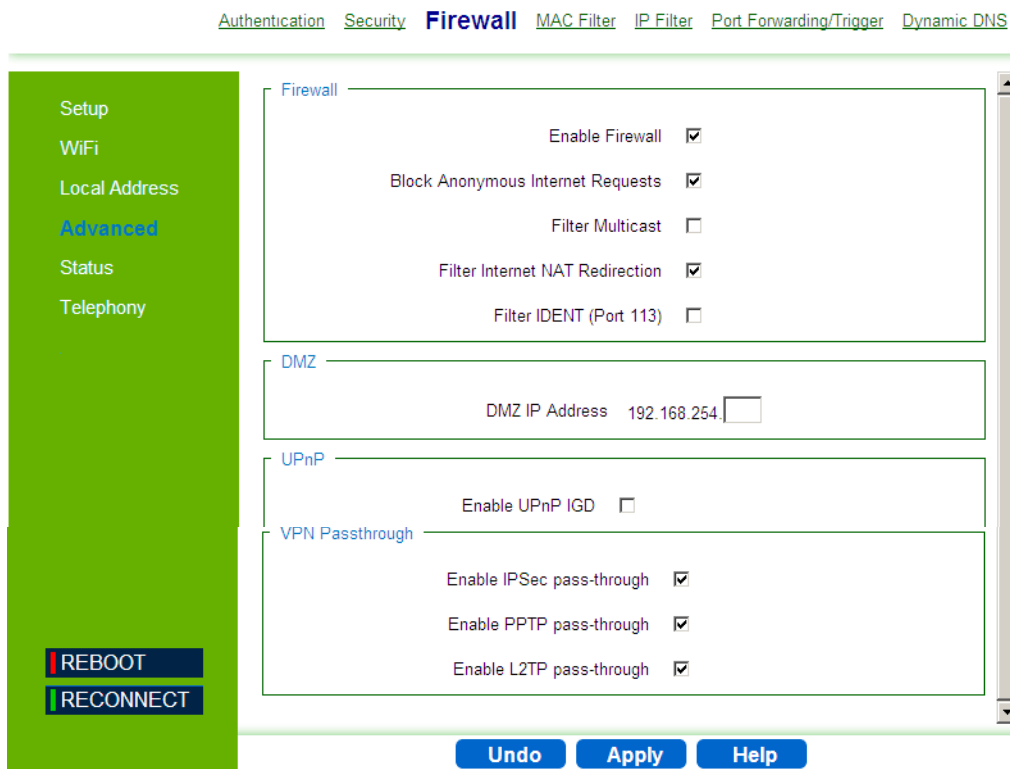
## 7.4 Firewall

The BreezeMAX Si 4000 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).

### IMPORTANT



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.



**Figure 7-3: 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 multicast 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** - DMZ IP Address. Set a server that acts as a "neutral zone" (DMZ stands for "Demilitarized 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.

■ **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.

**IMPORTANT**

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

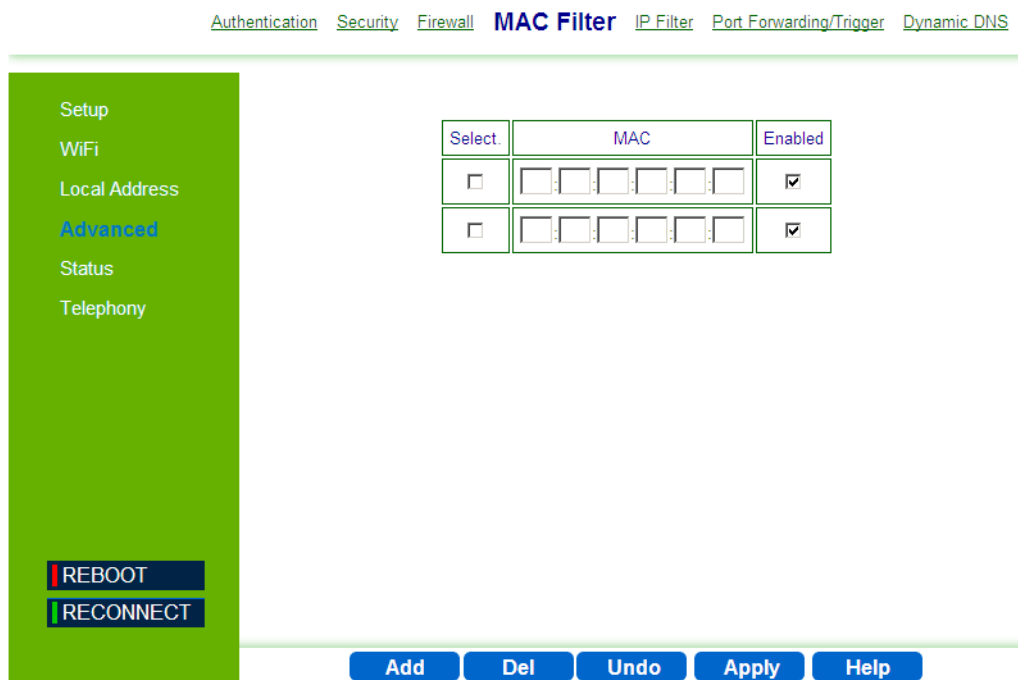
- » **Enable IPSec pass-through** - Internet Protocol Security. IPSec provides encrypted security services at the IP layer, and enables to use encrypted tunnels /traffic between two hosts.
- » **Enable PPTP pass-through** - Point to Point Tunneling Protocol. This protocol enables the transfer of data 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 multivendor interoperability and acceptance.

