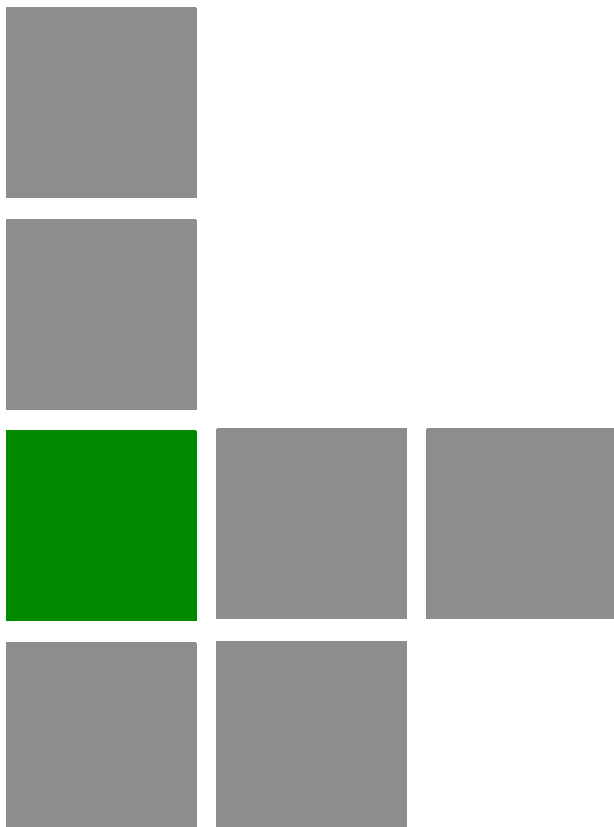


## BreezeMAX<sup>®</sup> Si 2000 CPE

---



## User Manual

---

SW Version: 1.0  
September 2009  
P/N 215401

## Document History

Topic	Description	Date Issued
BreezeMAX Si 2000 CPE User Manual	This is the document's first release.	December 2008
WiFi Radio Specifications <a href="#">Section 1.2.2</a>	Updated to correct error for Operation Mode.	August 2009
Configuration and Management <a href="#">Section 1.2.4</a>	Remove SNMP support.	August 2009
Accessing the Web Management Interface, <a href="#">Section 3.1.1</a>	Added information for Operator mode access.	August 2009
Using the Basic Setup <a href="#">Section 3.1.2</a>	Updated "Setup Wizard" to "Basic Setup".	August 2009
The Advanced Setup Menu <a href="#">Section 3.2</a>	Added Operator Mode menu, including WAN setup option.	August 2009
System Settings <a href="#">Chapter 4</a>	Added Operator Mode sections for Host Name, TR069 Settings, and System Log.	August 2009
Administrator Settings <a href="#">Section 4.4</a>	Added default password for Operator Mode.	August 2009
Configuration Tools <a href="#">Section 4.6</a>	Added information on Backup Settings/Restore Settings for Operator Mode	August 2009
TR069 Settings <a href="#">Section 4.8</a>	Added TR069 Settings for software release v1.0.0.24.	August 2009
Gateway Configuration <a href="#">Chapter 5</a>	Added Operator Mode sections for Operation Mode, and WAN Settings.	August 2009
Gateway Configuration Introduction <a href="#">Section 5.1</a>	Added menu for Operator Mode.	August 2009
Operation Mode <a href="#">Section 5.2</a>	Added Operation Mode for software release v1.0.0.24.	August 2009
WAN Settings <a href="#">Section 5.3</a>	Added Operator Mode section for WAN Settings.	August 2009
WiMAX Settings <a href="#">Chapter 6</a>	Modified WiMAX Login section for Profile Settings and added Advanced Configuration	August 2009
WiMAX Settings Introduction <a href="#">Section 6.1</a>	Added menu for Operator Mode.	August 2009
WiMAX Login <a href="#">Section 6.2</a>	Added Profile Settings for Operator Mode.	August 2009
Advanced Configuration <a href="#">Section 6.5</a>	Added Operator Mode section for Advanced Configuration.	August 2009

Topic	Description	Date Issued
VoIP Settings <a href="#">Chapter 7</a>	Modified SIP Account section and added SIP Settings, Call Feature, Codecs, Call Block Setting, and Phone Setting.	August 2009
VoIP Settings Introduction <a href="#">Section 7.1</a>	Added menu for Operator Mode.	August 2009
SIP Account <a href="#">Section 7.2</a>	Added SIP Account settings for Operator Mode.	August 2009
SIP Setting <a href="#">Section 7.3</a>	Added Operator Mode section for SIP Settings.	August 2009
Call Feature <a href="#">Section 7.5</a>	Added Operator Mode section for Call Feature.	August 2009
Codecs <a href="#">Section 7.6</a>	Added Operator Mode section for Codecs.	August 2009
Call Block Setting <a href="#">Section 7.7</a>	Added Operator Mode section for Call Block Setting.	August 2009
Phone Setting <a href="#">Section 7.8</a>	Added Operator Mode section for Phone Settings.	August 2009
Wireless Settings <a href="#">Section 8.2</a>	Removed “G Only” option for working mode.	August 2009

## Legal Rights

© Copyright 2009 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>, BreezeCONFIG<sup>™</sup>, MGW<sup>™</sup>, eMGW<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).

### 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.

## Radio Frequency Interference Statement

The BreezeMAX Si 2000 Access Unit has been tested and found to comply with the limits for a class B digital device, pursuant to part 15 of the FCC rules and to EN 301 489-1 rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential environment notwithstanding use in commercial, business and industrial environments. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

## FCC Radiation Hazard Warning

To comply with FCC RF exposure requirements in Section 1.1307 and 2.1091 of FCC Rules, the antenna used for this transmitter must be fixed-mounted on outdoor permanent structures with a separation distance of at least 2 meter from all persons.

## 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.

## Outdoor Unit and Antenna Installation and Grounding

Ensure that outdoor units, antennas and supporting structures are properly installed to eliminate any physical hazard to either people or property. Make sure that the installation of the outdoor unit, antenna and cables is performed in accordance with all relevant national and local building and safety codes. Even

where grounding is not mandatory according to applicable regulation and national codes, it is highly recommended to ensure that the outdoor unit and the antenna mast (when using external antenna) are grounded and suitable lightning protection devices are used so as to provide protection against voltage surges and static charges. In any event, Alvarion is not liable for any injury, damage or regulation violations associated with or caused by installation, grounding or lightning protection.

## Disposal of Electronic and Electrical Waste



### 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 (Pb)	镉 (Cd)	汞 (Hg)	六价铬 (Cr <sup>6+</sup> )	PBB (多溴联苯)	PBDE (多溴二苯乙醚)
含铜线材	×	○	○	○	○	○
连接器	×	○	○	○	○	○
变压器	×	○	○	○	○	○
陶瓷电容	×	○	○	○	○	○
高温锡材	×	○	○	○	○	○
○：表示此部件使用的所有同类材料中此种有毒或有害物质的含量均低于 SJ/T11363-2006 规定的限制要求。 ×：表示此部件使用的至少一种同类材料中，此种有毒或有害物质的含量高于 SJ/T11363-2006 规定的限制要求。						
The above table provides information required under the following Chinese legislation: Management methods for Controlling Pollution by Electronic Information Products(No.39) (also known as China RoHS)						



## Important Notice

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

- This manual contains proprietary information belonging to Alvarion Ltd. Such information is supplied solely for the purpose of assisting properly authorized users of the respective Alvarion products.
- No part of its contents may be used for any other purpose, disclosed to any person or firm or reproduced by any means, electronic and mechanical, without the express prior written permission of Alvarion Ltd.
- The text and graphics are for the purpose of illustration and reference only. The specifications on which they are based are subject to change without notice.
- The software described in this document is furnished under a license. The software may be used or copied only in accordance with the terms of that license.
- Information in this document is subject to change without notice.
- Corporate and individual names and data used in examples herein are fictitious unless otherwise noted.
- Alvarion Ltd. reserves the right to alter the equipment specifications and descriptions in this publication without prior notice. No part of this publication shall be deemed to be part of any contract or warranty unless specifically incorporated by reference into such contract or warranty.
- The information contained herein is merely descriptive in nature, and does not constitute an offer for the sale of the product described herein.
- Any changes or modifications of equipment, including opening of the equipment not expressly approved by Alvarion Ltd. will void equipment warranty and any repair thereafter shall be charged for. It could also void the user's authority to operate the equipment.

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 2000 and details how to install, operate and manage it.

This manual is intended for technicians responsible for installing, setting and operating the BreezeMAX Si 2000 system, and for system administrators responsible for managing the system.

This manual contains the following chapters and appendices:

- **Chapter 1 - Product Description** - Describes the BreezeMAX Si 2000 unit and its functionality.
- **Chapter 2 - Hardware Installation** - Describes how to install the BreezeMAX Si 2000 and how to connect to subscriber's equipment.
- **Chapter 3 - Initial Configuration** - Describes how to initially configure the BreezeMAX Si 2000 in order to test basic link operation.
- **Chapter 4 - System Settings** - Describes general management functions for the BreezeMAX Si 2000.
- **Chapter 5 - Gateway Configuration** - Describes the gateway functions of the BreezeMAX Si 2000.
- **Chapter 6 - WiMAX Settings** - Describes the WiMAX configuration for the BreezeMAX Si 2000.
- **Chapter 7 - VoIP Settings** - Describes the Voice over Internet Protocol functions of the BreezeMAX Si 2000.
- **Chapter 8 - WiFi Settings** - Describes the 802.11 b/g radio functions of the BreezeMAX Si 2000 3.5 GHz model.
- **Appendix A - Troubleshooting**
- **Appendix B - GNU License**

- **Glossary** - Glossary of terms used in the BreezeMAX Si 2000 User Guide.

# Contents

## Chapter 1 - Product Description

<b>1.1 Introducing the BreezeMAX Si 2000 .....</b>	<b>3</b>
1.1.1 The BreezeMAX Si 2000 Family of Products.....	3
<b>1.2 Specifications .....</b>	<b>6</b>
1.2.1 WiMAX Radio.....	6
1.2.2 WiFi Radio.....	6
1.2.3 VoIP Specifications .....	7
1.2.4 Configuration and Management.....	8
1.2.5 Mechanical .....	9
1.2.6 Electrical.....	9
1.2.7 Environmental .....	9
1.2.8 Standards Compliance.....	10

## Chapter 2 - Hardware Installation

<b>2.1 Installation Requirements .....</b>	<b>13</b>
2.1.1 Packing List.....	13
<b>2.2 Installation Steps.....</b>	<b>14</b>
2.2.1 Selecting a Location.....	14
2.2.2 Installing the Unit.....	14
<b>2.3 BreezeMAX Si 2000 Hardware Description .....</b>	<b>16</b>
2.3.1 Scan Button.....	19
2.3.2 Reset Button .....	19
2.3.3 WiMAX Antennas .....	19
2.3.4 WiMAX External Antenna Connectors .....	19

2.3.5 LED Indicators.....	20
2.3.6 10BASE-T/100BASE-TX LAN Ports .....	22
2.3.7 10/100BASE-TX Pin Assignments .....	22
2.3.8 BreezeMAX Si 2000 Cables.....	24
2.3.9 VoIP Phone Ports.....	25
2.3.10 Power Adapter Socket .....	25
2.3.11 SIM Card Slot.....	25
2.3.12 BreezeMAX Si 2000 Wi-Fi Option .....	27
2.3.13 Cable Connections.....	28

## Chapter 3 - Initial Configuration

<b>3.1 Introduction .....</b>	<b>32</b>
3.1.1 Accessing the Web Management Interface .....	32
3.1.2 Using the Basic Setup.....	33
<b>3.2 The Advanced Setup Menu .....</b>	<b>36</b>

## Chapter 4 - System Settings

<b>4.1 Introduction .....</b>	<b>40</b>
<b>4.2 Host Name.....</b>	<b>41</b>
<b>4.3 System Status.....</b>	<b>42</b>
<b>4.4 Administrator Settings.....</b>	<b>44</b>
<b>4.5 Firmware Upgrade.....</b>	<b>45</b>
<b>4.6 Configuration Tools .....</b>	<b>46</b>
<b>4.7 System Time .....</b>	<b>48</b>
<b>4.8 TR069 Settings .....</b>	<b>50</b>
<b>4.9 System Log .....</b>	<b>52</b>
<b>4.10 Reset .....</b>	<b>53</b>

## Chapter 5 - Gateway Configuration

<b>5.1 Introduction .....</b>	<b>56</b>
<b>5.2 Operation Mode .....</b>	<b>57</b>
5.2.1 Operation Mode Settings .....	57
5.2.2 Management Settings .....	58
5.2.3 VoIP Settings .....	58
<b>5.3 WAN Settings.....</b>	<b>59</b>
5.3.1 Dynamic IP Address.....	60
5.3.2 Static IP Settings.....	60
5.3.3 L2TP Settings.....	61
5.3.4 PPPoE Settings.....	62
<b>5.4 LAN.....</b>	<b>63</b>
5.4.1 LAN Settings .....	63
5.4.2 DHCP Client List .....	65
<b>5.5 NAT.....</b>	<b>66</b>
5.5.1 Virtual Server .....	66
5.5.2 Port Mapping.....	67
5.5.3 DMZ .....	68
<b>5.6 Firewall.....</b>	<b>69</b>
5.6.1 Firewall Options .....	69
5.6.2 Client Filtering .....	70
5.6.3 MAC Control.....	71
<b>5.7 Route .....</b>	<b>72</b>
<b>5.8 UPnP.....</b>	<b>73</b>

## Chapter 6 - WiMAX Settings

<b>6.1 Introduction</b> .....	<b>76</b>
<b>6.2 WiMAX Login</b> .....	<b>77</b>
<b>6.3 Subscriber Station Information</b> .....	<b>80</b>
<b>6.4 Antenna Setting</b> .....	<b>81</b>
<b>6.5 Advanced Configuration</b> .....	<b>82</b>

## Chapter 7 - VoIP Settings

<b>7.1 Introduction</b> .....	<b>86</b>
<b>7.2 SIP Account</b> .....	<b>87</b>
<b>7.3 SIP Setting</b> .....	<b>89</b>
<b>7.4 Dial Plan</b> .....	<b>91</b>
<b>7.5 Call Feature</b> .....	<b>93</b>
<b>7.6 Codecs</b> .....	<b>95</b>
<b>7.7 Call Block Setting</b> .....	<b>97</b>
<b>7.8 Phone Setting</b> .....	<b>98</b>

## Chapter 8 - WiFi Settings

<b>8.1 Introduction</b> .....	<b>102</b>
<b>8.2 Wireless Settings</b> .....	<b>103</b>
<b>8.3 Wireless Security</b> .....	<b>107</b>
8.3.1 Wireless Security .....	107
8.3.2 WEP Shared Key Security .....	108
8.3.3 WPA/WPA2 Security.....	109
<b>8.4 MAC Authentication</b> .....	<b>110</b>

## Chapter 9 - Troubleshooting

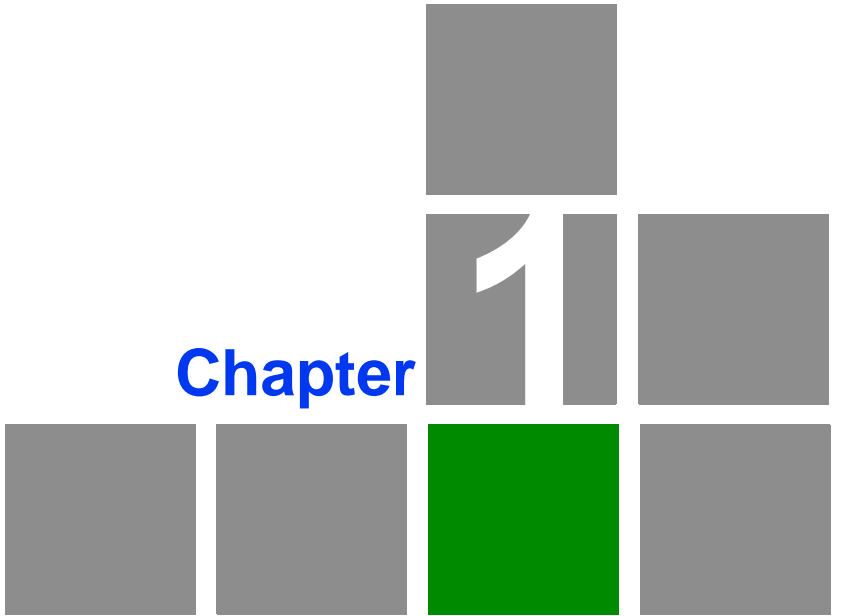
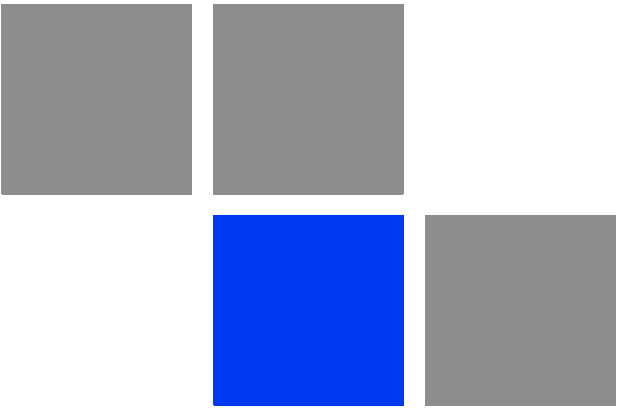
## Chapter 10 - GNU License

<b>B.1 The GNU General Public License</b> .....	<b>118</b>
---	------------



B.1.1 Preamble ..... 118

B.1.2 GNU General Public License Terms and Conditions for Copying, Distribution and Modification 119



**Product Description**

## In This Chapter:

- “Introducing the BreezeMAX Si 2000” on page 3
- “The BreezeMAX Si 2000 Family of Products” on page 3
- “Specifications” on page 6

## 1.1 Introducing the BreezeMAX Si 2000

BreezeMAX Si 2000 is a family of 20 high capacity residential gateways and WiMAX Wireless Broadband Access subscriber stations, for a home or small office. Each 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.

Part of an extended and field-proven product portfolio, BreezeMAX Si 2000 is an integral part of the BreezeMAX family, the latest most technologically advanced wireless solution for broadband deployment. With capacity of up to 13 Mbps download and 3.5 Mbps upload speed per unit, the BreezeMAX Si 2000 solution enables the delivery of powerful wireless broadband services to the subscriber. BreezeMAX Si 2000 is an out-of-the-box solution with immediate available local stock enabling virtually instant network expansion and simplified deployment. BreezeMAX-Si 2000 provides a wireless solution for the subscriber to connect to the internet.

With a range of up to 15 Km and lower equipment and deployment costs, BreezeMAX-Si 2000 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 2000 is a plug-and-play indoor unit (IDU). There are six available models for each of the 2.3, 2.5 and 3.5 GHz WiMAX licensed frequency band, see [“The BreezeMAX Si 2000 Family of Products” on page 3](#). Which model you use will depend on the frequency band of your service provider’s WiMAX service. The BreezeMAX Si 2000 models also include built-in WiMAX antennas, either standard “omnidirectional” type.

The BreezeMAX Si 2000 includes four RJ-45 Ethernet switch ports for LAN connections and two RJ-11 Voice over IP (VoIP) phone ports. An 802.11b/g Wi-Fi module providing a local WiFi access point service is included.

### 1.1.1 The BreezeMAX Si 2000 Family of Products

The following table lists the available BreezeMAX Si 2000 models:

**Table 1-1: BreezeMAX Si 2000 2.3 GHz Models**

Frequency Band	Model Number	Ports	Description
2.3 GHz	4M-CPE-Si-1D-2.3-Omni	■ 1 data port (RJ-45)	■ Omnidirectional WiMAX antennas as standard.
	4M-CPE-Si-1D2V-2.3-Omni	■ 1 data port (RJ-45) ■ 2 VoIP phone ports (RJ-11)	
	4M-CPE-Si-4D2V-2.3-Omni	■ 4 data ports (RJ-45) ■ 2 VoIP phone ports (RJ-11)	■ Omnidirectional WiMAX antennas as standard.

**Table 1-2: BreezeMAX Si 2000 2.5 GHz Models**

Frequency Band	Model Number	Ports	Description
2.5 GHz	4M-CPE-Si-1D-2.5-Omni	■ 1 data port (RJ-45)	■ Omnidirectional WiMAX antennas as standard.
	4M-CPE-Si-1D2V-2.5-Omni	■ 1 data port (RJ-45) ■ 2 VoIP phone ports (RJ-11)	
	4M-CPE-Si-4D2V-2.3-Omni	■ 4 data ports (RJ-45) ■ 2 VoIP phone ports (RJ-11)	■ Omnidirectional WiMAX antennas as standard.

**Table 1-3: BreezeMAX Si 2000 3.5 GHz Models**

Frequency Band	Model Number	Ports	Description
3.5 GHz	4M-CPE-Si-1D-3.5-Omni	■ 1 data port (RJ-45)	■ Omnidirectional WiMAX antennas as standard.
	4M-CPE-Si-1D2V-3.5-Omni	■ 1 data port (RJ-45) ■ 2 VoIP phone ports (RJ-11)	
	4M-CPE-Si-4D2V-WiFi-3.5-Omni	■ 4 data ports (RJ-45) ■ 2 VoIP phone ports (RJ-11)	■ Omnidirectional WiMAX antennas as standard. ■ WiFi (802.11b/g) enabled.

The BreezeMAX Si 2000 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).

The initial configuration steps can be made through the web browser interface using the Setup Wizard. It is recommended to make the initial changes by connecting a PC directly to one of the unit's LAN ports.

## 1.2 Specifications

### 1.2.1 WiMAX Radio

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

Item	Description
<b>Radio Type</b>	IEEE 802.16e WAVE 1 & WAVE 2
<b>Frequency Band</b>	<ul style="list-style-type: none"> <li>■ 2300 MHz or</li> <li>■ 2500 MHz or</li> <li>■ 3500 MHz</li> </ul>
<b>Antenna Type</b>	<ul style="list-style-type: none"> <li>■ Omnidirectional: Built-in dual dipole antennas</li> <li>Transmit: Single antenna</li> </ul>
<b>Channel Bandwidth</b>	5.00, 7.00, and 10.00 MHz
<b>Maximum Throughput</b>	3.5 Mbps Upload, 13 Mbps download
<b>Antenna Technology</b>	Maximum-Ratio Combining (MRC)
<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>■ Down Link: QPSK, 16 QAM, 64 QAM</li> <li>■ Up Link: QPSK, 16 QAM, 64 QAM</li> <li>■ FEC 1/2, 3/4, 5/6</li> </ul>
<b>Antenna Gain</b>	<ul style="list-style-type: none"> <li>■ Omnidirectional: Gain: 5 dBi at 2.5 GHz, 4 dBi at 3.5 GHz, and 3 dBi at 2.3 GHz</li> </ul>
<b>TPL (Transmit Power Level)</b>	+26 dBm maximum
<b>Receive Sensitivity</b>	-94 dBm maximum

### 1.2.2 WiFi Radio



#### NOTE

This section only applies to the 4M-CPE-Si-4D2V-WiFi-3.5-Omni.

**Table 1-5: WiFi Radio Specifications**

Item	Description
<b>Radio Type</b>	IEEE 802.11b, IEEE 802.11g
<b>Frequency Band</b>	<ul style="list-style-type: none"> <li>■ 2.4 ~ 2.4835 GHz (US, Canada)</li> <li>■ 2.4 ~ 2.497 GHz (Japan)</li> <li>■ 3.4 ~ 3.6 GHz (ETSI)</li> </ul>
<b>Maximum Channels</b>	<ul style="list-style-type: none"> <li>■ FCC/IC: 1-11</li> <li>■ ETSI: 1-13</li> <li>■ France: 10-13</li> <li>■ MKK: 1-14</li> </ul>
<b>Data Rates</b>	<ul style="list-style-type: none"> <li>■ 802.11g: 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps (automatic fall back)</li> <li>■ 802.11b: 1, 2, 5.5, 11 Mbps (automatic fall back)</li> </ul>
<b>Radio Technology</b>	Orthogonal Frequency Divisional Multiplexing (OFDM)
<b>Modulation Technique</b>	<ul style="list-style-type: none"> <li>■ 802.11g: CCK, BPSK, QPSK, OFDM</li> <li>■ 802.11b: CCK, BPSK, QPSK</li> </ul>
<b>FEC Coding Rates</b>	1/2 2/3, 3/4
<b>Max Tx Power Levels at Antenna Port</b>	<ul style="list-style-type: none"> <li>■ 802.11b: 18 dBm*</li> <li>■ 802.11g: 14 dBm*</li> </ul>
<b>RF Receive Sensitivity</b>	<ul style="list-style-type: none"> <li>■ 802.11b: -88 dBm @ 11 Mbps</li> <li>■ 802.11g: -74 dBm @ 54 Mbps</li> </ul>
<b>TPC (Transmit Power Control)</b>	100%, 50%, 25%, 12.5%, Min (0 dBm).
<b>Antenna</b>	Diversity Antenna
*The maximum value can be lower depending on the radio band and modulation used. Check <a href="#">Table 1-6</a> for details.	

### 1.2.3 VoIP Specifications

**Table 1-6: VoIP Specifications**

Item	Description
<b>Voice Signalling Protocol</b>	SIP v2 (RFC 3261)



**Table 1-6: VoIP Specifications**

Item	Description
<b>Voice Codecs</b>	<ul style="list-style-type: none"> <li>■ G.711 (a-law and u-law)</li> <li>■ G.726</li> <li>■ G.729ab</li> <li>■ G.723</li> <li>■ AMR-NB</li> </ul>
<b>Voice Quality</b>	<ul style="list-style-type: none"> <li>■ VAD (Voice Activity Detection)</li> <li>■ CNG (Comfortable Noise Generation)</li> <li>■ Echo cancellation (G.165/G.168)</li> <li>■ Adaptive jitter buffer, up to 200 milliseconds</li> <li>■ DTMF tone detection and generation</li> </ul>
<b>Call Features</b>	<ul style="list-style-type: none"> <li>■ Call transfer</li> <li>■ Call waiting/hold/retrieve</li> <li>■ 3-way conference call</li> <li>■ Call blocking</li> <li>■ T.38 fax relay</li> <li>■ Dial plan (E.164 dialing plan)</li> <li>■ Call forwarding: No Answer/Busy/All</li> </ul>
<b>REN (Ring Equivalent Number)</b>	<ul style="list-style-type: none"> <li>■ 3 REN total in system</li> </ul>

## 1.2.4 Configuration and Management

**Table 1-7: 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>
<b>Management access</b>	From Wired LAN, Wireless Link
<b>Management access protection</b>	Access Password

**Table 1-7: Configuration and Management**

Item	Description
<b>Encryption</b>	WEP 152-bits
<b>Allocation of IP parameters</b>	Configurable or automatic (DHCP client)
<b>Software upgrade</b>	HTTP
<b>Configuration Upload/Download</b>	HTTP

## 1.2.5 Mechanical

**Table 1-8: Mechanical Specifications**

Item	Description
<b>Dimensions</b>	169mm (H) X 184mm (W) X 80 (T) X 74mm
<b>Weight</b>	1.6kg
<b>Mounting</b>	Desktop

## 1.2.6 Electrical

**Table 1-9: Electrical Specifications**

Type	Details
<b>AC Power Supply</b>	Input: 100-240 VAC, 50-60 Hz, maximum power consumption 0.5A Output: 19 VDC, maximum power consumption 3.4A

## 1.2.7 Environmental

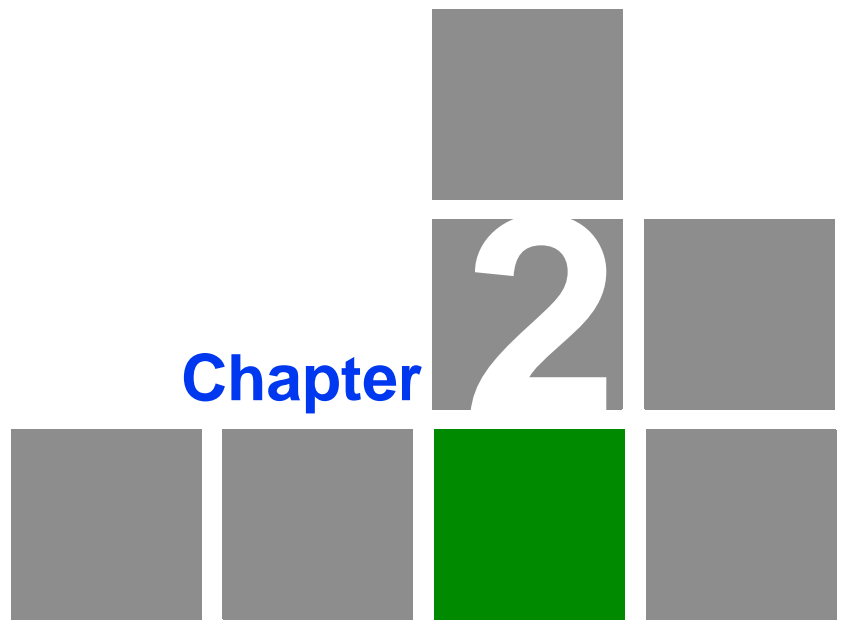
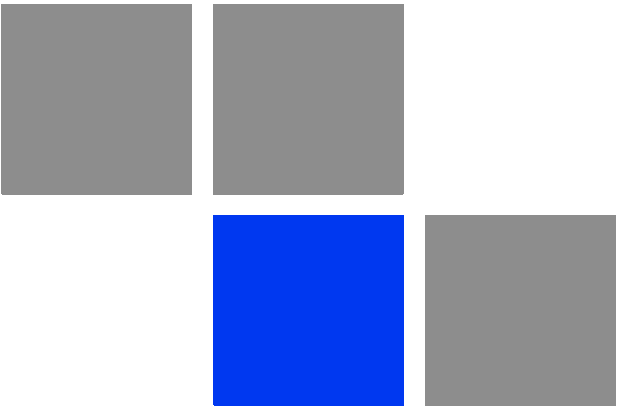
**Table 1-10: Environmental Specifications**

Item	Details
<b>Operating Temperature</b>	-5°C to 45°C
<b>Storage Temperature</b>	-40 to 75 °C
<b>Humidity</b>	Maximum 95%, non-condensing

## 1.2.8 Standards Compliance

**Table 1-11: Standards Compliance**

Type	Standard
<b>EMC</b>	<ul style="list-style-type: none"> <li>■ FCC Part 15B Class B</li> <li>■ ETSI EN 301 489-1/4</li> <li>■ EN 55022 Class B</li> </ul>
<b>Safety</b>	<ul style="list-style-type: none"> <li>■ UL 60950-1</li> <li>■ EN 60950-1 / IEC 60950-1</li> </ul>
<b>Radio</b>	<ul style="list-style-type: none"> <li>■ FCC Part 25, 27</li> <li>■ EN 300 328, EN 302 326-1, EN 302 326-2</li> <li>■ ETSI EN 302 544-2</li> </ul>
<b>Standards</b>	<ul style="list-style-type: none"> <li>■ IEEE 802.16e-2005 WAVE 1 and WAVE 2</li> <li>■ IEEE 802.3-2005 10BASE-T and 100BASE-TX</li> <li>■ IEEE 802.11b and 802.11g</li> <li>■ UPnP</li> </ul>



# Chapter 2

## Hardware Installation

## In This Chapter:

- “Installation Requirements” on page 13
- “Packing List” on page 13
- “Installation Steps” on page 14
- “Selecting a Location” on page 14
- “BreezeMAX Si 2000 Hardware Description” on page 16
- “Cable Connections” on page 28

## 2.1 Installation Requirements

This section describes how to install and connect the BreezeMAX Si 2000 WiMAX Residential Gateway.

### 2.1.1 Packing List

The BreezeMAX Si 2000 package includes the following components:

- BreezeMAX Si 2000 unit with integrated antennas\*
- RJ-45 Category 5 network cable
- AC power adapter
- Software Utilities and User Guide CD

\*For the particular specifications of your choice of model see [“The BreezeMAX Si 2000 Family of Products” on page 3](#)



**Figure 2-1: Package Contents**

## 2.2 Installation Steps



### CAUTION

The BreezeMAX Si 2000 is an indoor unit and must not be installed outdoors.

Before installing the BreezeMAX Si 2000, 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 dealer. Also, be sure you have all the necessary tools and cabling before installing the BreezeMAX Si 2000.

### 2.2.1 Selecting a Location

The BreezeMAX Si 2000 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, which is out of direct sunlight.
- The device should have adequate space (approximately two inches) on all sides for proper air flow.
- The device must be near an AC power outlet that provides 100 to 240 V, 50 to 60 Hz.
- The device should be accessible for network cabling and allow the status LED indicators to be clearly visible.
- Care should be taken to avoid mounting the unit close to metal objects as this can deflect the BTS WiMAX signal.

### 2.2.2 Installing the Unit

The BreezeMAX Si 2000 is a plug-and-play device, so once it has been connected to your PC and powered up, it is fully operable.

- 1 Mount the unit on a flat horizontal surface indoors.
- 2 Connect the Ethernet cable to your PC or notebook computer.
- 3 Connect the power injector to the unit, and plug the AC connector into a suitable power source.

- 4 Align the unit so that you receive the strongest signal by monitoring the readout of 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**

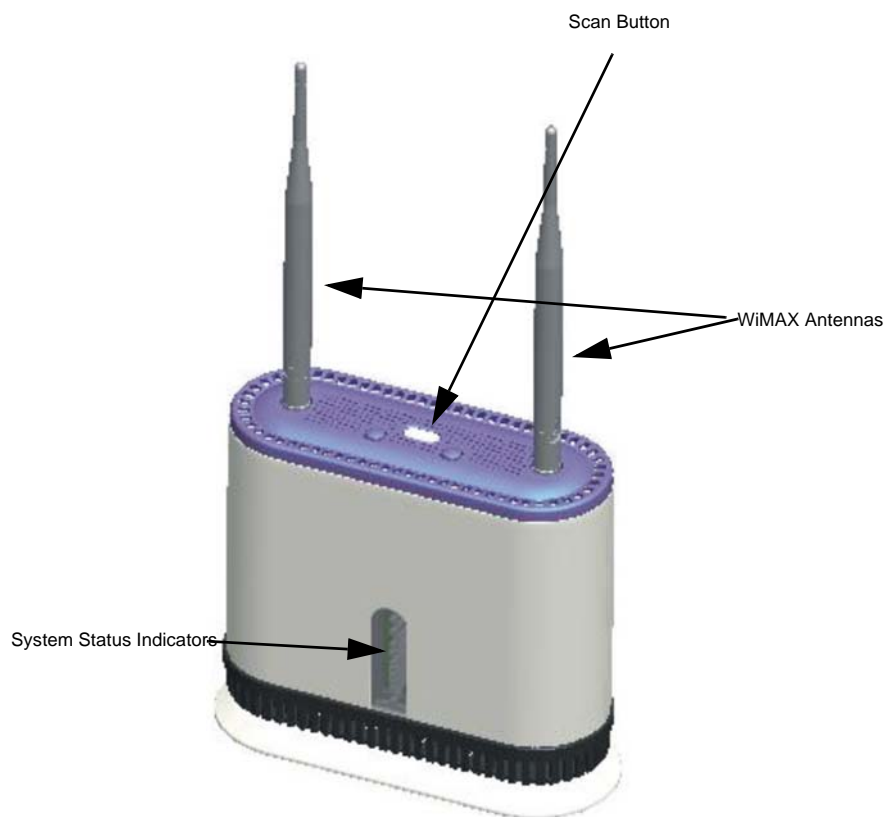
If the BreezeMAX Si 2000 displays a weak WiMAX receive signal, try moving it to another location. Alternatively, you can connect optional external antennas to the unit to improve performance.



## 2.3 BreezeMAX Si 2000 Hardware Description

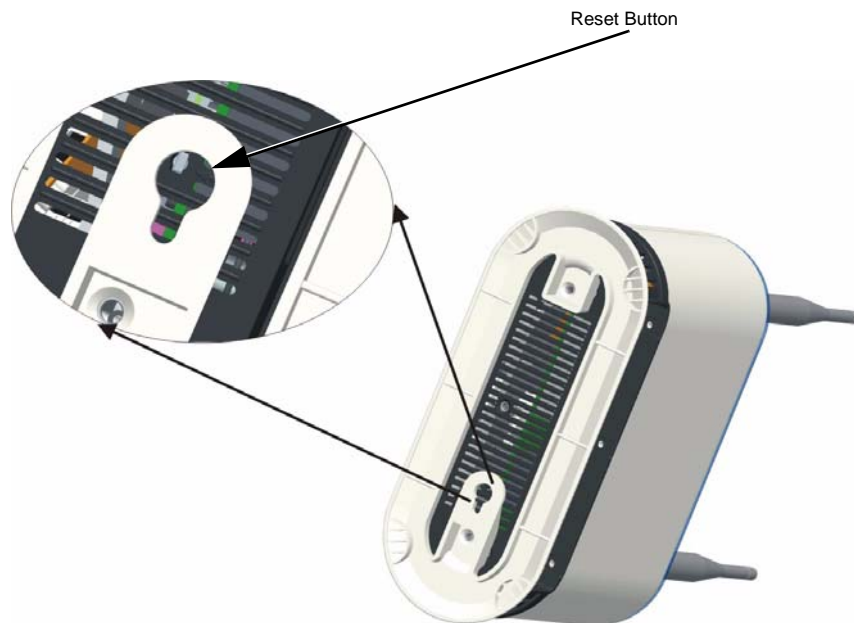
The front of the BreezeMAX Si 2000 provides an array of system status indicators. The back includes one~four LAN ports for 10/100 Mbps Ethernet connections (depending on your choice of model), two RJ-11 Voice over IP (VoIP) phone ports, and a DC power jack.

The following figures show the external components of the BreezeMAX Si 2000:



**Figure 2-2: Components View**

The following figure shows the base of the BreezeMAX Si 2000 and the location of the reset button.



**Figure 2-3: Reset Button**

The following figures show the rear of each different BreezeMAX Si 2000 model and the location of their ports.



**NOTE**

The location and number of ports on the BreezeMAX Si 2000 range is dependent on the model you have purchased.