## 7.5 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.



**Figure 7-4: Advance - MAC Filter**

The following configuration parameters are available:

- **Select** - Select this check-box to add this row to delete the 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.

## 7.6 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.

[Authentication](#)
[Security](#)
[Firewall](#)
[MAC Filter](#)
[IP Filter](#)
[Port Forwarding/Trigger](#)
[Dynamic DNS](#)

Setup

WiFi

Local Address

Advanced

Status

Telephony

REBOOT

RECONNECT

Select	IP Range	Port Range	Protocol	Enabled
<input type="checkbox"/>	192.168.254. <input type="text"/> ~ <input type="text"/>	<input type="text"/> ~ <input type="text"/>	TCP	<input checked="" type="checkbox"/>
<input type="checkbox"/>	192.168.254. <input type="text"/> ~ <input type="text"/>	<input type="text"/> ~ <input type="text"/>	TCP	<input checked="" type="checkbox"/>

Add
Del
Undo
Apply
Help

**Figure 7-5: 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.

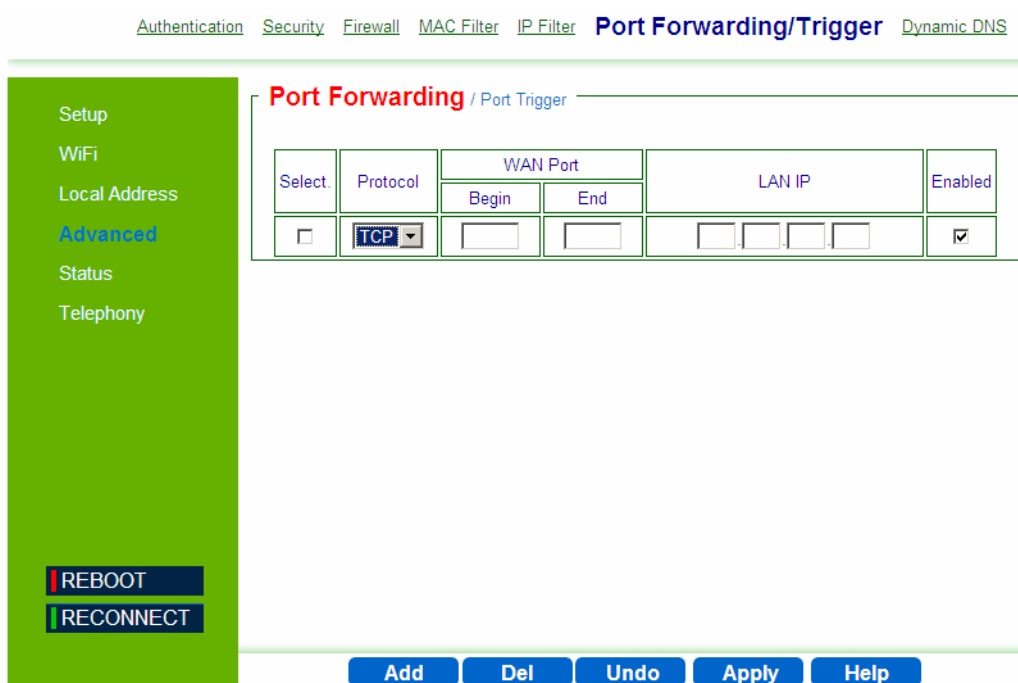


## 7.7 Port Forwarding/Trigger

### 7.7.1 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.



**Figure 7-6: 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.

## 7.7.2 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.

Authentication Security Firewall MAC Filter IP Filter **Port Forwarding/Trigger** Dynamic DNS

Port Forwarding / **Port Trigger**

Select	No.	Application Name	Triggered Range	Forwarded Range	Enabled
<input type="checkbox"/>	1	<input type="text"/>	<input type="text"/> ~ <input type="text"/>	<input type="text"/> ~ <input type="text"/>	<input checked="" type="checkbox"/>

REBOOT  
RECONNECT

Add Del Undo Apply Help

**Figure 7-7: 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.

## 7.8 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.

The screenshot shows a web interface for configuring Dynamic DNS. At the top, there are navigation links: Authentication, Security, Firewall, MAC Filter, IP Filter, Port Forwarding/Trigger, and Dynamic DNS (which is highlighted). On the left, a green sidebar contains a menu with items: Setup, WiFi, Local Address, Advanced (highlighted), Status, and Telephony. At the bottom of the sidebar are two buttons: REBOOT and RECONNECT. The main content area has a header with the same navigation links. Below the header, there is a form with two fields: 'Enable DDNS' with an unchecked checkbox, and 'DDNS Service Provider' with a dropdown menu showing 'www.dyndns.org'. At the bottom of the form are three buttons: Undo, Apply, and Help.