- 4M-CPE-Si-4D2V-2.3-Omni;
- 4M-CPE-Si-4D2V-2.5-Omni;
- 4M-CPE-Si-4D2V-WiFi-3.5-Omni:

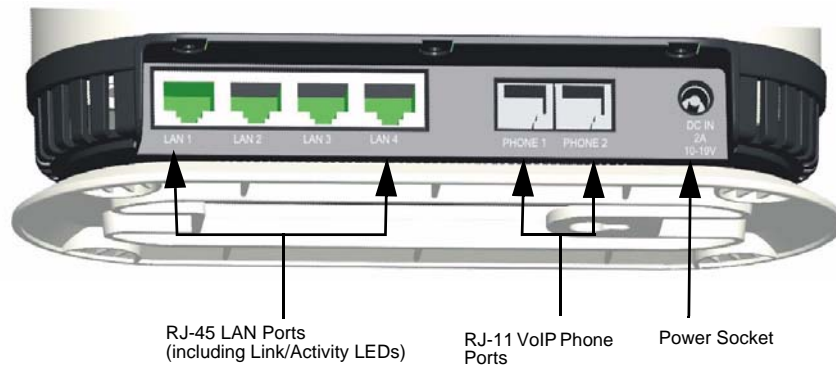


Figure 2-4: 4 Data/2 VoIP Port Model

- 4M-CPE-Si-1D2V-2.3-Omni;
- 4M-CPE-Si-1D2V-2.5-Omni;
- 4M-CPE-Si-1D2V-3.5-Omni:

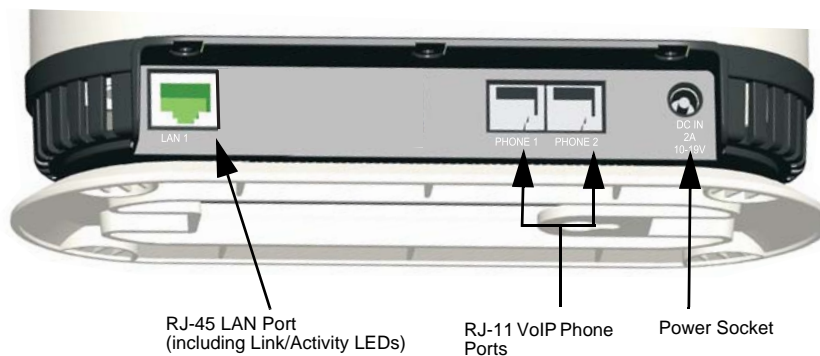
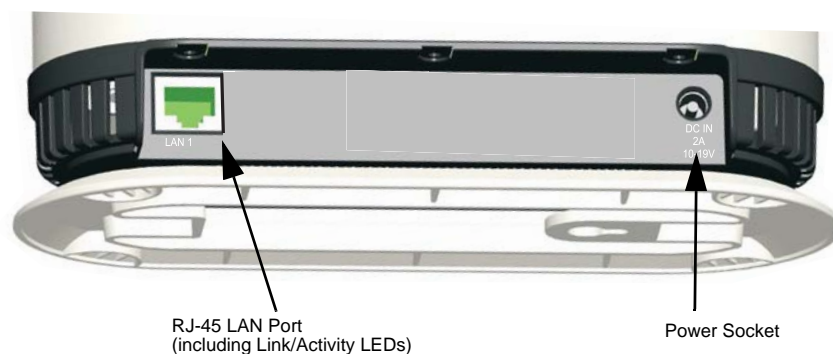


Figure 2-5: 1 Data/2 VoIP Port Model

- 4M-CPE-Si-1D-2.3-Omni;
- 4M-CPE-Si-1D-2.5-Omni;
- 4M-CPE-Si-1D-3.5-Omni:



**Figure 2-6: 1 Data Port Model**

### 2.3.1 Scan Button

This button initiates a scan of predefined frequency channels.

### 2.3.2 Reset Button

This button is used to reset the BreezeMAX Si 2000 or restore the factory default configuration. If you press the button for less than 1 second, the unit will perform a hardware reset. If you press and hold down the button for 5 seconds or more, any configuration changes you may have made are removed, and the factory default configuration is restored to the unit.

### 2.3.3 WiMAX Antennas

Two omnidirectional antennas are included with the BreezeMAX Si 2000 for WiMAX communications. The omnidirectional antennas transmit and receive signals in all directions equally.

### 2.3.4 WiMAX External Antenna Connectors

Two connectors are available on the top of the unit for attaching optional external antennas. Depending on a user's location, the use of an external antenna can

provide a better connection to a WiMAX base station. External antennas also offer various possible mounting locations.

## 2.3.5 LED Indicators

The figure below shows the BreezeMAX Si 2000's LED status indicators. Each LED is described in the sections that follow.

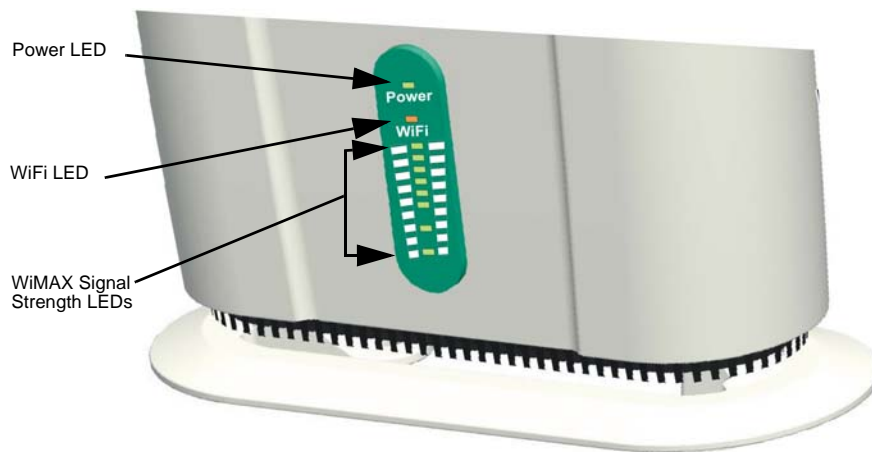


Figure 2-7: LEDs

### 2.3.5.1 Power Status Indicator LED

The BreezeMAX Si 2000 includes a Power LED indicator that simplifies installation and WiMAX network troubleshooting. The LED, which is located on the front panel, is described in the following table.

**Table 2-1: Power Status LEDs**

LED	Status	Description
Power	On Green	Power is supplied to the unit.
	Flashing Green	When flashing with three of the WiMAX signal LEDs turned on, indicates authentication has failed.
	On Orange	Indicates one of the following conditions: <ul style="list-style-type: none"> <li>■ After power on, indicates the unit is running its self test.</li> <li>■ Indicates the network entry process has restarted.</li> </ul>
	On Red	A system failure has occurred.
	Off	No power is being supplied to the unit.

### 2.3.5.2 Wi-Fi Status Indicator LED

The 3.5 GHz BreezeMAX Si 2000 model, which supports Wi-Fi operation, includes a Wi-Fi LED indicator that displays the Wi-Fi network status. The LED, which is located on the front panel, is described in the following table:

**Table 2-2: Wi-Fi Status Indicator LED**

LED	Status	Description
WiFi	On Green	The Wi-Fi radio is enabled and operating normally.
	Flashing Green	Indicates data traffic in the Wi-Fi network.
	Off	There is no Wi-Fi connection or the radio is disabled.

### 2.3.5.3 WiMAX Signal Indicator LEDs

The BreezeMAX Si 2000 includes seven WiMAX signal strength LED indicators that display the current WiMAX receive signal status. The LEDs, which are located on the front panel, are described in the following table.

**Table 2-3: WiMAX Signal Indicator LEDs**

LED	Status	Description
1	On Green	Indicates the receive signal is between 5 dB and 8 dB.
2	On Green	Indicates the receive signal is between 8 dB and 12 dB.
3	On Green	Indicates the receive signal is between 12 dB and 15 dB.
4	On Green	Indicates the receive signal is between 15 dB and 18dB.
5	On Green	Indicates the receive signal is between 18 dB and 20 dB.
6	On Green	Indicates the receive signal is between 20 dB and 25 dB.
7	On Green	Indicates the receive signal is 25 dB or more.
All 7 LEDs	Off	No power is being supplied to the unit.

### 2.3.6 10BASE-T/100BASE-TX LAN Ports

The BreezeMAX Si 2000 provides a maximum of four 10BASE-T/100BASE-TX RJ-45 ports. These LAN ports are standard RJ-45 Ethernet network ports that connect directly to PCs. They can also be connected to an Ethernet switch or hub to support more users and provide a data link to the local network.

The unit appears as an Ethernet node and performs a wireless bridging function by moving packets from the wired LAN to the remote BreezeMAX Si 2000.

All ports support automatic MDI/MDI-X operation, so you can use straight-through cables for all network connections to PCs or servers, or to other switches or hubs. Each of these ports support auto-negotiation, so the optimum transmission mode (half or full duplex), and data rate (10 or 100 Mbps) is selected automatically.

Each RJ-45 port includes a built-in LED indicator. This LED indicator is described in the following table.

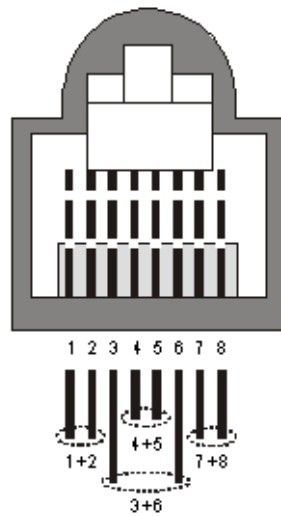
**Table 2-4: LAN Port LEDs**

LED	Status	Description
Link/Activity	On Green	Ethernet port has a valid link with an attached device.
	Flashing Green	The port is transmitting or receiving data.
	Off	Ethernet port has no link with another device.

### 2.3.7 10/100BASE-TX Pin Assignments

The BreezeMAX Si 2000 cable provides pin-to-pin connection on both ends.

The following figure shows the required wire pair connections.



**Figure 2-8: Ethernet Pin Assignments and Wire Pairs**

The color codes used in standard cables supplied by Alvarion are as listed in the following table:

**Table 2-5: Cable Color Codes**

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

**Table 2-6: 10/100BASE-TX MDI and MDI-X Port Pinouts**

PIN	MDI-X Signal Name	MDI Signal Name
1	Receive Data plus (RD+)	Transmit Data plus (TD+)
2	Receive Data minus (RD-)	Transmit Data minus (TD-)
3	Transmit Data plus (TD+)	Receive Data plus (RD+)
6	Transmit Data minus (TD-)	Receive Data minus (RD-)



**Table 2-6: 10/100BASE-TX MDI and MDI-X Port Pinouts**

PIN	MDI-X Signal Name	MDI Signal Name
4,5,7,8	Not used	Not used
<b>Note:</b> The "+" and "-" signs represent the polarity of the wires that make up each wire pair.		

## 2.3.8 BreezeMAX Si 2000 Cables



### NOTE

The length of the Ethernet cable connecting the BreezeMAX Si 2000 to the data equipment, should not exceed 100 meters.

Use only Category 5E Ethernet cables from either Alvarion or any of the approved manufacturers, listed in [Table 2-7](#). Consult with Alvarion's specialists on the suitability of other cables.

**Table 2-7: 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
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 GroupTel/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.

## 2.3.9 VoIP Phone Ports

The BreezeMAX Si 2000 provides a maximum of two RJ-11 telephone ports that connect directly to a standard (analog) telephone set. This allows a regular telephone to be used for making VoIP calls over the Internet.

## 2.3.10 Power Adapter Socket

The power socket is located on the rear panel of the BreezeMAX Si 2000. The power socket is for the AC power adapter connection.

The unit is powered on when connected to its AC power adapter, and the power adapter is connected to an AC power source between 100-240 volts at 50-60Hz.

## 2.3.11 SIM Card Slot

### NOTE



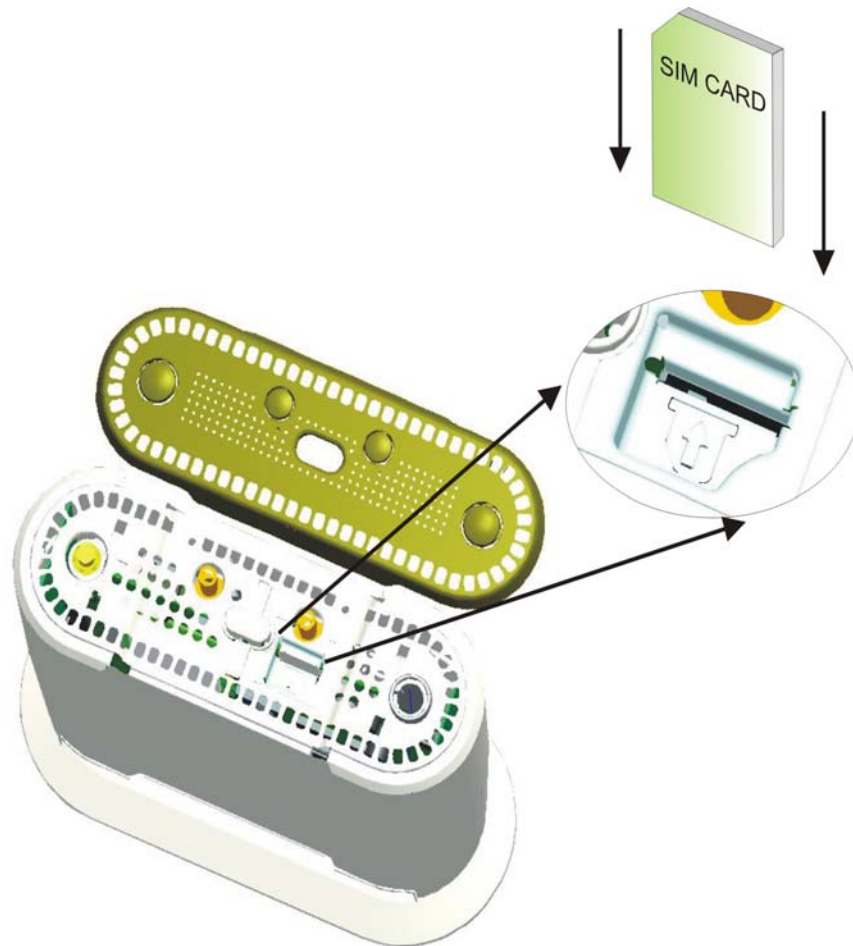
The SIM Card Slot is not supported in the current release.

The BreezeMAX Si 2000 also includes a standard SIM card slot that can be accessed by removing the unit's top cover.

Some WiMAX service providers may require an optional SIM Card to be installed in the BreezeMAX Si 2000 unit. The SIM card can include all required

configuration details, including security set up, operator information, and other end-user specific parameters.

The following figure shows the location of the SIM card slot under the top cover.

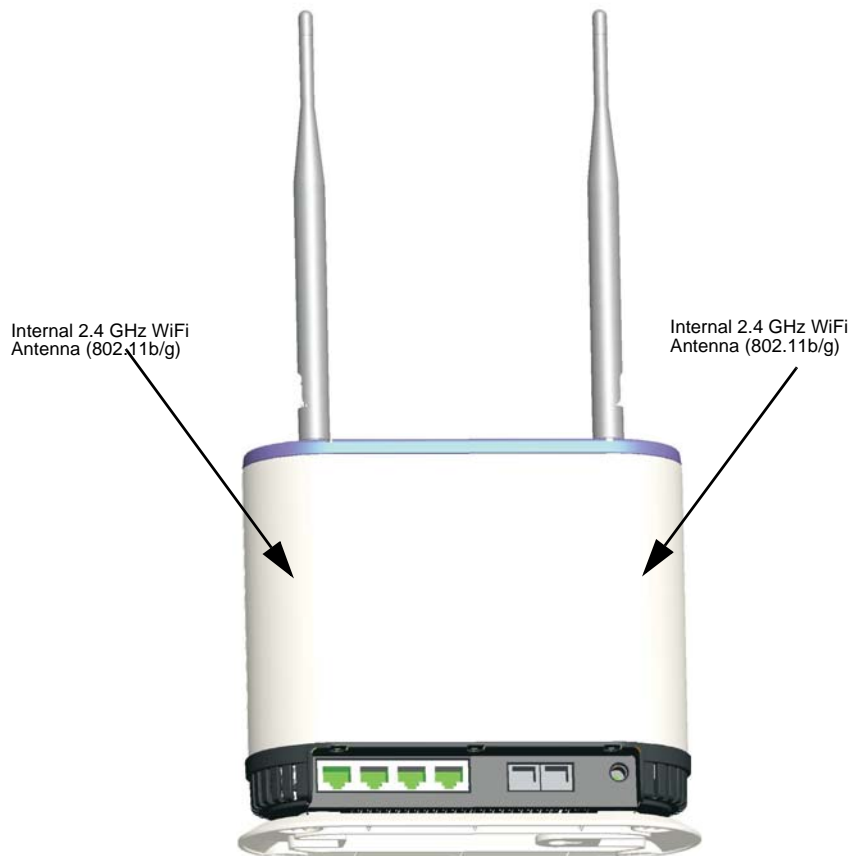


**Figure 2-9: SIM Card Slot**

### 2.3.12 BreezeMAX Si 2000 Wi-Fi Option

The BreezeMAX Si 2000 3.5 GHz model includes the 802.11b/g Wi-Fi option. This unit includes internal antennas for local wireless connections to PCs.

The following figure shows the 3.5 GHz BreezeMAX Si 2000 and the location of the internal Wi-Fi support.



**Figure 2-10: WiFi Option**

### 2.3.13 Cable Connections

The BreezeMAX Si 2000 is a plug-and-play device, so once it has been connected to your PC and powered up, it is fully operable.

Functioning as a gateway, the unit routes traffic between a WiMAX network and PCs or notebooks in the local network.

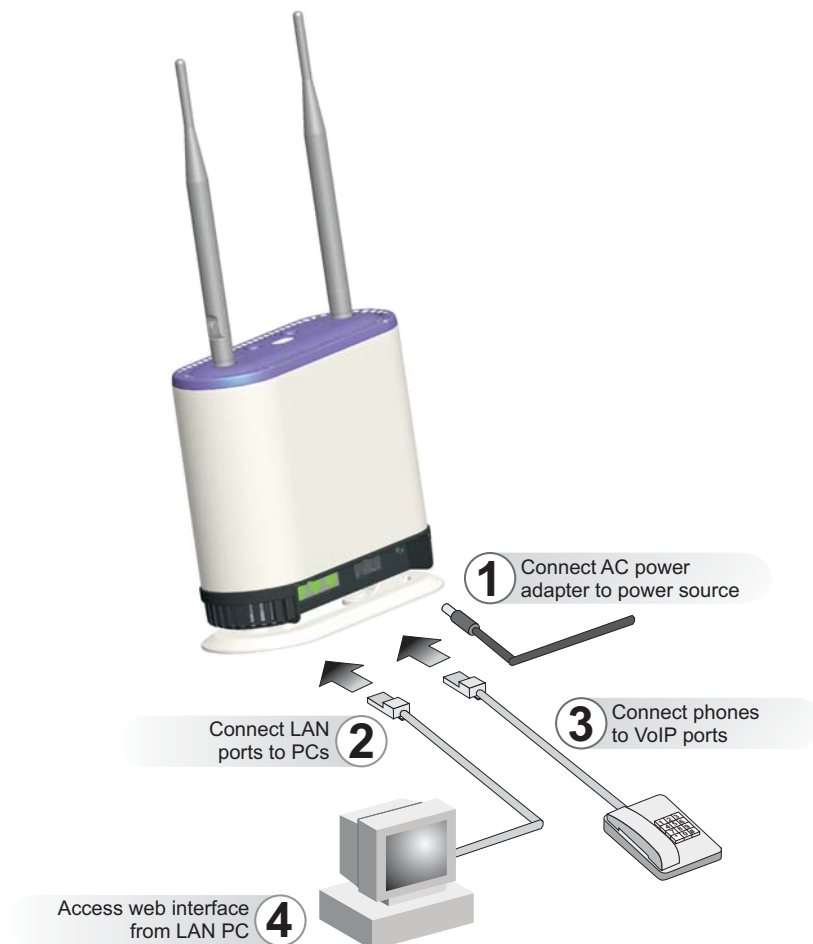


Figure 2-11: Cable Connections



#### To connect the BreezeMAX Si 2000:

- 1** Power on the BreezeMAX Si 2000 by connecting the AC power adapter and plugging it into an AC power source.



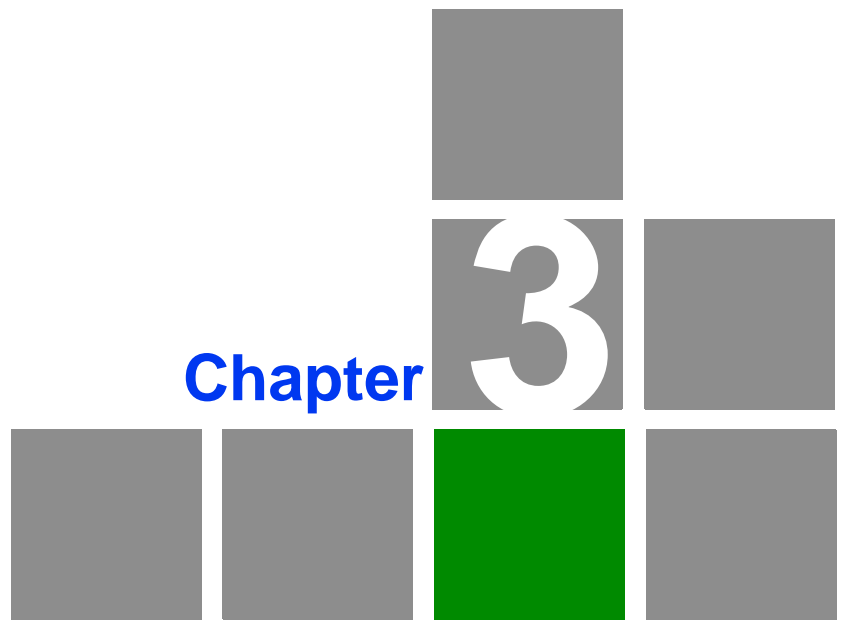
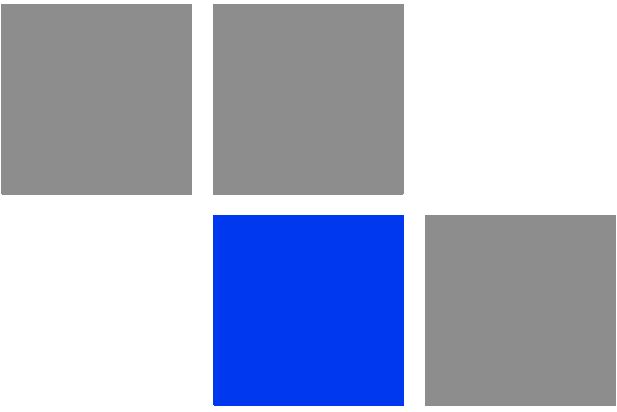
#### CAUTION

Use **ONLY** the power adapter supplied with the BreezeMAX Si 2000. Otherwise, the product may be damaged.

- 2 Observe the Indicator LEDs. When you power on the BreezeMAX Si 2000, verify that the Power LED turns on and that the other LED indicators start functioning as described under [“LED Indicators” on page 20](#).
- 3 Connect Category 5 or better Ethernet cables from the BreezeMAX Si 2000’s LAN ports to the network ports of your PCs. Alternatively, you can connect the LAN ports to an Ethernet switch or other devices. Make sure the length of each cable does not exceed 100 meters (328 ft).
- 4 If your PCs are powered on, the RJ-45 LAN port LEDs on the BreezeMAX Si 2000 should turn on to indicate valid links.
- 5 Connect one or two standard (analog) telephone sets to the BreezeMAX Si 2000’s VoIP ports using standard telephone cable with RJ-11 plugs. The BreezeMAX Si 2000 enables VoIP calls to be made through the unit using a standard (analog) telephone set connected to a VoIP port, or from PCs or other network devices connected to the LAN ports. 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.
- 6 Use your PC’s web browser to access the unit’s management interface and run the Setup Wizard to make any configuration changes. For more information, see [“Initial Configuration” on page 30](#).

**NOTE**

If you use an optional external WiMAX antenna with the unit, be sure to access the web management interface and configure the BreezeMAX Si 2000 to use the correct antenna. See “Antenna Setting” on page 6-4 for more information.



**Initial Configuration**

## In This Chapter:

- [“Introduction” on page 32](#)
- [“The Advanced Setup Menu” on page 36](#)



## 3.1 Introduction

The BreezeMAX Si 2000 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).

The web interface provides the options of Basic Setup or Advanced Setup.

The initial configuration steps can be made through the web-browser interface using the default IP address.

### 3.1.1 Accessing the Web Management Interface

The BreezeMAX Si 2000 has the default IP address of 192.168.1.1 and the subnet mask 255.255.255.0. If your PC is set to have an IP address assigned by DHCP (Dynamic Host Configuration Protocol), you can connect immediately to the web management interface. Otherwise, you must first check if your PC's IP address is set on the same subnet as the BreezeMAX Si 2000 (that is, the PC's IP address starts 192.168.1.x).

In the web browser's address bar, type the default IP address: `http://192.168.1.1`.

The web browser displays the BreezeMAX Si's login page.



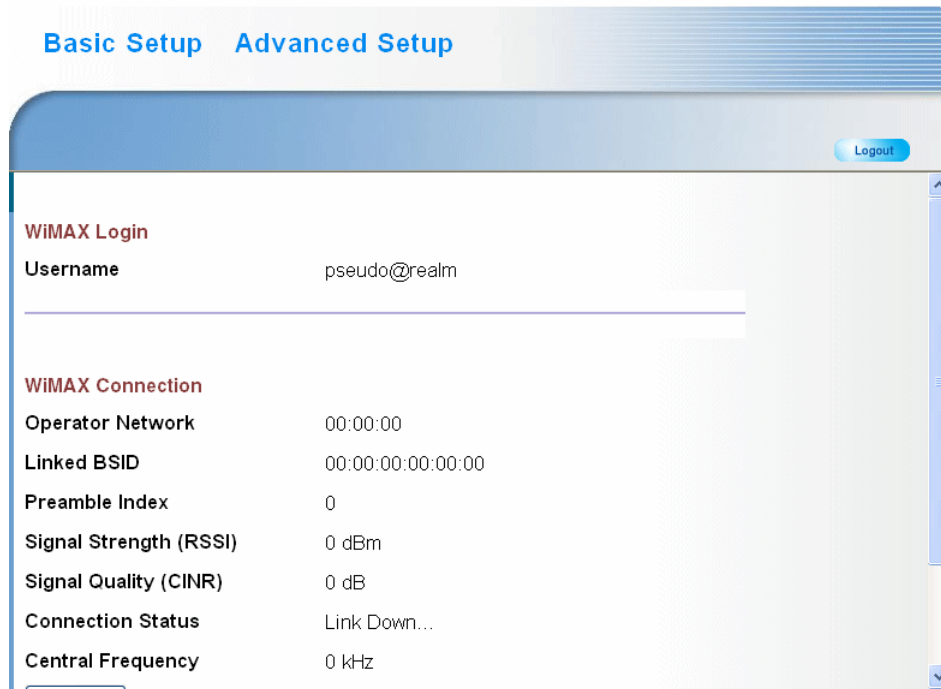
**Figure 3-1: Login Window**

To log in, enter the user name and password, and click Login. For Admin mode, the default user name is **admin** and the default password is **admin**. The home page displays.

For Operator mode, the default user name is **Operator** and the default password is **oper1234**. In Operator mode, additional parameters are available for more detailed configuration.

**NOTE**

Admin user credentials are intended for the end user.



**Figure 3-2: Main Window**

To configure basic settings for the current operating mode, click Basic Setup. For more information, see [“Using the Basic Setup” on page 33](#) (below).

Alternatively, to configure more detailed settings, click Advanced Setup. For more information, see [“The Advanced Setup Menu” on page 36](#).

**NOTE**

It is strongly recommended that you configure your own password. If a password is not configured, the management interface is not protected and anyone who can connect to the BreezeMAX Si 2000 may be able to compromise your network security.

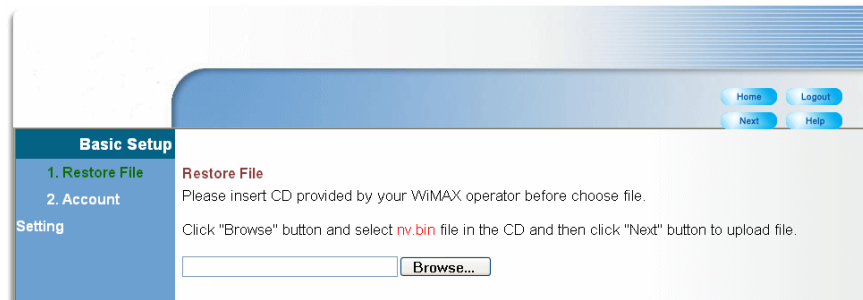
### 3.1.2 Using the Basic Setup

The Basic Setup allows you to run the BreezeMAX Si 2000 with minimal configuration requirements.

**Launching the Basic Setup** – To perform basic configuration, click Basic Setup on the home page.

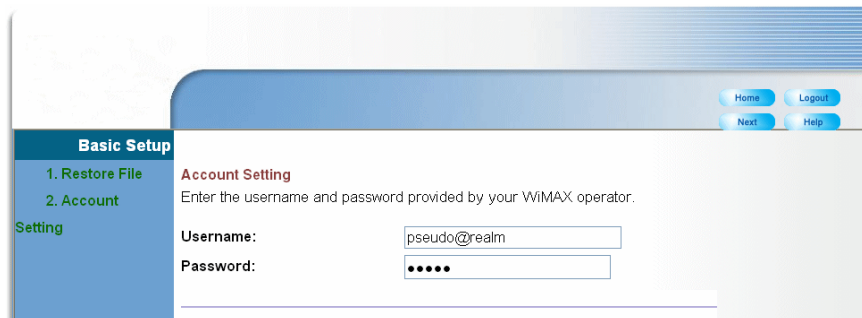
When configuring the unit through the Basic Setup, proceed through the following steps:

- 1 For first-time setup, place the CD supplied by your WiMAX operator in the CD drive of the PC. Navigate to the CD's location using the "Browse" button.
- 2 Click Next; this enables the Basic Setup to copy the WiMAX operator's settings to the gateway.



**Figure 3-3: Basic Setup - CD Directory**

- 3 **WiMAX Login** – The Account Setting page sets the user name and password required to gain access to the WiMAX network.



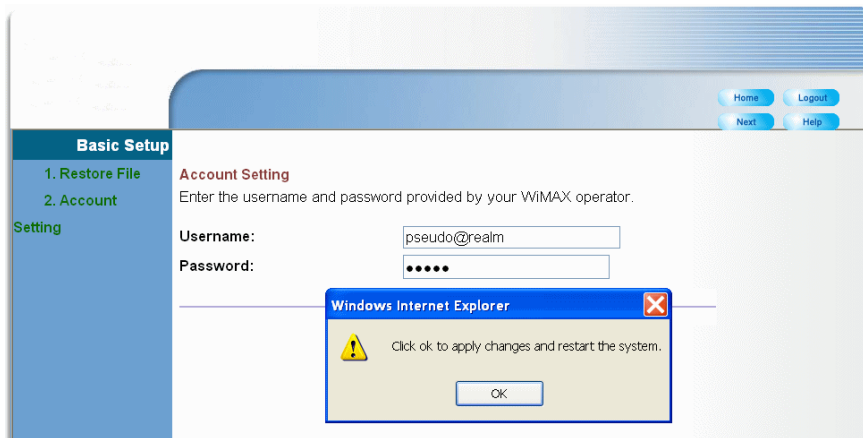
**Figure 3-4: Basic Setup - WiMAX Login**

**Username** – The user name required for network authentication, as supplied by the WiMAX service provider. (Default: pseudo@realm)

**Password** – The user password required for network authentication, as supplied by the WiMAX service operator. (Range: 1-32 characters; Default: hello)

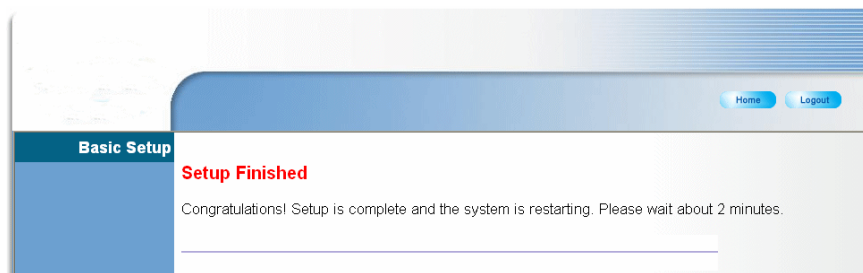
- 4 **Apply Settings** – When you click "Apply" the settings on the operator-supplied CD are copied to the gateway, then the unit reboots and attempts to connect to the specified WiMAX network.

The unit will prompt for confirmation of the Username and Password, click “OK.”



**Figure 3-5: Basic Setup- Apply Changes**

- 5 The system will inform you when the configuration changes have taken effect and will perform a two minute reboot.



**Figure 3-6: Basic Setup - Setup Complete**

- 6 After waiting approximately two minutes, you must type the IP address of the unit (192.168.1.1) into your web browser to re-access the management interface.

## 3.2 The Advanced Setup Menu

The Advanced Setup menu provides access to all the configuration settings available for the BreezeMAX Si 2000. The advanced setup menu is available both for operator and admin user credentials. Some of the menus are not available to the admin user. The menus for both users are described.

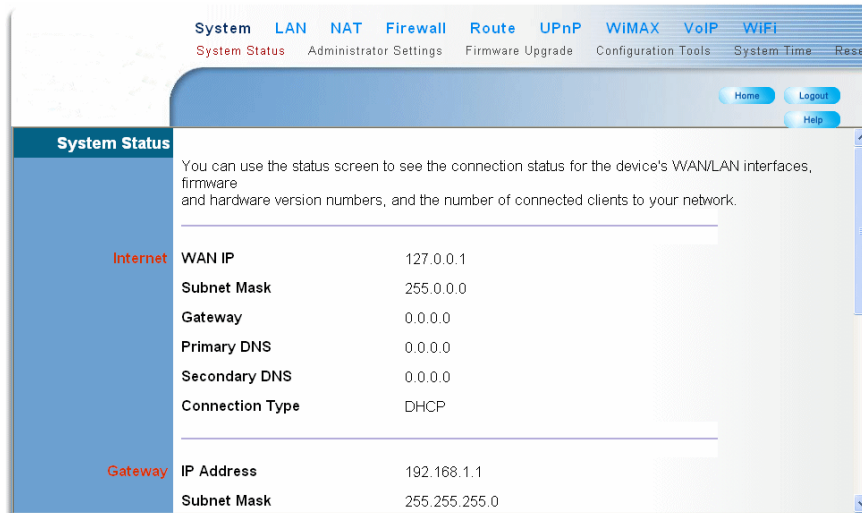


Figure 3-7: Advanced Setup Home Page – Admin Mode

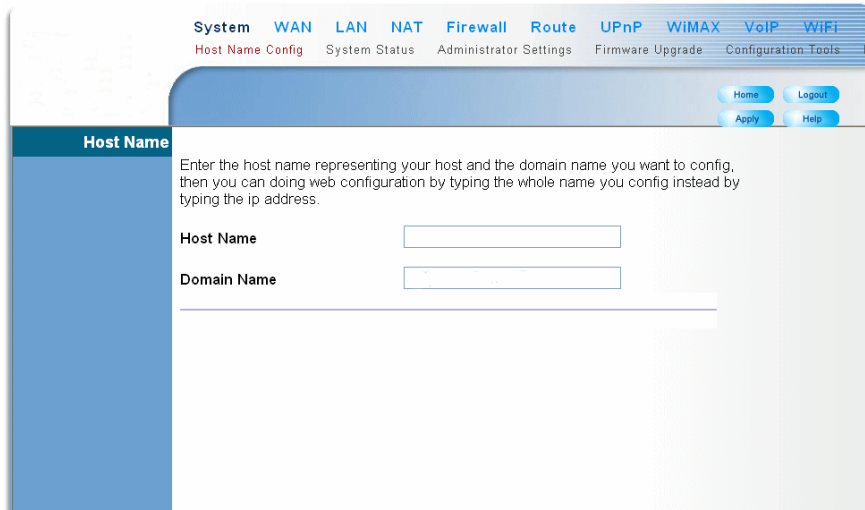
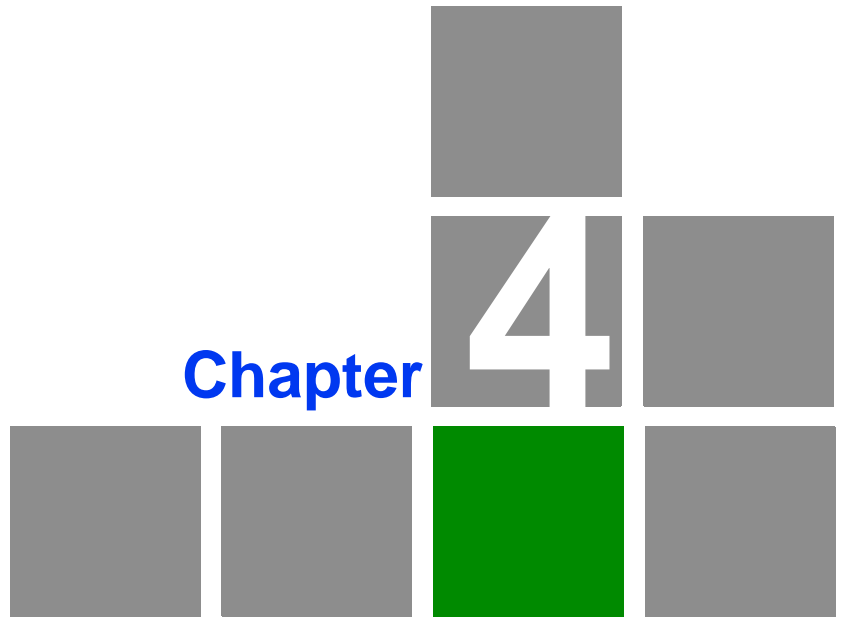
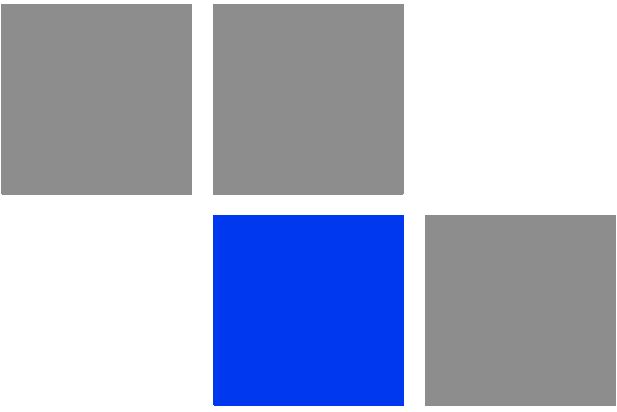


Figure 3-8: Advanced Setup Home Page – Operator Mode

Each primary menu item is summarized below with links to the relevant section in this guide where configuration parameters are described in detail:

- System – Configures general device settings, see [“System Settings” on page 38](#).
- WAN – Configures WAN settings, see [“WAN Settings” on page 59](#). (WAN settings are only available in Operator mode.)
- LAN – Configures LAN settings, see [“LAN” on page 63](#).
- NAT – Configures Network Address Translation settings, see [“NAT” on page 66](#).
- Firewall – Configures firewall settings, see [“Firewall” on page 69](#).
- Route – Displays static routing settings, see [“Route” on page 72](#).
- UPnP – Enables UPnP, see [“UPnP” on page 73](#).
- WiMAX – Configures the wireless connection status, see [“WiMAX Settings” on page 74](#).
- VoIP – Configures VoIP SIP settings, see [“VoIP Settings” on page 84](#).
- WiFi – Configures 802.11 access point settings, see [“WiFi Settings” on page 100](#).