**Figure 7-8: Advanced - Dynamic DNS**

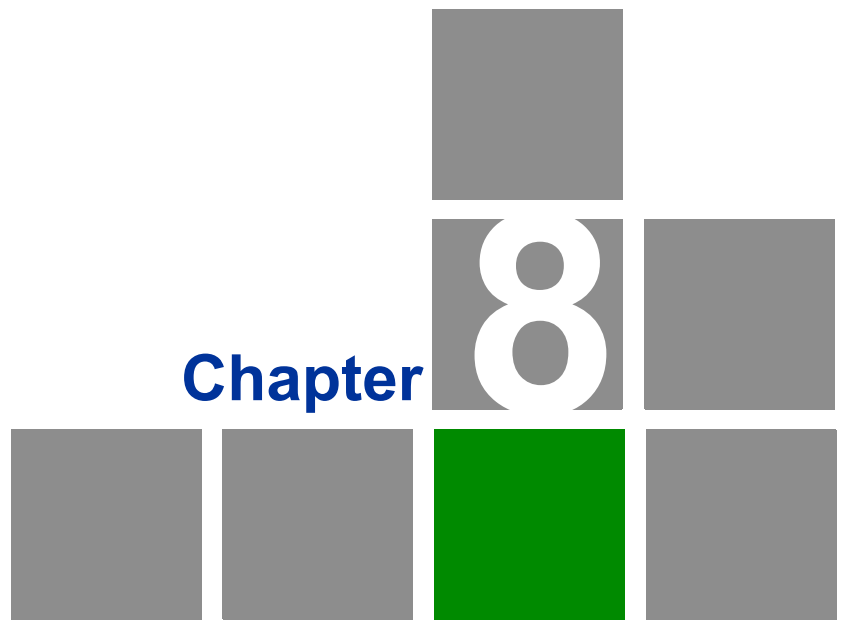
The Dynamic DNS page includes the following parameters:

- **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).



## Displaying Status Details

## In this chapter

- [“Introduction” on page 87](#)
- [“Device Status” on page 88](#)
- [“WiMAX Status” on page 90](#)
- [“Software Status” on page 95](#)
- [“Telephony Status” on page 96](#)
- [“Certificate Status” on page 97](#)
- [“About” on page 99](#)

## 8.1 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.

## 8.2 Device Status

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

The screenshot shows the 'Device Status' page with a navigation menu on the left and a central display area. The navigation menu includes: Setup, WiFi, Local Address, Advanced, Status (highlighted), and Telephony. At the bottom of the menu are 'REBOOT' and 'RECONNECT' buttons. The central display area shows the following system parameters:

```

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
  
```

At the bottom of the page are three buttons: 'Refresh', 'Auto', and 'Help'.

**Figure 8-1: 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 8-1: 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 <a href="#">“Setting Basic Parameters” on page 44</a> . Available option: Router.
Connection Mode	Connection type for the unit, as defined in <a href="#">“Setting Basic Parameters” on page 44</a> . Available options: DHCP, Static



**Table 8-1: Device Status Parameters (Continued)**

Item	Description
IP Address	WAN IP address, if the Static connection mode was selected, as defined in <a href="#">“Setting Basic Parameters” on page 44</a> . For DHCP mode - IP address acquired on the WAN interface is displayed. Otherwise it is 0.0.0.0
MAC	WAN MAC Address
IP Subnet Mask	The IP subnet mask, if the Static connection mode was selected, as defined in <a href="#">“Setting Basic Parameters” on page 44</a> , 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 <a href="#">“Setting Basic Parameters” on page 44</a> . 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 <a href="#">“Firewall” on page 75</a> .
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. 78 dBm)
CINR	Carrier to Interference-plus-Noise Ratio [in decibels (dB)] (e.g. 13 dB). This value should be maximized for best signal quality.

## 8.3 WiMAX Status

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

The screenshot displays the WiMAX Status interface with the following sections:

- Navigation:** Device Status, **WiMAX Status**, Software, Telephony Status, Certificate, About
- 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
- Buttons:** Refresh, Auto

Figure 8-2: 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 8-2: WiMAX System Parameters**

Parameter	Description	Possible values
<b>WiMAX System</b>		
State	The status of WiMAX connection.	<ul style="list-style-type: none"> <li>■ Network Entry - the unit has just been connected to the network</li> <li>■ Operational - the unit is functional</li> <li>■ Scan - the unit scans the network</li> <li>■ Idle - the unit is de-registered from the network, however will continue to scan the network and keep track of its location</li> </ul>
BSID	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	Network security technologies and protocols status	Authorized - has authentication settings Unauthorized - without authentication setting
Bandwidth		Depending on unit model: 5000, 7000, or 10000
Max Tx Power	Maximum uplink transmit power	
Max RSSI	Maximum received signal strength indication	-35 to -100 dBm
Max CINR	Maximum Carrier to Interference-plus-Noise Ratio	
Connection Time	Time (in seconds) during which the unit is connected to the BS	

**Table 8-2: WiMAX System Parameters (Continued)**

Parameter	Description	Possible values
Scan Type	The method by which the network is scanned	<ul style="list-style-type: none"> <li>■ Fullband - The system will try to scan the whole frequency band.</li> <li>■ CAPL - Channel Allocation Priority Level. The system allocates priority to channels for scanning order.</li> <li>■ 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.</li> <li>■ 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.</li> </ul>
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	Minimum received signal strength indication	
Min CINR	Minimum Carrier to Interference-plus-Noise Ratio	
Center Frequency	The middle frequency of the bandwidth of a channel. The unit is synchronised on this frequency.	
<b>WiMAX TX</b>		
Data Rate	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 connection	
UGS bytes	Total number of bytes sent on Unsolicited Grant Service connection	

Table 8-2: WiMAX System Parameters (Continued)

Parameter	Description	Possible values
ERTPS bytes	Total number of bytes sent on ERTPS - Extended Real-time Polling Service data packets.	
TX bytes	Total of uplink transmitted bytes	
<b>WiMAX RX</b>		
Data Rate	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	
<b>WiMAX PHY</b>		
DL Mode	Downlink connection mode	SISO, MIMO, MiMO A, MiMO B
DL max mcs	Maximum modulation reached	
DL min mcs	Minimum modulation reached	
DL mcs	Current modulation	
UL max mcs	Maximum modulation reached	
UL min mcs	Minimum modulation reached	
UL mcs	Current modulation	
List of various modulations: ■ QPSK DL/UL PDUs ■ 16QAM DL/UL PDUs ■ 64QAM DL/UL PDUs	Number of packets in this modulation	
<b>TX Service Flow / Rx Service Flow</b>		
Type	The service flow type	Best effort, ERT, NRT, UGS
SFID	Service flow ID	
CID	Connection ID	

**Table 8-2: WiMAX System Parameters (Continued)**

<b>Parameter</b>	<b>Description</b>	<b>Possible values</b>
DropPackets (Tx only)	Number of packets that were dropped	
DropBytes (Tx only)	Number of packets that were dropped	

## 8.4 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.

### NOTE



Use this page only upon instructions from Alvarion.

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

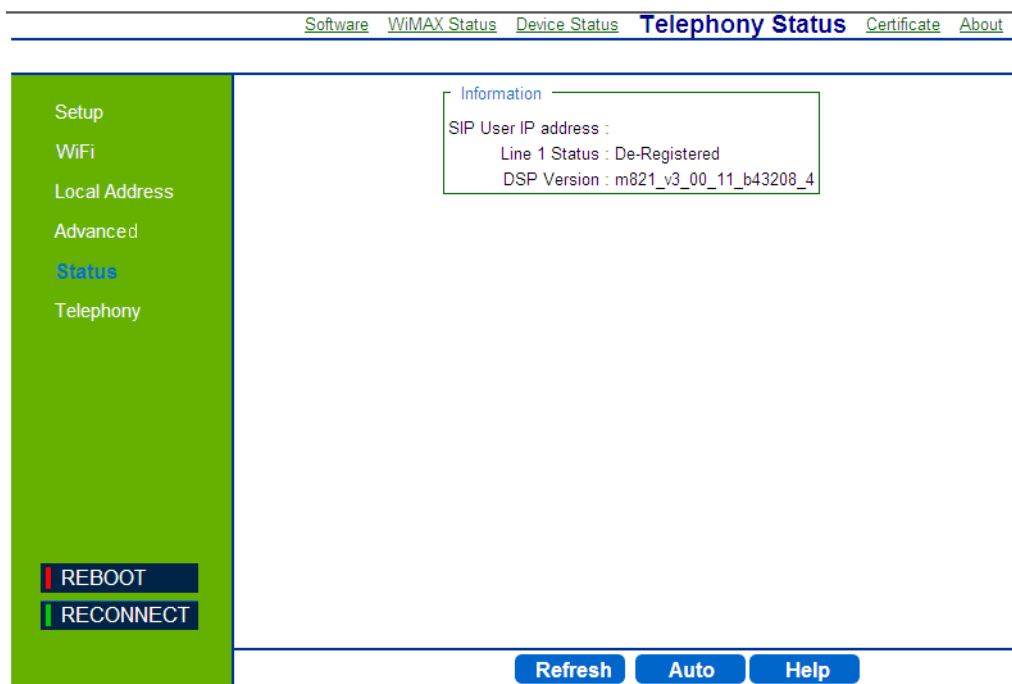
**Figure 8-3: Status - Software**

- 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

## 8.5 Telephony Status

This page displays information on the telephone line status.



**Figure 8-4: 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 and Line 2 Status** - Registered or De-registered in the SIP server. This information should be confirmed by observing the status of the front panel voice line LEDs (only on the BreezeMAX 4000 Si Premium 2.5 model).
- **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).