Chapter

4

System Settings

## In This Chapter:

- “Introduction” on page 40
- “Host Name” on page 41
- “System Status” on page 42
- “Administrator Settings” on page 44
- “Firmware Upgrade” on page 45
- “Configuration Tools” on page 46
- “System Time” on page 48
- “TR069 Settings” on page 50
- “System Log” on page 52
- “Reset” on page 53



## 4.1 Introduction

The BreezeMAX Si 2000's System menu allows you to perform general management functions for the unit, including setting the system time, configuring an access password, and upgrading the system software.

Through an easy to use web management interface the BreezeMAX Si 2000 can be configured to be a powerful wireless connection to any telecommunications network.



### NOTE

You can use the web browser interface to access the WAN IP address only if the BreezeMAX Si 2000 already has an IP address that is reachable through your network.

The default IP address of the BreezeMAX Si 2000 is 192.168.1.1. The CPE operates by default in DHCP mode.

## 4.2 Host Name

The gateway allows you to define a name that identifies your unit and the domain name used by the local network. Setting a host name enables the web interface to be accessed using an easy-to-remember name instead of its IP address.



### NOTE

The Host Name settings are only available in Operator mode

**Host Name**

Enter the host name representing your host and the domain name you want to config, then you can doing web configuration by typing the whole name you config instead by typing the ip address.

Host Name

Domain Name

**Figure 4-1: System Host Name**

- Host Name – Enter the name chosen for the unit. (Default: cpe)
- Domain Name – Enter the domain to which the unit is connected.

## 4.3 System Status

The system status page displays connectivity status information for the unit's WiMAX (WAN) and LAN interfaces, firmware and hardware version numbers, and the number of clients connected to your network.

<b>INTERNET</b>	<b>WAN IP</b>	127.0.0.1
	<b>Subnet Mask</b>	255.255.255.0
	<b>Gateway</b>	0.0.0.0
	<b>Primary DNS</b>	0.0.0.0
	<b>Secondary DNS</b>	0.0.0.0
	<b>Connection Type</b>	DHCP

**Figure 4-2: System Status**

**INTERNET** – Displays WAN (WiMAX) connection status:

- **WAN IP** – Displays the IP address assigned by the service provider.
- **Subnet Mask** – Displays the WAN subnet mask assigned by the service provider.
- **Gateway** – Displays the WAN gateway address assigned by the service provider.
- **Primary DNS** – Displays the WAN primary DNS address.
- **Secondary DNS** – Displays the WAN secondary DNS address.
- **Connection Type** – Displays the connection type for the WAN. Either FIXED for a static IP setting, or DHCP for dynamic IP assignment.

<b>GATEWAY</b>	<b>IP Address</b>	192.168.1.1
	<b>Subnet Mask</b>	255.255.255.0
	<b>DHCP Server</b>	Enable
	<b>Firewall</b>	Disable

**Figure 4-3: System Status Gateway**

**GATEWAY** – Display system IP settings, as well as DHCP, NAT and firewall status:

- **IP Address** – Displays the unit’s IP address.
- **Subnet Mask** – Displays the subnet mask.
- **DHCP Server** – Displays the DHCP server status.
- **Firewall** – Displays the firewall status.

VoIP STATUS	Phone 1 Status	Registration request timed out
	Phone 2 Status	Registration request timed out

**Figure 4-4: System Status VoIP Status**

**VoIP STATUS** - Displays the status of the connection of each of the phone lines.

- **Phone 1 Status** – Displays the SIP status of phone line 1.
- **Phone 2 Status** – Displays the SIP status of phone line 2.

Information	Connected Clients	0
	Runtime Code Version	1.0.0.12
	LAN MAC Address	08:01:11:11:11:11
	LAN MTU Size	1500
	WAN MAC Address	00:12:CF:7C:32:AF
	WAN MTU Size	1400

**Figure 4-5: System Status Information**

**INFORMATION** – Displays the number of connected clients, as well as the unit’s LAN and WAN MAC addresses:

- **Connected Clients** – Displays the number of connected clients, if any.
- **Runtime Code Version** – Displays the runtime code version.
- **LAN MAC Address** – Displays the LAN MAC address.
- **LAN MTU Size** – Sets the LAN maximum transmission unit size in bytes.
- **WAN MAC Address** – Displays WAN MAC address.
- **WAN MTU Size** – Sets the WAN maximum transmission unit size in bytes.

## 4.4 Administrator Settings

The Administrator Settings page enables you to change the default password for management access to the BreezeMAX Si 2000.

Set a password to restrict management access to the device.

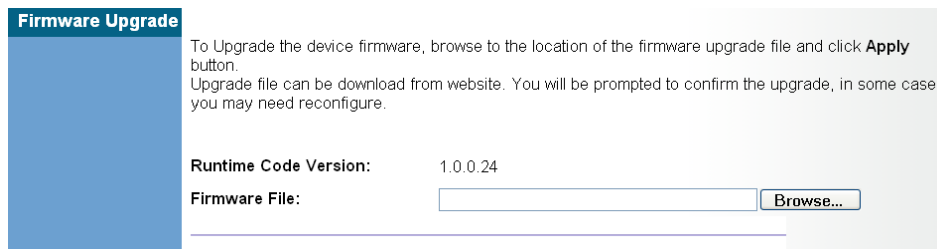
Current Password	<input type="text"/>
New Password	<input type="text"/>
Confirm New Password	<input type="text"/> (3-12 Characters)
Auto-Logout Time	<input type="text" value="30"/> Min (Auto-Logout Time, at least >= 1 Min)

**Figure 4-6: Setting a Password**

- **Current Password** – You need to first enter your current administrator password to be able to configure a new one. (Admin Mode Default: admin; Operator Mode Default: oper1234)
- **New Password** – Enter a new administrator password. (Range: 3~12 characters)
- **Confirm New Password** – Enter the new password again for verification. (Range: 3~12 characters)
- **Auto-Logout Time** – The time of inactivity after which the unit terminates a web management session. (Default: 30 minutes; Range: 1~99 minutes)

## 4.5 Firmware Upgrade

The Firmware Upgrade page enables you to download new software to the unit. By clicking the “Browse” button you can navigate to the directory on your PC or network where the firmware is kept.



**Firmware Upgrade**

To Upgrade the device firmware, browse to the location of the firmware upgrade file and click **Apply** button.  
Upgrade file can be download from website. You will be prompted to confirm the upgrade, in some case, you may need reconfigure.

Runtime Code Version: 1.0.0.24

Firmware File:

**Figure 4-7: Firmware Upgrade**

- **Firmware Update** – Downloads an operation code file from the web management station to the BreezeMAX Si 2000 using HTTP. Use the Browse button to locate the code file locally on the management station and click Apply to proceed.

## 4.6 Configuration Tools

The Configurations Tools page allows you to restore factory default settings, or save and restore the unit's configuration settings to or from a file on the management station.



### NOTE

The Backup Settings/Restore Settings option is not available in Admin mode.

Use the "Backup Settings" tool to save the device's current configuration to a file named "nv.bin" on your PC. You can then use the "Restore Settings" tool to restore the saved configuration of the device. Alternately, you can use the "Restore to Factory Defaults" tool to force the device to perform reset and restore the original factory settings.

- Restore Factory Default Configuration
- Backup Settings / Restore settings

**Figure 4-8: Configuration Tools**

- **Restore Factory Default Configuration** – Resets the unit to its factory default settings.
- **Backup Settings/Restore Settings** – When selected, prompts either to backup the current configuration to a file, or select a previously backed up file to restore to the unit.

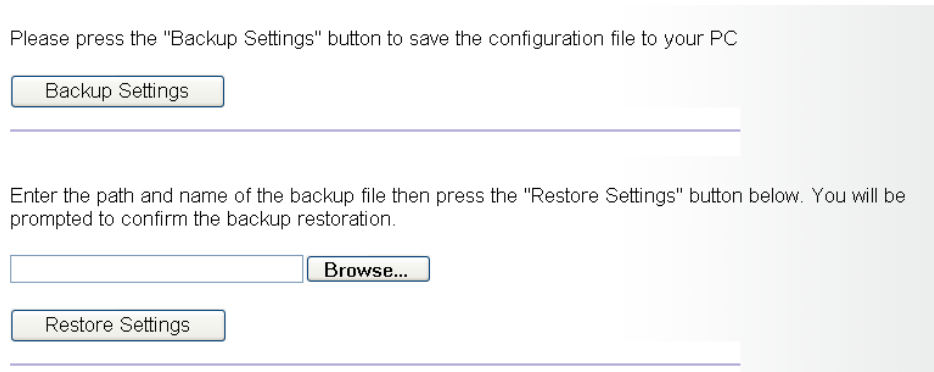
When you select “Restore Factory Default Configuration” and click Apply, a confirmation message displays. Click the Restore button to continue.

To restore the factory default settings of the Router, click on the "Restore" button. You will be asked to confirm your decision.

Restore...

**Figure 4-9: Restoring the Factory Default Configuration**

When you select “Backup Settings/Restore Settings” and click Apply, the following page displays.



Please press the "Backup Settings" button to save the configuration file to your PC

---

Enter the path and name of the backup file then press the "Restore Settings" button below. You will be prompted to confirm the backup restoration.

**Figure 4-10: Backup/Restore Settings**

- **Backup Settings** – Saves the current configuration settings to a file named “nv.bin” on the web management station.
- **Restore Settings** – Restores a saved configuration file to the unit. You can use the Browse button to locate the file on the web management station.



## 4.7 System Time

The BreezeMAX Si 2000 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.

SNTP uses Greenwich Mean Time, or GMT (sometimes known as UTC) based on the time at the Earth's prime meridian, zero degrees longitude. To display a time corresponding to your local time, you must select your time zone, for example GMT-06.00, for Central Time (US and Canada.)

**Figure 4-11: Setting the System Time**

- **Time Protocol** – Select SNTP to enable the unit to set its internal clock based on periodic updates from a time server. The unit acts as an SNTP client, periodically sending time synchronization requests to a specified time server. Alternatively, you can select “None” and set the time and date manually. (Default: SNTP)
- **Time Server Address** – The IP address of a time server that the unit attempts to poll for a time update. (Default: 192.43.244.18)
- **Current Time (hh:mm:ss)** – Displays the current time of the system clock.
- **New Time (hh:mm:ss)** – Sets the system clock to the time specified. The time can only be set manually when the Time Protocol is set to “None.”
- **Current Date (yyyy:mm:dd)** – Displays the current date of the system clock.

- **New Date (yyyy:mm:dd)** – Sets the system clock to the date specified. The date can only be set manually when the Time Protocol is set to “None.”
  
- **Set Time Zone** – SNTP uses Greenwich Mean Time (GMT) based on the time at the Earth’s prime meridian, zero degrees longitude. To display a time corresponding to your local time, you must select your time zone from the pull-down list. (Default: (GMT+08:00) Taipei)

## 4.8 TR069 Settings

The Technical Report 069 (TR069) protocol defines a specification for remote management of CPE devices. The protocol uses HTTP for two-way communication between the CPE device and an Auto Configuration Server (ACS), allowing service providers to provide CPE configuration, software upgrades, and other service functions for end-users.

The TR069 Settings page allows you to set up the basic TR069 connection parameters.



### NOTE

The TR069 Settings page is only available in Operator mode.

TR069 Settings	
Enable Periodic Report	<input checked="" type="checkbox"/> Enable
Periodic Report Interval	<input type="text" value="86400"/> Seconds
User Name	<input type="text" value="admin"/>
Password	<input type="password" value="....."/>
Connection Request URL	<input type="text"/>
Connection Request User	<input type="text" value="orcadmin"/>
Name	<input type="text"/>
Connection Request Password	<input type="password" value="....."/>
ACS URL	<input type="text" value="8.24.50.197"/>

Figure 4-12: TR069 Settings

- **Enable Periodic Report** – Enables the sending of TR069 reports from the CPE to the ACS server. (Default: Enabled)
- **Periodic Report Interval** – Sets the time interval for sending TR069 reports to the ACS server. (Range: 0-65535 seconds; Default: 86400 seconds)
- **User Name** – The CPE user name required for authentication during session set up with the ACS server. (Default: admin)
- **Password** – The CPE password required for authentication during session set up with the ACS server. (Default: admin)

- **Connection Request URL** – Specifies the URL required for an ACS server to connect to the CPE.
- **Connection Request User Name** – The user name required for an ACS server to make a connection request to the CPE.
- **Connection Request Password** – The password required for an ACS server to make a connection request to the CPE.
- **ACS URL** – Specifies the URL required for the CPE to connect to the ACS server.

## 4.9 System Log

The System Log page allows you to display system event messages. The logged messages can serve as a valuable tool for isolating device and network problems, and also indicate if any unauthorized attempts have been made to gain access to your network.



### NOTE

The System Log page is only available in Operator mode.

System log messages according to syslog level.

The screenshot shows a web interface for viewing system logs. At the top, there is a green header labeled 'Log File'. Below it is a scrollable area containing the following log entries:

```

Jan 1 00:00:04 (none) kern.info kernel: Dentry cache hash table entries: 4096 (order: 3,
Jan 1 00:00:04 (none) kern.info kernel: Inode cache hash table entries: 2048 (order: 2, 1
Jan 1 00:00:04 (none) kern.info kernel: Mount cache hash table entries: 512 (order: 0, 40
Jan 1 00:00:04 (none) kern.info kernel: Buffer cache hash table entries: 1024 (order: 0,
Jan 1 00:00:04 (none) kern.warn kernel: Page-cache hash table entries: 8192 (order: 3, 32
Jan 1 00:00:04 (none) kern.warn kernel: Checking for 'wait' instruction... unavailable.
Jan 1 00:00:04 (none) kern.warn kernel: POSIX conformance testing by UNIFIX
Jan 1 00:00:04 (none) kern.warn kernel: PCI: Probing PCI hardware on host bus 0.
Jan 1 00:00:04 (none) kern.warn kernel: Autoconfig PCI channel 0x8023cd10
Jan 1 00:00:04 (none) kern.warn kernel: Scanning bus 00, I/O 0x1ae00000:0x1b000001, Mem 0
Jan 1 00:00:04 (none) kern.warn kernel: 00:0e.0 Class 0200: 168c:001a (rev 01)
Jan 1 00:00:04 (none) kern.warn kernel: Mem at 0x18000000 [size=0x10000]
Jan 1 00:00:04 (none) kern.info kernel: Linux NET4.0 for Linux 2.4
Jan 1 00:00:04 (none) kern.info kernel: Based upon Swansea University Computer Society NE
Jan 1 00:00:04 (none) kern.warn kernel: Initializing RT netlink socket
Jan 1 00:00:04 (none) kern.info kernel: LSP Revision 2
Jan 1 00:00:04 (none) kern.warn kernel: Starting kswapd
  
```

Below the log entries, there are three buttons: 'Download', 'Clear', and 'Refresh'.

Figure 4-13: System Logs

- **Syslog Level** – Sets the minimum severity level for event logging. The system allows you to limit the messages that are logged by specifying a minimum severity level. Error message levels range from the most severe (Emergency) to least severe (Debug). The message levels that are logged include the specified minimum level up to the Emergency level. (Default: Info)
- **Download** – Downloads the current log file to the web management station.
- **Clear** – Deletes all entries in the current log file.
- **Refresh** – Updates the displayed log entries on the web page.



### NOTE

Log messages saved in the unit's memory are erased when the device is rebooted.

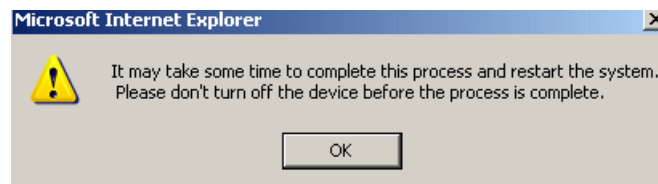
## 4.10 Reset

The Reset page allows you to restart the device's software.

In the event that the device stops responding correctly or in some way stops functioning, you can perform a reset. Your settings will not be changed. To perform the reset, click on the "Reset" button below. You will be asked to confirm your decision. The reset will be complete when the power light stops blinking.



**Figure 4-14: Reset Page**



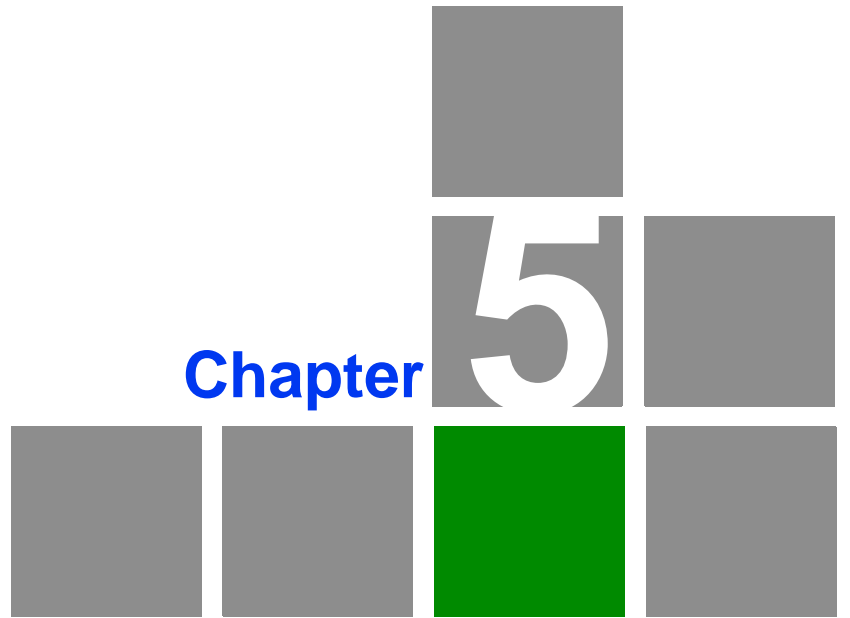
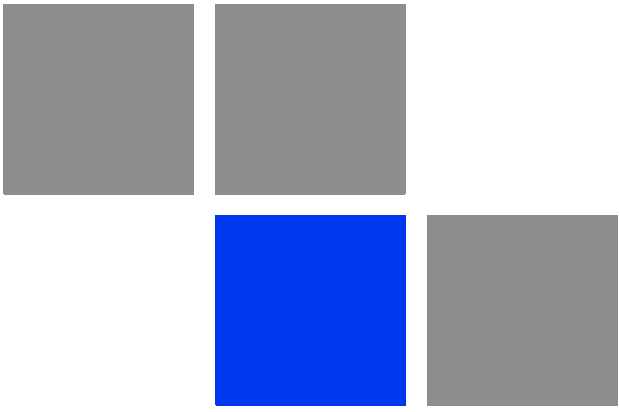
**Figure 4-15: Resetting the System**

- **Reset** – Resets the unit. All current settings are retained.