## 8.6 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.

### IMPORTANT



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

[Device Status](#)
[WiMAX Status](#)
[Software](#)
[Telephony Status](#)
[Certificate](#)
[About](#)

---

Setup

WiFi

Local Address

Advanced

Status

REBOOT

RECONNECT

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 8-5: 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)

**NOTE**

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.

## 8.7 About

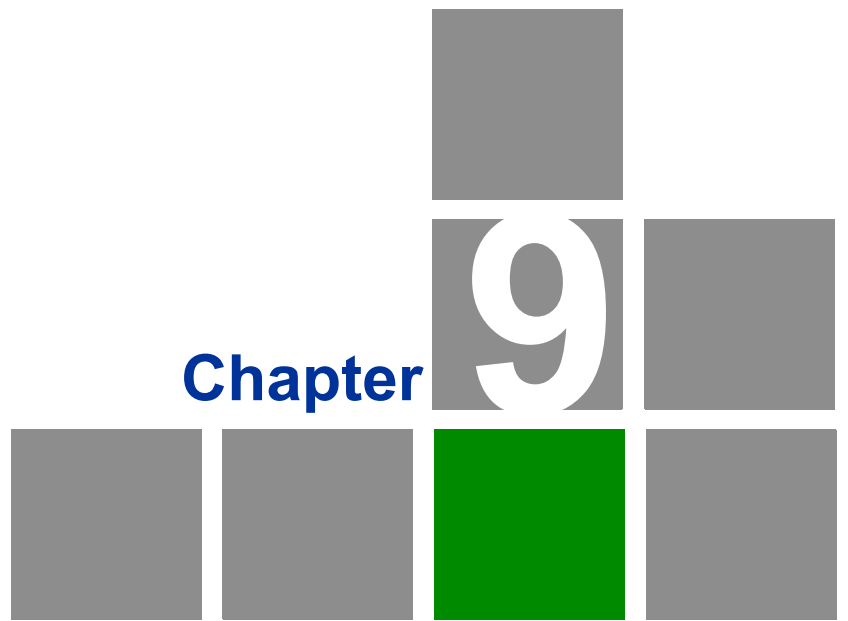
This page displays the current information about the unit. The information is set by the manufacturer as the factory defaults.

The information includes:

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



Figure 8-6: Status - About



# Configuring Telephony Parameters

## In this chapter

- [“VoIP Parameters” on page 102](#)

## VoIP Parameters

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 or two voice lines. 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 two Phone ports to be configured separately with different settings.

### IMPORTANT



You do not need to modify the user name, password, or user account settings; they are automatically populated when the modem is configured after purchase. If you are having trouble with your voice service, contact Customer Care for support. Do not make changes to these items in an attempt to restore your service.

**VoIP**

Line1

User Name:

PassWord:

Confirm PassWord:

User Account:

Display Name:

Call Waiting:

Call Waiting TimeOut:  seconds

Call Block

No	Incoming	Outgoing
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>
11	<input type="text"/>	<input type="text"/>
12	<input type="text"/>	<input type="text"/>

**Figure 9-1: 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** - Enables suspending the current telephone call and switch to a new incoming call (Default: Enabled).
- **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).



A decorative graphic consisting of a staircase of gray squares. The bottom row has four squares, the middle row has two squares, and the top row has one square.

**Chapter** **10**

**Troubleshooting**

## In This Chapter:

This chapter provides a lists of things to check in case of problems before contacting local Customer Support.

Check the following before contacting local Customer Support.

- 1 If you cannot access the Internet from the PC, check the following:
  - » If you cannot access the Internet, be sure your Windows system is correctly configured for TCP/IP. The IP settings should be set to “obtain an IP address automatically”.
  - » You may be out of the service area of the WiMAX base station. Check with the WiMAX service provider for service coverage information.
  - » If you cannot resolve the problem, check the System Status page of the web interface and contact your WiMAX service provider.
- 2 If the management interface cannot be accessed using a web browser:
  - » Be sure the management station is correctly configured for TCP/IP. The IP settings should be set to “obtain an IP address automatically.”
  - » Try a Ping command from the management station to the unit’s IP address to verify that the entire network path between the two devices is functioning correctly.
  - » Check that the management station has a valid network connection and that the Ethernet port that you are using has not been disabled.
  - » Check the network cabling between the management station and the unit. If the problem is not resolved, try using a different port or a different cable.
- 3 Forgot or Lost the Password
  - » Set the unit to its default configuration by pressing the reset button on the rear panel for 5 seconds or more. Then use the default password Alvarion to access the management interface.

**NOTE**



All user settings will be lost, including WiFi and Voice settings. Voice settings can be reconfigured by contacting Customer Support.

- 4 If all other recovery measures fail and the unit is still not functioning properly, take either of these steps:
  - » Reset the unit using the web interface, or through a power reset.
  - » Reset the unit to its factory default configuration by pressing the reset button on the rear panel for 5 seconds or more. Then use the default user

name and password to access the management interface (see [“Accessing the Web Management Interface”](#) on page 33).