### NOTE

Resetting the system will cause you to lose your currently unsaved settings. After pressing "Reset" you will be prompted to give confirmation that you really want to reset.



# Gateway Configuration

## In This Chapter:

- [“Introduction” on page 56](#)
- [“Operation Mode” on page 57](#)
- [“WAN Settings” on page 59](#)
- [“LAN” on page 63](#)
- [“NAT” on page 66](#)
- [“Firewall” on page 69](#)
- [“Route” on page 72](#)
- [“UPnP” on page 73](#)



## 5.1 Introduction

The information in this chapter covers the configuration options for the BreezeMAX Si 2000's Internet gateway functions.

The BreezeMAX Si 2000 provides comprehensive firewall features and NAT isolation for Internet traffic passing from the WiMAX service provider to the local network connected to the LAN ports. The DHCP server feature can assign IP addresses for up to 32 local network PCs and wireless clients.

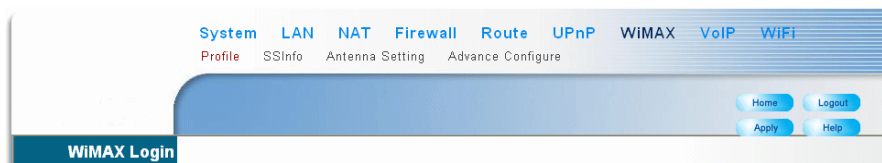


Figure 5-1: Gateway Settings Menu – Admin Mode

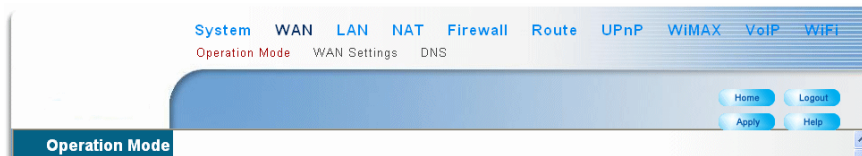


Figure 5-2: Gateway Settings Menu – Operator Mode

## 5.2 Operation Mode

Sets appropriate parameters for forwarding data between the service provider's WiMAX network and the local network.



### NOTE

The Operation Mode settings are only available in Operator mode

### 5.2.1 Operation Mode Settings

Specifies how various packets are forwarded to and from the WiMAX network to the local network.

**Figure 5-3: Operation Mode**

- **Operation Mode** – Specifies the mode for forwarding data packets from the WiMAX network to the local network. Packets transmitted in ETH CS (Ethernet conversion sublayer) mode contain an 802.3 header, packets transmitted in IP CS mode do not contain this header. Only IP CS is available in the current software release.
- **Data Transfer Mode** – Sets the forwarding mode for sending data packets to the WiMAX network. Bridge mode forwards packets based on Layer 2 MAC addresses. Router mode forwards packets based on Layer 3 IP addresses.
- **Management Transfer Mode** – Sets the forwarding mode for sending management packets to the WiMAX network. Bridge mode forwards packets based on Layer 2 MAC addresses. Router mode forwards packets based on Layer 3 IP addresses.
- **VoIP Transfer Mode** – Sets the forwarding mode for sending VoIP packets to the WiMAX network. Bridge mode forwards packets based on Layer 2 MAC addresses. Router mode forwards packets based on Layer 3 IP addresses.

## 5.2.2 Management Settings

Sets the Differentiated Services Code Point (DSCP) value used in management traffic between the BreezeMAX Si 2000 and the WiMAX network. The DSCP value in the IP header of data packets is used to give traffic priority treatment by network equipment.



**Figure 5-4: Operation Mode - Management Settings**

- **Factory Defaults DSCP Classifier** – The factory default Differentiated Services Code Point (DSCP) value is 6.
- **Configured DSCP Classifier** – The factory default Differentiated Services Code Point (DSCP) value is 6. The configurable DSCP range is 0 to 63. If there is no management connection to the BreezeMAX Si 2000, the DSCP classifier value will be changed by the system until a connection is successful.
- **Actual Used DSCP Classifier** – The DSCP classifier value used for successful management connection.
- **eCPE Manager Connection Status** – Displays the current status of the management connection; either Connected or Not Connected.

## 5.2.3 VoIP Settings

Enables the assignment of the SIP Proxy and Registrar Address by DHCP option 120.



**Figure 5-5: Operation Mode - VoIP Settings**

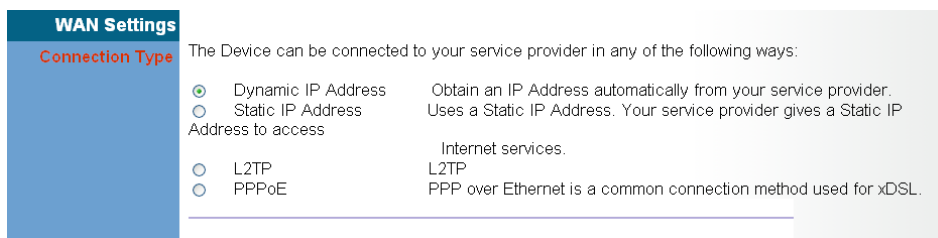
## 5.3 WAN Settings

Select the WAN connection type used by your service provider and specify DNS (Domain Name System) servers.



### NOTE

The WAN settings are only available in Operator mode



**Figure 5-6: WAN Settings**

The unit can be connected to your ISP in one of the following ways:

- **Dynamic IP Address** – Selects configuration for an Internet connection using DHCP for IP address assignment. This is the default setting.
- **Static IP Address** – Selects configuration for an Internet connection using a fixed IP assignment.



### NOTE

Static IP setting is not supported in the current software release.

- **L2TP** – Selects configuration for an Internet connection using the Layer 2 Tunneling Protocol, an access protocol often used for virtual private networks.
- **PPPoE** – Selects configuration for an Internet connection using the Point-to-Point Protocol over Ethernet (PPPoE), a common connection method used for DSL access.



### NOTE

For the Dynamic IP Address (DHCP) option, the unit requires no further configuration. Selecting other WAN types displays the parameters that are required for configuring the connection.

### 5.3.1 Dynamic IP Address

For dynamic IP assignment from the service provider, the unit functions as a Dynamic Host Configuration Protocol (DHCP) client. When enabled, no other settings are required.

**WAN Settings**  
**Connection Type**

The Device can be connected to your service provider in any of the following ways:

- Dynamic IP Address Obtain an IP Address automatically from your service provider.
- Static IP Address Uses a Static IP Address. Your service provider gives a Static IP Address to access Internet services.
- L2TP L2TP
- PPPoE PPP over Ethernet is a common connection method used for xDSL.

**Figure 5-7: Dynamic IP Address**

### 5.3.2 Static IP Settings

Selecting Static IP Address for the WAN type enables you to enter static IP settings as assigned by the service provider.



#### NOTE

Static IP setting is not supported in the current software release.

**Static IP Settings**

If your service provider has assigned a fixed IP Address, enter the assigned IP Address, Subnet Mask and ISP Gateway Address provided.

**IP Address assigned by your ISP**  
 1 . 1 . 1 . 10

**Subnet Mask**  
 255 . 255 . 255 . 0

**Gateway**  
 1 . 1 . 1 . 3

**Figure 5-8: Static IP Settings**

- **IP Address assigned by your ISP** – The IP address provided by your service provider. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods.
- **Subnet Mask** – Indicates the subnet mask, such as 255.255.255.0.
- **Gateway** – The gateway IP address provided by your service provider.

### 5.3.3 L2TP Settings

If your service provider supports Layer 2 Tunneling Protocol (L2TP) for your Internet connection, configure the settings described below.

**L2TP Settings** If your ISP provided you the L2TP Account, L2TP Password, Host Name, Service IP Address, IP Address, Subnet Mask and the Connection ID, then your ISP uses L2TP. You have to choose this option and enter the required information.

**User Name**  (Max length : 20 chars)

**Password**  (Max length : 20 chars)

**L2TP Network Server**  .  .  .

**Keep Alive:**

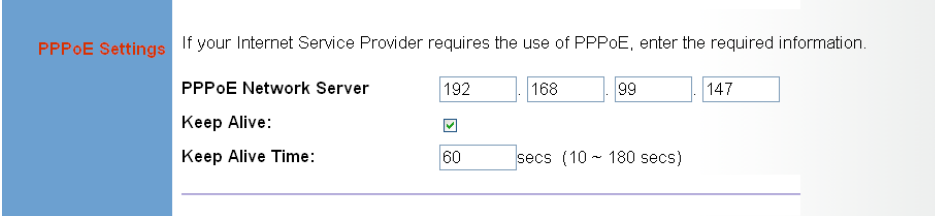
**Keep Alive Time:**  secs (10 ~ 180 secs)

**Figure 5-9: L2TP Settings**

- **User Name** – Enter your user name for connecting to the L2TP service, as supplied by the service provider. (Range: 1-20 characters; Default: *No name*)
- **Password** – Specify the password for your connection, as supplied by the service provider. (Range: 1-20 characters; Default: *No password*)
- **L2TP Network Server** – The IP address of the L2TP server, as specified by the service provider.
- **Keep Alive** – This option enables the unit to check periodically that the L2TP connection is still operating. If the connection is found to be lost, the unit automatically attempts to reconnect to the service provider. (Default: Enabled)
- **Keep Alive Time** – The time period the unit waits before checking that the L2TP connection is still operating. This parameter only applies when Keep Alive is enabled. (Default: 60 seconds; Range: 10-180 seconds)

## 5.3.4 PPPoE Settings

If your service provider supports Point-to-Point Protocol over Ethernet (PPPoE) for your Internet connection, configure the settings described below.



The screenshot shows a configuration window titled "PPPoE Settings". On the left, there is a blue vertical bar with the text "PPPoE Settings" in white. To the right of this bar, the text "If your Internet Service Provider requires the use of PPPoE, enter the required information." is displayed. Below this text, there are three configuration fields: "PPPoE Network Server" with four input boxes containing the values "192", "168", "99", and "147"; "Keep Alive:" with a checked checkbox; and "Keep Alive Time:" with an input box containing "60" followed by the text "secs (10 ~ 180 secs)".

**Figure 5-10: PPPoE Settings**

- **PPPoE Network Server** – The IP address of the PPPoE server, as specified by the service provider.
- **Keep Alive** – This option enables the unit to check periodically that the PPPoE connection is still operating. If the connection is found to be lost, the unit automatically attempts to reconnect to the service provider. (Default: Enabled)
- **Keep Alive Time** – The time period the unit waits before checking that the PPPoE connection is still operating. This parameter only applies when Keep Alive is enabled. (Default: 60 seconds; Range: 10-180 seconds)

## 5.4 LAN

The BreezeMAX Si 2000 must have a valid IP address for management using a web browser and to support other features. The unit has a default IP address of 192.168.1.1. You can use this IP address or assign another address that is compatible with your existing local network. The unit can also be enabled as a Dynamic Host Configuration Protocol (DHCP) server to allocate IP addresses to local PCs.

### 5.4.1 LAN Settings

The BreezeMAX Si 2000 includes a DHCP server that can assign temporary IP addresses to any attached host requesting the service. Addresses are assigned to clients from a common address pool configured on the unit. Configure an address pool by specifying start and end IP addresses. Be sure not to include the unit's IP address in the address pool range.

**LAN Settings**

You can disable DHCP to set static IP addresses to your client PCs.

**IP Address** 192 . 168 . 1 . 1

**Subnet Mask** 255.255.255.0

**The Gateway acts as DHCP Server**  Enable

**IP Pool Starting Address** 192.168.1.2

**IP Pool Ending Address** 192.168.1.254

**Lease Time** Half hour

**Local Domain Name** openrange.net (optional)

**Figure 5-11: Local Area Network Settings**

- **IP Address** – The IP address of the unit. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. The default setting is 192.168.1.1.



#### CAUTION

Changing the IP address of the BreezeMAX Si 2000 will prompt a warning window and will require a system reboot.



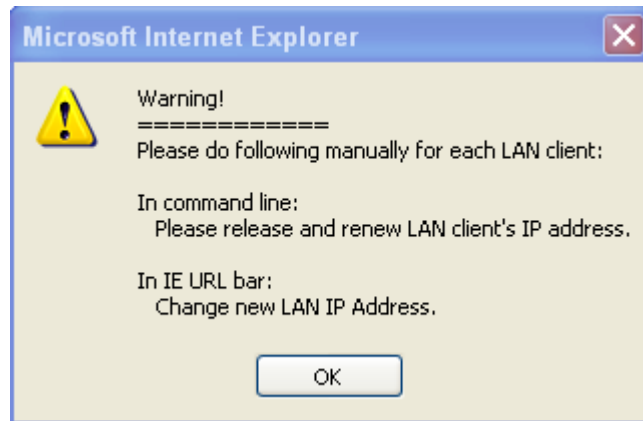



Figure 5-12: IP Address Warning

- **Subnet Mask** – Indicates the local subnet mask is fixed as 255.255.255.0.
- **The Gateway acts as DHCP Server** – Check this box to enable the DHCP server.
- **IP Pool Starting/Ending Address** – Specifies the start and end IP address of a range that the DHCP server can allocate to DHCP clients. You can specify a single address or an address range. Note that the address pool range is always in the same subnet as the unit's IP setting. (Default: 192.168.1.2 to 192.168.1.254)
- **Lease Time** – Selects a time limit for the use of an IP address form the IP pool. When the time limit expires, the client has to request a new IP address. (Default: Half hour; Options: Half hour, one hour, two hours, half day, one day, two days, one week, two weeks)
- **Local Domain Name** – This optional parameter specifies the name of the domain to which the unit is attached.

## 5.4.2 DHCP Client List

The DHCP Client List page enables you to see the MAC address of devices that are currently connected to the unit and have been assigned an IP address by the DHCP server.



The DHCP client list allows you to see which clients are connected to the Router via IP address, host name, and MAC address.

IP Address	MAC Address
10.0.0.2	00:10:b5:c4:22:dd

Figure 5-13: DHCP Client List

## 5.5 NAT

Network Address Translation (NAT) is a standard method of mapping multiple “internal” IP addresses to one “external” IP address on devices at the edge of a network. For the BreezeMAX Si 2000, the internal (local) IP addresses are the IP addresses assigned to local PCs by the DHCP server, and the external IP address is the IP address assigned to the WiMAX interface.

### 5.5.1 Virtual Server

Using the NAT Virtual Server feature, remote users can access different servers on your local network using your single public IP address.

Remote users accessing services such as web or FTP at your local site through your public IP address, are redirected (mapped) to other local server IP addresses and TCP/UDP port numbers. For example, if you set Public Port to TCP/80 (HTTP or web) and the Private IP/Port to 192.168.1.9/80, then all HTTP requests from outside users are forwarded to 192.168.1.45 on port 80. Therefore, by just using your external IP address provided by your ISP, Internet users can access the services they need at the local addresses to which you redirect them.

The more common TCP service port numbers include: HTTP: 80, FTP: 21, Telnet: 23, and POP3: 110.

Virtual Server

You can configure the device as a virtual server so that remote users accessing services such as the Web or FTP at your local site via public IP addresses can be automatically redirected to local servers configured with private IP addresses. In other words, depending on the requested service (TCP/UDP port numbers), the device redirects the external service request to the appropriate server (located at another internal IP address)..

	Private IP	Private Port	Type	Public Port	Enabled
1	192.168.1.45	80	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	80	<input checked="" type="checkbox"/>
2	192.168.1.35	21	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	21	<input checked="" type="checkbox"/>
3	192.168.1.		<input checked="" type="radio"/> TCP <input type="radio"/> UDP		<input type="checkbox"/>
4	192.168.1.		<input checked="" type="radio"/> TCP <input type="radio"/> UDP		<input type="checkbox"/>
5	192.168.1.		<input checked="" type="radio"/> TCP <input type="radio"/> UDP		<input type="checkbox"/>

**Figure 5-14: NAT Virtual Server**

- **Private IP** – The IP address of the server on the local Ethernet network. The specified address must be in the same subnet as the BreezeMAX Si 2000 and its DHCP server address pool. (Range: 192.168.1.1 to 192.168.1.254)
- **Private Port** – Specifies the TCP/UDP port number used on the local server for the service. (Range: 1-65535)

- **Type** – Specifies the port type. (Options: TCP or UDP; Default: TCP)
- **Public Port** – Specifies the public TCP/UDP port used for the service on the WAN interface. (Range: 1-65535)
- **Enabled** – Enables the virtual server mapping on the specified ports. (Default: Disabled)

## 5.5.2 Port Mapping

Some applications, such as Internet gaming, video conferencing, Internet telephony and others, require multiple connections. These applications cannot work with Network Address Translation (NAT) enabled. If you need to run applications that require multiple connections, use port mapping to specify the additional public ports to be opened for each application.

**Port Mapping**

For some applications, you need to assign a set or a range of ports to a specified local machine to route the packets. Device allows the user to configure the needed port mappings to suit such applications..

The valid value of "Mapping Port" is such as "80", "20-21", or "20-21,80,139".

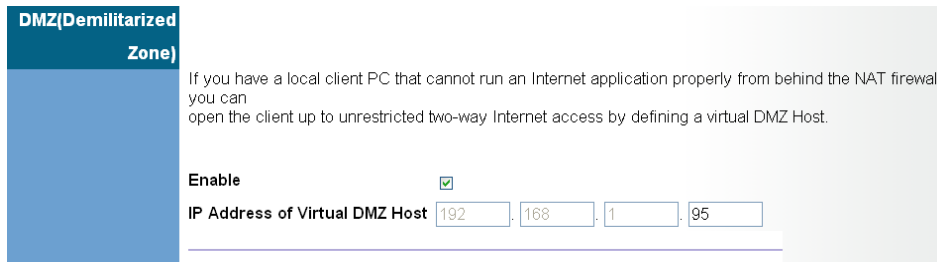
	Server IP	Mapping Ports	Enabled
1	192.168.1.19	5431	<input type="checkbox"/>
2	192.168.1.35	4532,6543	<input checked="" type="checkbox"/>
3	192.168.1.		<input type="checkbox"/>
4	192.168.1.		<input type="checkbox"/>
5	192.168.1.		<input type="checkbox"/>

**Figure 5-15: NAT Port Mapping**

- **Server IP** – The IP address of the local server. (Range: 192.168.1.1 to 192.168.1.254)
- **Mapping Ports** – Specifies the TCP/UDP ports that the application requires. The ports may be specified individually, in a range, or a combination of both. For example, 7, 11, 57, 72-96. (Range: 1-65535)
- **Enabled** – Enables port mapping for the specified IP address. (Default: Disabled)

### 5.5.3 DMZ

If you have a client PC that cannot run an Internet application properly from behind the NAT firewall, you can open the client up to unrestricted two-way internet access by defining a virtual-DMZ (virtual-demilitarized-zone) host.



**DMZ(Demilitarized Zone)**

If you have a local client PC that cannot run an Internet application properly from behind the NAT firewall, you can open the client up to unrestricted two-way Internet access by defining a virtual DMZ Host.

**Enable**

**IP Address of Virtual DMZ Host** 192 . 168 . 1 . 95

**Figure 5-16: DMZ**

- **Enable** – Enables the feature. (Default: Disabled)
- **IP Address of Virtual DMZ Host** – Specifies the IP address of the virtual DMZ host. (Range: 192.168.1.1 to 192.168.1.254; Default: 192.168.1.0)



#### NOTE

Adding a host to the DMZ may expose your local network to a variety of security risks, so only use this option as a last resort.

## 5.6 Firewall

The BreezeMAX Si 2000 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).

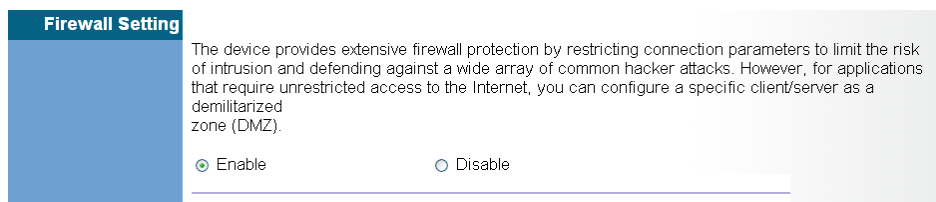


Figure 5-17: Firewall Setting

- **Enable** – Enables the feature.
- **Disable** – Disables the feature. (This is the default.)

### 5.6.1 Firewall Options

The BreezeMAX Si 2000's firewall enables access control of client PCs, blocks common hacker attacks, including IP Spoofing, Land Attack, Ping of Death, Smurf Attack, TCP null scan, ICMP defect, and TCP SYN flooding. The firewall does not significantly affect system performance and it is best to leave it enabled to protect your network.

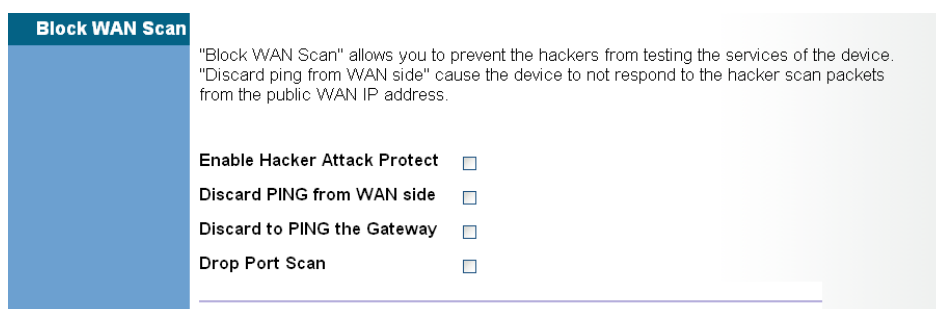


Figure 5-18: Firewall Options

- **Enable Hacker Attack Protect** – Network attacks that deny access to a network device are called DoS attacks. DoS attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access

to network resources. The Router protects against the following DoS attacks: IP Spoofing, Land Attack, Ping of Death, Smurf Attack, TCP null scan, ICMP defect, and TCP SYN flooding.

- **Discard PING from WAN side** – Prevents pings on the unit’s WiMAX interface from being routed to the network.
- **Discard to PING the Gateway** – Prevents any response to a ping to the unit’s IP address from the LAN.
- **Drop Port Scan** – Prevents outside hackers from testing the TCP/UDP port numbers on the unit for any services.

## 5.6.2 Client Filtering

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.

**Client Filtering**

You can block certain client PCs accessing the Internet based on IP and port number.

Enable Client Filter

	IP	Port	Type	Enabled
1	192.168.1. 50 ~ 70	1234 ~ 2345	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
2	192.168.1. 120 ~ 150	20 ~ 80	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
3	192.168.1. [ ] ~ [ ]	[ ] ~ [ ]	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
4	192.168.1. [ ] ~ [ ]	[ ] ~ [ ]	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
5	192.168.1. [ ] ~ [ ]	[ ] ~ [ ]	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>

**Figure 5-19: Client Filtering**

- **Enable Client Filter** – Enables client filtering for entries in the table. (Default: Disabled)
- **IP** – Specifies an IP address or range on the local network. (Range: 192.168.1.1 to 192.168.1.254)
- **Port** – Specifies a TCP/UDP port number range to filter. (Range: 1-65535)
- **Type** – Specifies the port type. (Options: TCP or UDP; Default: TCP)
- **Enable** – Enables filtering for the table entry. (Default: Disabled)

### 5.6.3 MAC Control

You can block access to the Internet from clients on the local network by MAC addresses. You can configure up to 20 MAC address filters on the unit.

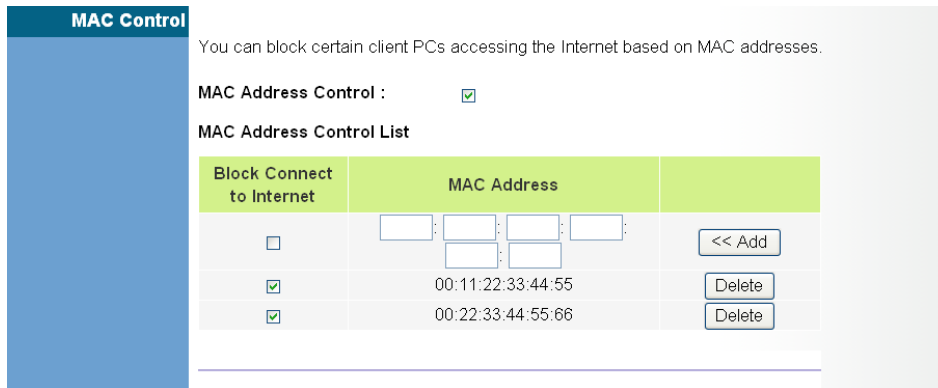


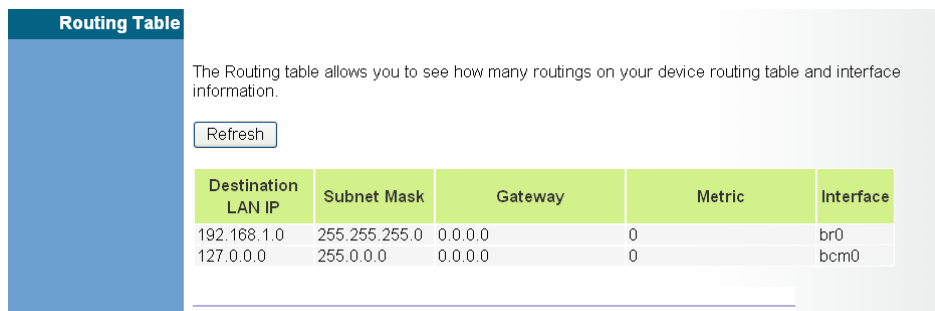
Figure 5-20: MAC Control

- **MAC Address Control** – Enables the feature. (Default: Enabled)
- **Block Connect to Internet** – Blocks Internet access for the specified MAC address. (Default: Enabled)
- **MAC Address** – Specifies a local PC MAC address.
- **Add** – Adds a new MAC address to the filter table.
- **Delete** – Removes a MAC address from the filter table.



## 5.7 Route

The Routing Table displays the list of static routes on the unit.



The Routing table allows you to see how many routings on your device routing table and interface information.

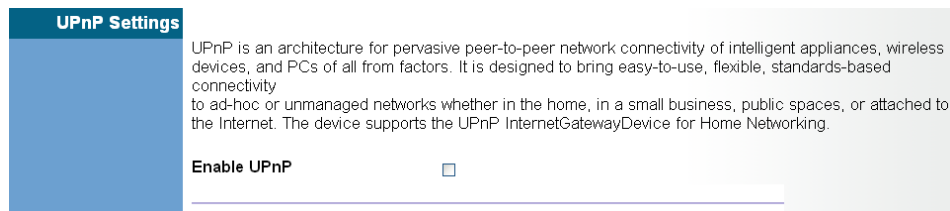
Destination LAN IP	Subnet Mask	Gateway	Metric	Interface
192.168.1.0	255.255.255.0	0.0.0.0	0	br0
127.0.0.0	255.0.0.0	0.0.0.0	0	bcm0

**Figure 5-21: Routing Table**

- **Destination LAN IP** – The IP address that identifies the IP subnet of the remote network.
- **Subnet Mask** – The mask that identifies the IP subnet of the remote network.
- **Gateway** – The IP address of the router within the local IP subnet that forwards traffic to the remote IP subnet.
- **Metric** – Cost for the local interface. This cost is only used when routes are imported by a dynamic routing protocol.
- **Interface** – Indicates the local network interface on the unit.

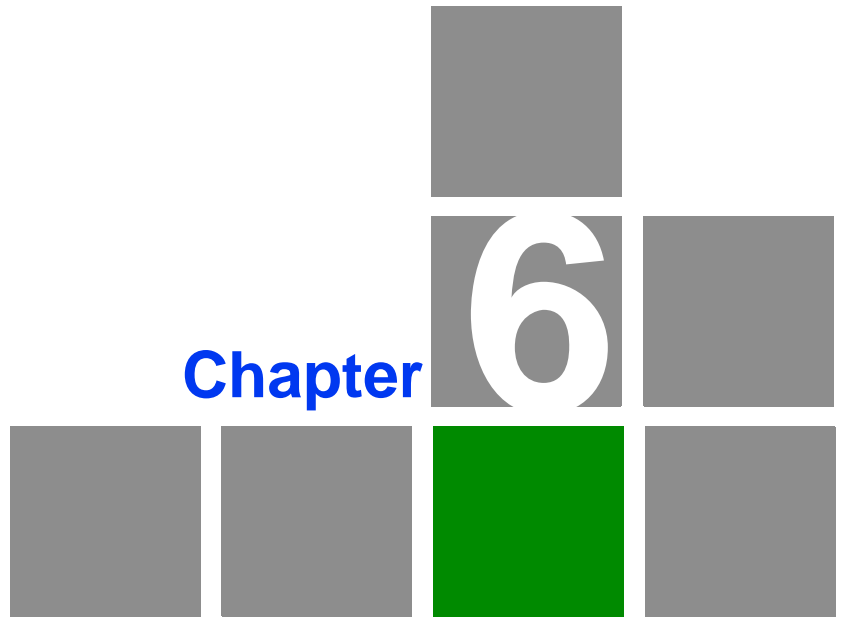
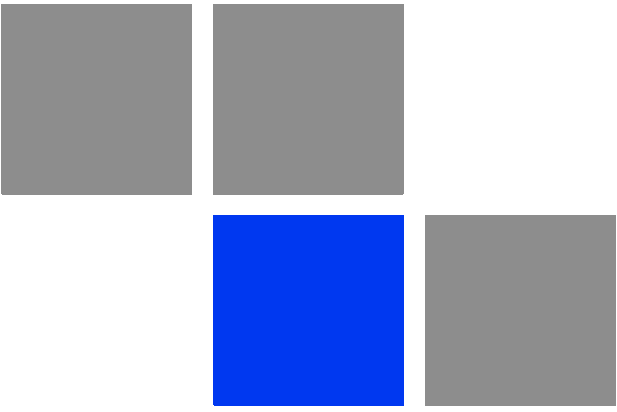
## 5.8 UPnP

UPnP (Universal Plug and Play Forum) provides inter-connectivity between devices supported by the same standard.



**Figure 5-22: UPnP**

- **UPnP** – Enables UpnP support on the unit. (Default: Disabled)



Chapter

6

**WiMAX Settings**

## In This Chapter:

- [“Introduction” on page 76](#)
- [“WiMAX Login” on page 77](#)
- [“Subscriber Station Information” on page 80](#)
- [“Antenna Setting” on page 81](#)
- [“Advanced Configuration” on page 82](#)

## 6.1 Introduction

The BreezeMAX Si 2000's WiMAX menu enables you to configure WiMAX network authentication, view subscriber station information, and select an operating antenna.

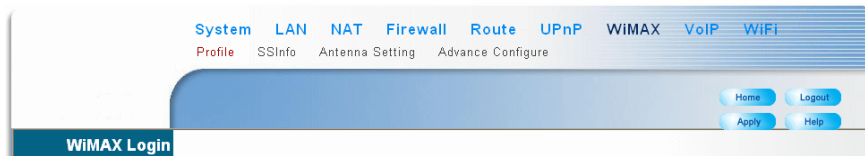


Figure 6-1: WiMAX Menu – Admin Mode

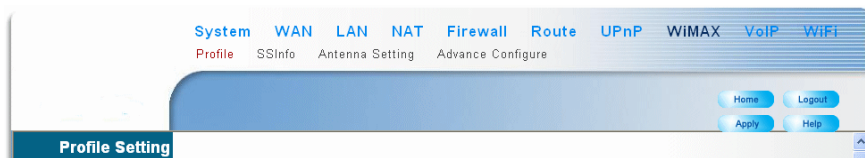


Figure 6-2: WiMAX Menu – Operator Mode

## 6.2 WiMAX Login

The BreezeMAX Si 2000's WiMAX menu enables you to configure WiMAX network settings and authentication.

**Figure 6-3: WiMAX Login – Admin Mode**

- **Username** – The user name required for network authentication, as supplied by the WiMAX service provider. (Default: pseudo@realm)
- **Password** – The user password required for network authentication, as supplied by the WiMAX service operator. (Range: 1-32 characters; Default: hello)

**Figure 6-4: Profile Setting – Operator Mode**

**GENERAL:** Sets the operator ID, name and restriction.

- **Operator ID** – A numeric string that uniquely identifies the WiMAX operator, separated by colons.
- **Operator Names** – The name of the WiMAX operator.
- **Operator Restriction** – When Operator Restriction is selected the user can only connect to the service provider specified in the profile. When not selected, the operator specified in the profile is used when the network is detected, otherwise the user can roam to other networks.

**SCAN:** Sets the scanned frequencies for the WiMAX profile.

- **Frequency** – Specifies a center frequency to scan. (Range: 2000M~4000M)
- **Bandwidth** – Specifies the bandwidth of the channel; 5, 7, or 10 MHz. Currently only bandwidths 5 and 10 MHz are supported.
  - » **Add/Remove:** Adds or Removes the specified frequency.

**AUTHENTICATION:** Sets WiMAX network authentication.

- **Enable Authentication** – Enables authentication.
- **EAP Method** – Selects the Extensible Authentication Protocol (EAP) method to use for authentication. (Default: EAP-TTLS-MSCHAPV2)
  - » **EAP-TLS:** Transport Layer Security. Provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based encryption keys to secure subsequent communications between the user and the network. A unique X.509 authentication certificate is included with the gateway firmware.
  - » **EAP-TTLS-CHAP:** Tunneled Transport Layer Security with Challenge-Handshake Authentication Protocol (CHAP). This security method provides for certificate-based, mutual authentication of the client and network through an encrypted channel. Unlike EAP-TLS, EAP-TTLS

requires only server-side certificates. The CHAP protocol requires a user name and password to be configured.

- » **EAP-TTLS-MSCHAPV2:** Tunneled Transport Layer Security with Microsoft's version 2 of CHAP. The MS-CHAP protocol requires a user name and password to be configured.

■ **EAP Mode** – Defines the authentication mode.

- » **device only:** Specifies authentication using the unique X.509 authentication certificate included with the gateway firmware.
- » **user-only:** Specifies authentication using the configured user name and password.
- » **user-device:** Specifies authentication using the configured user name and password, and the unique X.509 authentication certificate.

■ **Username** – The user name required for EAP-TTLS authentication.  
(Default: pseudo@realm)

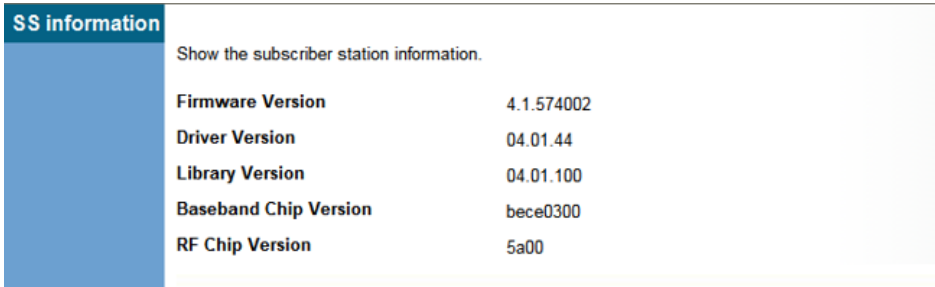
■ **Password** – The user password required for EAP-TTLS authentication.  
(Range: 1-32 characters; Default: hello)

■ **MAC Address @ domain** – A text string that is used to identify the authentication realm for device authentication. This identity is used to proxy an authentication request to another remote server. The authentication is then performed using the unique X.509 authentication certificate included with the device firmware. The identity string consists of the device MAC address together with an operator-specified domain name. For example;  
1f:20:30:10:4d:50@service-telecom.



## 6.3 Subscriber Station Information

The SSInfo page displays information about the software versions on the BreezeMAX Si 2000 unit.



The screenshot shows a web interface with a blue sidebar on the left containing the text 'SS information'. The main content area has a light gray background and contains the text 'Show the subscriber station information.' followed by a table of software versions.

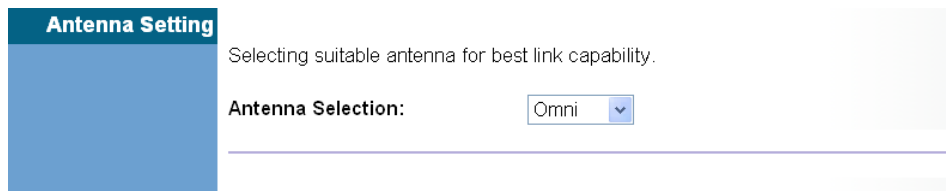
Firmware Version	4.1.574002
Driver Version	04.01.44
Library Version	04.01.100
Baseband Chip Version	bece0300
RF Chip Version	5a00

**Figure 6-5: Subscriber Station Information**

- **Firmware Version** – The version of software code running on the unit.
- **Driver Version** – The version of the WiMAX chip driver software.
- **Library Version** – The version of WiMAX library software.
- **Baseband Chip Version** – The version of the WiMAX baseband chip.
- **RF Chip Version** – The version of the WiMAX radio chip.

## 6.4 Antenna Setting

The BreezeMAX Si 2000 provides the option of using an external antenna instead of the antennas integrated into the unit. If you decide to use an external antenna, set the Antenna Selection setting to “External.”



**Figure 6-6: Antenna Setting**

- **Antenna Selection** – Selects either the default omnidirectional (Omni) antennas or an optional external antenna for WiMAX communications. (Default: Omni)

## 6.5 Advanced Configuration

The Advanced Configuration screen allows you to configure extended features for the WiMAX connection.