**Table 10-1: Troubleshooting Chart**

Ports	Description
<ul style="list-style-type: none"> <li>■ Power LED is Off</li> </ul>	<ul style="list-style-type: none"> <li>■ AC power adapter may be disconnected. Check connections between the unit, the AC power adapter, and the wall outlet.</li> </ul>
<ul style="list-style-type: none"> <li>■ WiMAX LED is Off</li> </ul>	<ul style="list-style-type: none"> <li>■ Check with the WiMAX service provider for service coverage information.</li> </ul>
<ul style="list-style-type: none"> <li>■ WiMAX Signal Strength LEDs are Off</li> </ul>	<ul style="list-style-type: none"> <li>■ Change the location of the unit, to a nearby window or an upper floor if possible. Keep away from metal objects.</li> <li>■ Check with the WiMAX service provider for service coverage information.</li> </ul>
<ul style="list-style-type: none"> <li>■ LAN link LED is Off</li> </ul>	<ul style="list-style-type: none"> <li>■ Verify that the unit and attached device are powered on.</li> <li>■ Be sure the cable is plugged into both the unit and corresponding device.</li> <li>■ Verify that the proper cable type is used and its length does not exceed specified limits.</li> <li>■ Check the cable connections for possible defects. Replace the defective cable if necessary.</li> </ul>

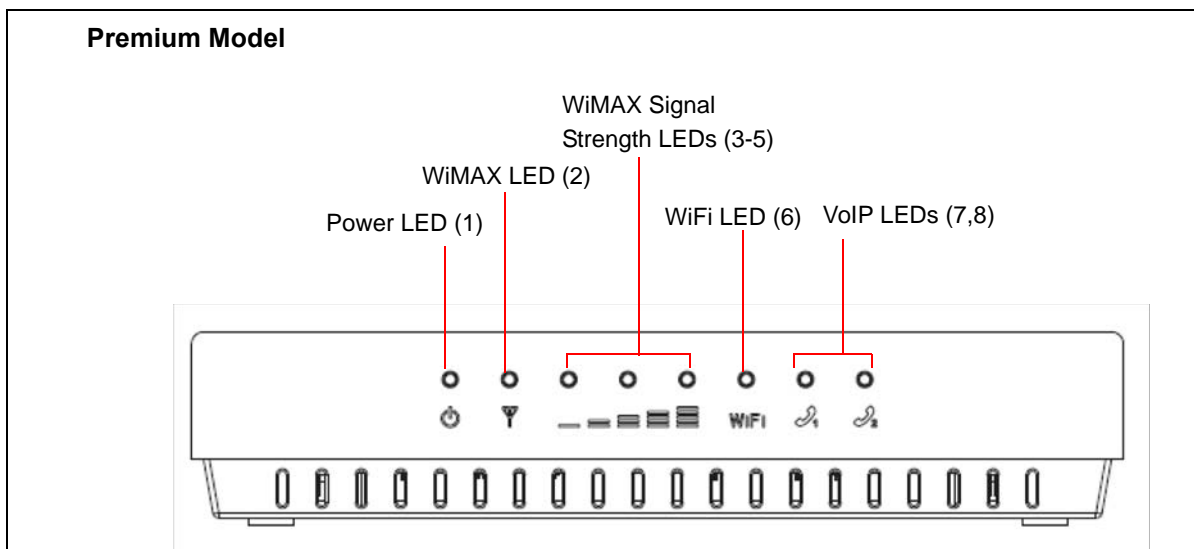
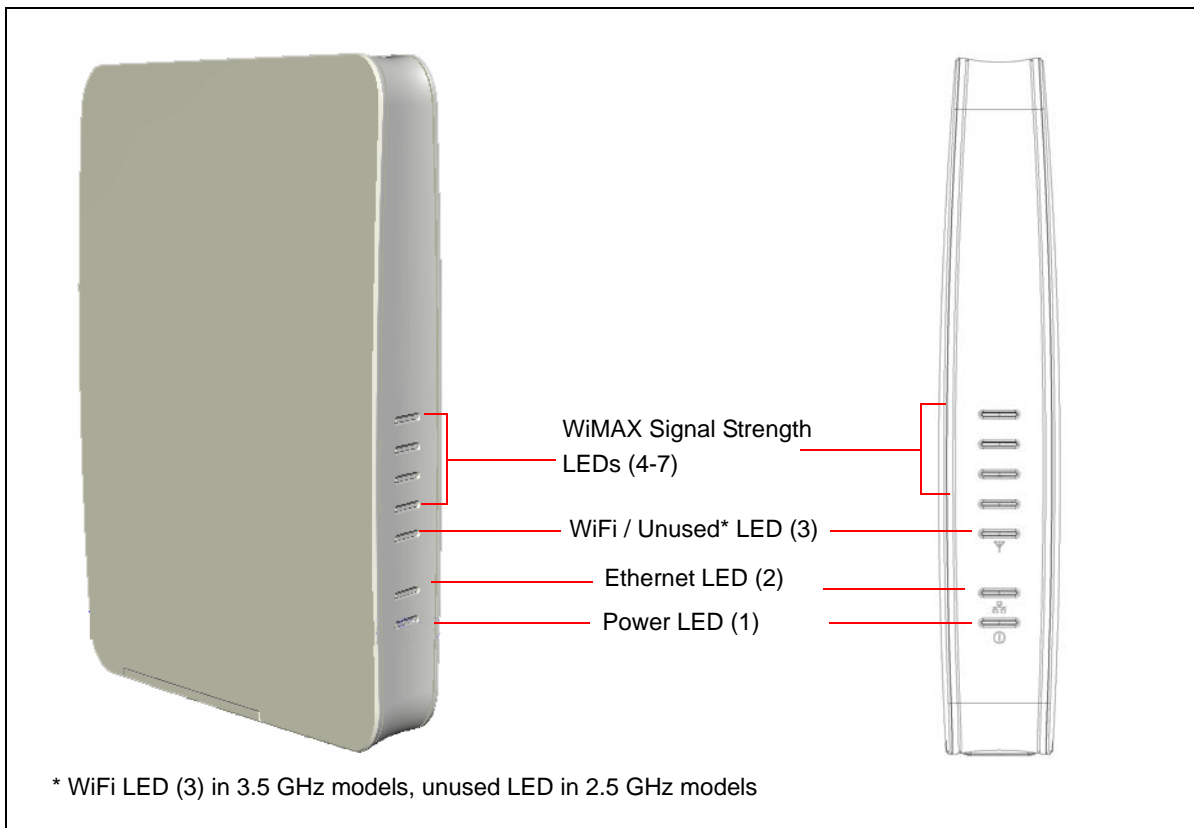


Figure 10-1: BreezeMAX Si 4000 and BreezeMAX Si 4000 Premium model Front Panel



Glossary

<b>100BASE-TX</b>	IEEE 802.3u specification for 100 Mbps Fast Ethernet over two pairs of Category 5 or better UTP cable.
<b>10BASE-T</b>	IEEE 802.3 specification for 10 Mbps Ethernet over two pairs of Category 3 or better UTP cable
<b>Advanced Encryption Standard (AES)</b>	An strong encryption algorithm that implements symmetric key cryptography.
<b>Access List (ACL)</b>	A list of MAC addresses which are allowed to access the device
<b>Automatic Gain Control (AGC)</b>	Automatic electronic regulation by recording devices of video and audio signals at a predetermined rate (by electronic control).
<b>Authentication</b>	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.
<b>Auto-negotiation</b>	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.
<b>Best Effort (BE)</b>	One of the five QoS service types defined in the IEEE 802.16 WiMAX.
<b>Base Station</b>	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.
<b>Broadcast Key</b>	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.
<b>Channel Allocation Priority Level (CAPL)</b>	<p>CAPL scan list is defined by the customer provisioned list. There are some parameters with CAPL scan: NAPID, priority and RefID.</p> <p>NAPID is used to filter some BS if the NAPID is not matched.</p> <p>Priority is the customer defined priority scan order. Higher priority will be scanned first.</p> <p>RefID is a result of mapping from IDs into a scan list from the channel plan.</p>

<b>CINR</b>	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.).
<b>Clear to Send (CTS)</b>	Signal that gives a modem permission to send data.
<b>Customer Premise Equipment (CPE)</b>	Customer Premise Equipment: Communications equipment that resides on the customer's premises.
<b>Dynamic Host Configuration Protocol (DHCP)</b>	A protocol used to assign IP addresses to computers on a Microsoft NT local area network
<b>Domain Name System (DNS)</b>	A mechanism used for translating host names for network nodes into IP addresses.
<b>Dynamic Domain Name System (DDNS)</b>	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.
<b>Dynamic Host Control Protocol (DHCP)</b>	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.
<b>(“Demilitarized Zone”) DMZ</b>	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.
<b>Data/Digital Signal Processor (DSP)</b>	A system that controls voice quality
<b>Differentiated Services Code Point (DSCP)</b>	A field in the header of IP packets for packet classification purposes.
<b>Dual Tone Multi Frequency (DTMF)</b>	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.
<b>Extended Real-time POLLING SERVICE (ertPS)</b>	One of the five QoS service types defined in the IEEE 802.16 WiMAX.



<b>Ethernet</b>	A popular local area data communications network, which accepts transmission from computers and terminals.
<b>Ethernet Conversion Sublayer (ETH CS)</b>	A mode in which transmitted packets contain an 802.3 header
<b>Encryption</b>	Data passing between the SU-A-EZ and clients can use encryption to protect from interception and eavesdropping.
<b>Extended Service Set (ESS)</b>	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.
<b>Extensible Authentication Protocol (EAP)</b>	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
<b>EAP-Tunneled Transport Layer Security (EAP-TTLS)</b>	An EAP protocol that extends TLS.
<b>File Transfer Protocol (FTP)</b>	File Transfer Protocol: A TCP/IP protocol used for file transfer.
<b>Hypertext Transfer Protocol (HTTP)</b>	Hypertext Transfer Protocol: HTTP is a standard used to transmit and receive all data over the World Wide Web.
<b>IDENT</b>	An Internet protocol that helps identify the user of a particular TCP connection.
<b>IEEE 802.16e</b>	A standard that provides mobile broadband wireless access using Scalable Orthogonal Frequency Division Multiple Access (SOFDMA).
<b>Internet Low Bitrate Codec (iLBC)</b>	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.
<b>IP Conversion Sublayer (IP-CS)</b>	A mode in which transmitted packets contain an 802.3 header
<b>Itsy Package Management System (IPKG, ipkg)</b>	Itsy Package Management System - a lightweight package management system designed for embedded devices.

<b>Internet Protocol Security (IPsec)</b>	A protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream.
<b>Jitter Buffer (JB)</b>	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.
<b>Local Area Network (LAN)</b>	Local Area Network: A group of interconnected computer and support devices.
<b>Layer 2 Tunneling Protocol (L2TP)</b>	A tunneling protocol used to support virtual private networks (VPNs).
<b>Media Access Control (MAC)</b>	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.
<b>MAC Address</b>	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.
<b>Maximum Transmission Unit (MTU)</b>	Largest size of a data packet or frame that can be sent in one complete unit over a packet-based computer network
<b>Multiple Input Multiple Output (MIMO)</b>	Using multiple antennas in a Wi-Fi device to improve performance and throughput.
<b>MSCHAPV2 (MS-CHAP. v2)</b>	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.

<b>Network Access Point (NAP)</b>	Network exchange point equipped with large-scale switching facilities and serving as a connection point between individual Internet Service Providers
<b>Network Address Translation (NAT)</b>	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.
<b>Network Time Protocol (NTP)</b>	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.
<b>Open Mobile Alliance (OMA)</b>	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.
<b>Orthogonal Frequency Division Multiplexing (OFDM)</b>	Orthogonal Frequency Division Multiplexing: OFDM allows multiple users to transmit in an allocated band by dividing the bandwidth into many narrow bandwidth carriers.
<b>Physical Layer Device (PHY)</b>	The term used for a transceiver in Fast Ethernet and Gigabit Ethernet systems.
<b>Plain Old Telephone Service (POTS)</b>	Standard analog telephone service, regular telephone line without extra enhancements
<b>Power Over Ethernet (PoE)</b>	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 <sup>2</sup> s and network devices, and significantly decreased installation costs.
<b>Point to Point Tunneling Protocol (PPTP)</b>	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)
<b>Quadrature Phase Shift Keying (QPSK)</b>	A digital modulation scheme that conveys data by changing, or modulating, the phase of a reference signal (the carrier wave).

<b>Received signal strength indication (RSSI)</b>	<p>A measurement of the power present in a received radio signal.</p> <p>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.</p>
<b>Real-time Transport Protocol (RTP)</b>	<p>The Real-time Transport Protocol (RTP) defines a standardized packet format for delivering audio and video over the Internet.</p>
<b>Real-time Transport Control Protocol (RTCP)</b>	<p>Real-time Transport Control Protocol (RTCP) is a sister protocol of the Real-time Transport Protocol (RTP).</p> <p>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.</p>
<b>RTS Threshold</b>	<p>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.</p>
<b>Service Set Identifier (SSID)</b>	<p>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).</p>
<b>Session Key</b>	<p>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.</p>
<b>Shared Key</b>	<p>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.</p>
<b>Session Initiation Protocol (SIP)</b>	<p>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.</p>
<b>Simple Network Management Protocol (SNMP)</b>	<p>Simple Network Management Protocol: The application protocol in the Internet suite of protocols which offers network management services.</p>

<b>Simple Network Time Protocol (SNTP)</b>	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.
<b>Single Input Single Output (SISO)</b>	A form of antenna technology for wireless communications in which a single antenna at both the transmitter and at the destination (receiver) are used.
<b>Subscriber Station</b>	A general term for a customer's WIMAX terminal equipment that provides connectivity with a base station.
<b>Temporal Key Integrity Protocol (TKIP)</b>	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.
<b>TR-069 (Technical Report 069)</b>	<p>A DSL Forum technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices.</p> <p>It provides the communication between CPE and Auto Configuration Servers (ACS).</p>
<b>Trivial File Transfer Protocol (TFTP)</b>	Trivial File Transfer Protocol: A TCP/IP protocol commonly used for software downloads.
<b>Transport Layer Security (TLS)</b>	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.
<b>Point to Point Tunneling Protocol (PPTP)</b>	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)
<b>Unsolicited Grant Service (UGS)</b>	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.

<b>User Datagram Protocol (UDP)</b>	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)
<b>Universal Plug and Play Internet Gateway Device (UPnP IGD)</b>	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.
<b>UTP</b>	Unshielded twisted-pair cable.
<b>Voice Activity Detection (VAD)</b>	Enables the detection of periods of silence in the audio stream so that it is not transmitted over the network.
<b>Wide Area Network (WAN)</b>	Communications network intended to connect between remote local area networks
<b>Wired Equivalent Privacy (WEP)</b>	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.
<b>Wireless Application Protocol (WAP)</b>	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.
<b>Wi-Fi Protected Access (WPA)</b>	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.