### NOTE

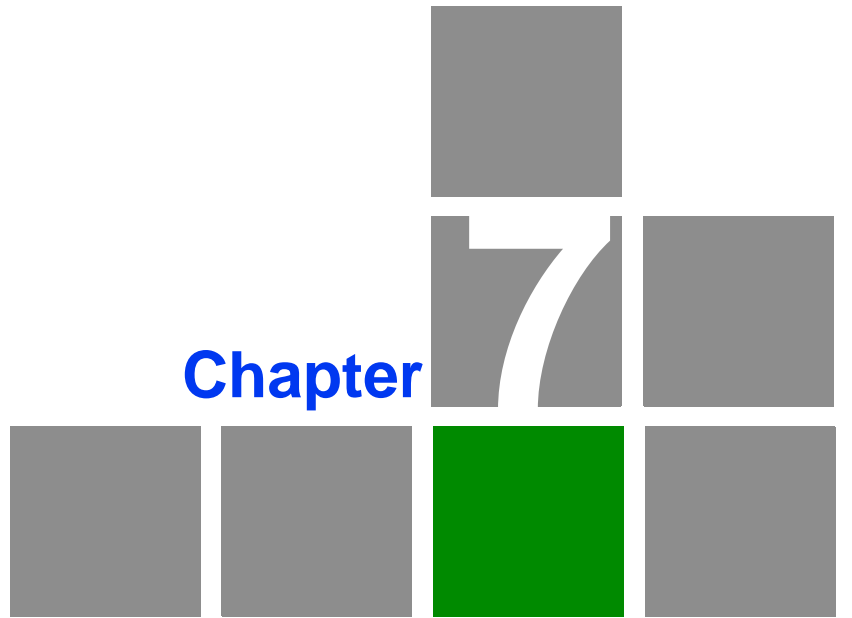
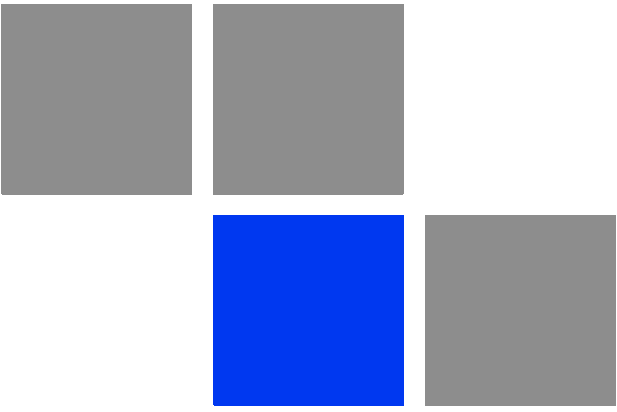
The Advanced Configuration page is only available in Operator mode

**Figure 6-7: Advanced Configuration**

- **Center Frequency** – Configures the centre frequency used by the WiMAX service.
- **Bandwidth** – Configures the channel bandwidth used by the WiMAX service.
- **Hand Over Enable** – Enable handoffs when moving between base stations.
- **ARQ Enable** – The ARQ (Automatic Repeat reQuest) mechanism is an optional part of the WiMAX MAC layer and a protocol for error control in data transmission. When a packet error is detected, the transmitter is automatically requested to resend the packet.
- **HARQ Enable** – Hybrid ARQ (HARQ) is a variation of the ARQ error control method. In standard ARQ, error-detection information (ED) bits are added to data to be transmitted (such as cyclic redundancy check, CRC). In Hybrid ARQ, forward error correction (FEC) bits are also added to the existing Error Detection (ED) bits (such as Reed-Solomon code or Turbo code).
- **PKMv2 Enable** – PKMv2 (Privacy Key Management version 2) is the standard security solution for WiMAX networks. The security protocol provides mutual authentication of the subscriber station and base station, as well as

distributing traffic encryption keys. It is also used to transport EAP (Extensible Authentication Protocol) messages. PKMv2 must not be enabled without authentication being also enabled on the device. PKMv2 is automatically enabled when authenticated mode is used.

- **DL MIMO Enable** – Enables the use of downlink multiple-input and multiple-output (DL MIMO) antennas.
  
- **PHS Enable** – Enables payload header suppression (PHS) a feature that conserves link layer bandwidth by suppressing unnecessary packet headers on upstream and downstream traffic flows.



**Chapter**

**VoIP Settings**

## In This Chapter:

- [“Introduction” on page 86](#)
- [“SIP Account” on page 87](#)
- [“SIP Setting” on page 89](#)
- [“Dial Plan” on page 91](#)
- [“Call Feature” on page 93](#)
- [“Codecs” on page 95](#)
- [“Call Block Setting” on page 97](#)
- [“Phone Setting” on page 98](#)

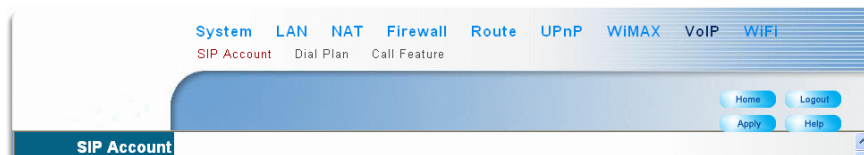
## 7.1 Introduction

Voice over Internet Protocol (VoIP) technology is a way of using the Internet to make phone calls. Phone calls can be transmitted over the Internet by encoding a voice call into data packets at one end and then decoding it back into voice calls at the other end. This encoding and decoding is from an analog signal (your voice) into a digital signal (data packets) and then back into an analog signal.

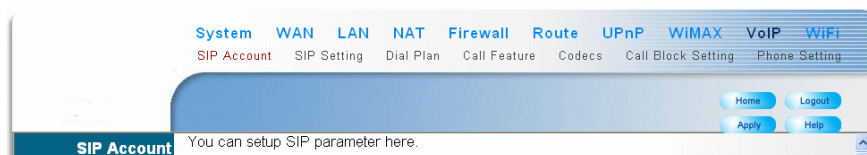
The BreezeMAX Si 2000 uses Session Initiation Protocol (SIP) as the control mechanism that sets up, initiates, and terminates calls between a caller and a called party. The SIP messaging makes use of “Proxy,” “Redirect,” and “Registration” servers to process call requests and find the location of called parties across the Internet. When SIP has set up a call between two parties, the actual voice communication is a direct peer-to-peer connection using the standard Real-Time Protocol (RTP), which streams the encoded voice data across the network.

You can make VoIP calls by connecting a regular phone to one of the BreezeMAX Si 2000’s RJ-11 Phone ports. You can also make VoIP calls from your computer using a VoIP application with a simple microphone and computer speakers. Using either method, VoIP provides an experience identical to normal telephoning.

Before using the VoIP Phone ports on the BreezeMAX Si 2000, you must have an account with a SIP service provider and configure the required parameters through the web interface. The BreezeMAX Si 2000 allows the two RJ-11 Phone ports to be configured separately with different settings.



**Figure 7-1: VoIP Menu – Admin Mode**



**Figure 7-2: VoIP Menu – Operator Mode**

## 7.2 SIP Account

From the VoIP SIP Account page, you can configure the basic SIP service parameters for Phone 1 and Phone 2.

**Figure 7-3: SIP Account Settings – Admin Mode**

**Figure 7-4: SIP Account Settings – Operator Mode**



- **Enable Proxy Outbound** – Enables the use of proxy servers in the local network to forward SIP requests. (Default: Disabled)
- **Always Proxy Outbound** – Forces all SIP requests to be forwarded through local proxy servers. (Default: Disabled)
- **Expire Time** – The time the BreezeMAX Si 2000 waits for a response from a proxy server before a VoIP call fails. (Range: 60-65535 seconds; Default: 3600 seconds)
- **SIP Account** – The SIP account user name.
- **Auth. User Name** – An alphanumeric string that uniquely identifies the user to the SIP server.
- **Auth. Password** – An alphanumeric string that uniquely identifies the SIP user's permission rights.
- **Display Name** – The name that is displayed to the other party during a call.
- **SIP Registrar** – The IP address of the SIP registrar server. A registrar is a server that accepts SIP register requests and places the information it receives in those requests into the location service for the domain it handles.
- **SIP Registrar Port Number** – The TCP port number used by the VoIP service provider's register server. (Range: 1-65535; Default: 5060)
- **Proxy Address** – Address of the VoIP service provider SIP proxy server.
- **Proxy Port** – The TCP port number used by the VoIP service provider's SIP proxy server. (Range: 1-65535; Default: 5060)

## 7.3 SIP Setting

From the VoIP SIP Setting page you can configure SIP parameter details.



### NOTE

The SIP Setting page is only available in Operator mode

**SIP Setting**

You can setup SIP parameter here.

RTP Packetization Time  ms

RTP Port Base

RTP Port Limit

---

Domain Name

Stun Server  :   
ex:0.0.0.0:3478 (0.0.0.0 means not available)

DTMF

Invite Timeout  secs

---

	Phone 1	Phone 2
T.38 Option	<input type="text" value="Voice and T.38 Fax Relay"/>	<input type="text" value="Voice and T.38 Fax Relay"/>

**Figure 7-5: SIP Settings**

- **RTP Packetization Time** – Specifies a maximum amount of time for transmission of a RTP data packet. (Options: 10, 20, 30 ms; Default: 20 ms)
- **RTP Port Base/Limit** – The Real-time Transport Protocol (RTP) and Real-time Control Protocol (RTCP) do not use specified port numbers. You can specify a port range that the RTP and RTCP traffic can use. Enter the port Base and Limit to define the range. (Range: 1024-65535)
- **Domain Name** – The host portion of the SIP Uniform Resource Identifiers (URIs) that are assigned to users in a network. The SIP domain name can sometimes be different from the internal network domain name.
- **Stun Server** – STUN (Simple Traversal of UDP through NAT (Network Address Translation)) is a protocol that assists devices behind a NAT firewall or router with packet routing. The problem of NAT firewalls can also be solved using a proxy server to control SIP traffic. Specify the IP address and TCP port used by the STUN server. (Default: 0.0.0.0:3478, “0.0.0.0” means not available; Port Range: 0-65535)

- **DTMF** – Enables the sending of dual-tone multi-frequency (touch tone) phone signals over the VoIP connection. There are several methods to choose from:
  - » **No DTMF**: The DTMF signals are not sent over the VoIP connection.
  - » **In-band Mode**: The DTMF signals are sent over the RTP voice stream. In the case when low-bandwidth codecs are used, the DTMF signals may be distorted.
  - » **2833 Relay**: Uses the RFC 2833 method to relay the DTMF signals over the RTP voice stream without any distortion. (This is the default.)
  - » **Both In-band and 2833**: Uses the best method depending on the called party.
  
- **Invite Timeout** – The time that the unit waits for a response to a SIP Invite message before a call fails. If network connections are slow and many SIP calls fail, you may need to increase this timeout value. (Range: 1-32 seconds; Default: 12 seconds)
  
- **T.38 Option** – Selects the method to use when sending fax messages over the VoIP network from a fax machine connected to one of the RJ-11 Phone ports on the BreezeMAX Si 2000. (Default: Voice and T.38 Fax Relay)
  - » **T.38 Fax Relay**: The SIP protocol sets up the VoIP call, then the T.38 Fax Relay protocol sends the fax data over the network.
  - » **Voice and T.38 Fax Relay**: Enables voice calls and faxes to be sent from the Phone port connection. When a fax tone signal is detected on the port, the T.38 Fax Relay standard is used instead of the voice codec.
  - » **Voice and Fax Pass Through**: Enables voice calls and faxes to be sent from the Phone port connection. For this option, fax signals are sent over the VoIP network using the voice codec, just as if it were a voice call.

## 7.4 Dial Plan

A dial-plan string can be specified to control phone numbers dialed out through the BreezeMAX Si 2000. A dial plan describes the number and pattern of digits that a user dials to reach a particular telephone number. Access codes, area codes, specialized codes, and combinations of the number of digits dialed can all be part of a dial plan. This enables a user to predefine dialling sequences that are permitted. It can help transfer, check, limit phone numbers, and handle prefixes to certain numbers.

The dial-plan string consists of a single digit rule. A typical example of a dial-plan string is: [0123]xxxxxx.t

Three standard dial plans are defined; Call Transfer Key, New Call Key, and 3-way Conference. Up to 10 other dial plans can be defined by the user.

Dial Plan Setting

A dial-plan string can be specified to control phone numbers dialed out through the gateway. A dial plan describes the number and pattern of digits that a user dials to reach a particular telephone number. Access codes, area codes, specialized codes, and combinations of the number of digits dialed can all be part of a dial plan. This enables a user to predefine dialling sequences that are permitted. It can help transfer, check, limit phone numbers, and handle prefixes to certain numbers. For more detailed description, please refer to the online help.

SNo	Action	Plan
1	Call Transfer Key	*#
2	New Call Key	**
3	3-way Conference	*3
4	Dial Plan 1	x.t
5	Dial Plan 2	
6	Dial Plan 3	
7	Dial Plan 4	
8	Dial Plan 5	
9	Dial Plan 6	
10	Dial Plan 7	

**Figure 7-6: Dial Plan Settings**

The function of elements allowed in a dial plan are described in the table below:

**Table 7-1: Dial Plan Functions**

Element	Example	Description
■ x	xxxx	Represents a digit of any value ( 0 to 9) that can be dialed on a phone. This example has a rule with four digits of any number.
■ .	xx.	Indicates zero or more occurrences of the previous symbol. The example acts like a wildcard, meaning any dialed phone number of two or more digits is allowed.
■ 0-9	01xx	Indicates dialed digits that must be matched. This example only allows four-digit numbers starting "01."
■ [ ]	[125-8]	Limits a dialed digit to specified values or a range of values. The example specifies that only digits 1, 2, 5, 6, 7, and 8 are permitted.
■ t	xx.t	The timeout indicator that can placed after dialed digits or at the end of the dial-plan string.

When a user dials a series of digits, the dial-plan rule is tested for a possible match. If a match is made, the dialed sequence is transmitted. If no match is made, the dialed number is blocked and the user will hear an error tone.

A dial-plan string cannot include spaces between elements. Dialed sequences that are longer than specified in a dial-plan rule are truncated after the number of specified digits. For example, if the dial-plan rule is "011x" and "0115678" is dialed, only the digit sequence "0115" is transmitted.

## 7.5 Call Feature

The BreezeMAX Si 2000 allows you to configure several call features, such as call waiting and call-forwarding. Other call features can be implemented by pressing specific phone buttons or entering dial patterns.

The table below describes the various call features available.



### NOTE

Some call features may be dependent on support at the SIP server. Check with the SIP service provider.

**Table 7-2: VoIP Call Features**

Call Feature	Description	Activation
■ Call Hold	Places an active call on hold for an unlimited period of time.	Press the “Flash,” “Flash Hook,” or “Hold” button on the phone.
■ Call Waiting	If during a call there is another incoming call, an alert tone is heard.	This feature must first be enabled using the web interface. You can place the active call on hold and switch to the incoming call. You can switch between the two calls by placing the active call on hold.
■ Call Switching	Calls two numbers, then switches between them.	Dial the first number, then place it on hold. Dial the key sequence “***” and wait until you hear the dial tone, then dial the second number. Placing the active call on hold switches to the other call. If the active call is hung up, the phone rings again to activate the other call.
■ Call Transfer	Transfers any received call to another number you specify.	First place the received call on hold, then dial the transfer key sequence “*#”. When you hear a dial tone, enter the transfer phone number, then hang up.
■ Call Forward	Forwards an incoming call to another number.	This feature can be configured using the web interface. You can specify forwarding numbers for all calls, when busy, or for no answer.
■ 3-Way Conference	Calls two numbers, then allows all to talk together.	Dial the first number, then place it on hold. Dial the key sequence “***” and wait until you hear the dial tone, then dial the second number. When the second call is active, dial “*3” to establish the three-way conference.

Call Feature Setting		
Call Waiting	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Call Waiting Timeout	<input type="text" value="30"/> secs	
	Phone 1	Phone 2
Always Forward Phone Number	<input type="text"/>	<input type="text"/>
On Busy Forward Phone Number	<input type="text"/>	<input type="text"/>
No Answer Forward Phone Number	<input type="text"/>	<input type="text"/>
No Answer Call Forward Timeout	<input type="text" value="10"/>	<input type="text" value="10"/>

Figure 7-7: VoIP Call Features

- **Call Waiting** – Enables a call waiting alert. If during a call there is another incoming call, an alert tone is heard. You can place the active call on hold (press the “Flash,” “Flash Hook,” or “Hold” button on the phone) and switch to the incoming call. (Default: Disabled)
- **Call Waiting Timeout** – The time a second incoming call waits before a “no answer” message is sent. (Must be less than or equal to the value of Answer Timeout; Default: 30 seconds)
- **Always Forward Phone Number** – Another phone number to which all incoming calls are forwarded.
- **On Busy Forward Phone Number** – Another phone number to which incoming calls are forwarded when the phone is busy.
- **No Answer Forward Phone Number** – Another phone number to which incoming calls are forwarded when there is no answer.
- **Call Forward No Answer Timeout** – The time a call waits for an answer before being forwarded to the No Answer Forward Phone Number. (Must be less than or equal to the value of Answer Timeout; Default: 10 seconds)

## 7.6 Codecs

A codec (coder/decoder) is the way a voice analog signal is converted into a digital bitstream to send over the network, and how it is converted back into an analog signal at the receiving end. Codecs differ in the type of data compression that is used to save network bandwidth and in the time delay caused in the signal. This results in different voice quality experienced by the user.

The voice codecs in common use today have been standardized by the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) and are identified by a standard number, such as G.711 or G.726. The same codec must be supported at each end of a VoIP call to be able to encode and decode the signal. Since devices in other networks may want to use different codecs, the BreezeMAX Si provides support for several common standards.



### NOTE

The Codecs page is only available in Operator mode

Codec	Enabled	Priority Codec List
PCMA(G711-aLaw)	<input checked="" type="checkbox"/>	G729ab
PCMU(G711-uLaw)	<input checked="" type="checkbox"/>	PCMU(G711-uLaw)
G723	<input checked="" type="checkbox"/>	PCMA(G711-aLaw)
G729ab	<input checked="" type="checkbox"/>	G726-32
G726-16	<input checked="" type="checkbox"/>	G726-16
G726-24	<input checked="" type="checkbox"/>	G726-24
G726-32	<input checked="" type="checkbox"/>	G726-40
G726-40	<input checked="" type="checkbox"/>	G723

[Check All](#)    UP    DOWN

**Figure 7-8: VoIP Codec Settings**

- **Codec** – Lists the codecs supported by the BreezeMAX Si 2000. You can enable specific codecs to use, or enable all. Alternatively, you may want to disable certain codecs, such as high-bandwidth codecs, to preserve network bandwidth.
- » **PCMA (G711.aLaw)**: The ITU-T G.711 with A-law standard codec that uses Pulse Code Modulation (PCM) to produce a 64 Kbps high-quality voice data



stream. This standard is used in Europe and most other countries around the world.

- » **PCMU (G711.uLaw):** The ITU-T G.711 with mu-law standard codec that uses Pulse Code Modulation (PCM) to produce a 64 Kbps high-quality voice data stream. This standard is used in North America and Japan.
  - » **G723.1:** The ITU-T G.723.1 standard low bitrate codec that uses Multi-Pulse Maximum Likelihood Quantization (MP-MLQ) and Algebraic Code Excited Linear Prediction (ACELP) speech coding to produce data streams of 6300 and 5300 bps.
  - » **G729ab:** The ITU-T G.729ab standard codec that uses Conjugate Structure Algebraic-Code Excited Linear Prediction (CS-ACELP) with silence suppression to produce a low-bandwidth data stream of 8 Kbps. Note that DTMF and fax tones do not transport reliably with this codec, it is better to use G.711 for these signals.
  - » **G726-16/24/32/40:** The ITU-T G.726 standard codecs that use Adaptive Differential Pulse Code Modulation (ADPCM) to produce good-quality, low-bandwidth data streams of either 16, 24, 32, or 40 Kbps.
- **Priority Codec List** – The BreezeMAX Si 2000 automatically negotiates the codec to use for each called party. You can specify a priority for the codecs that you prefer to use. For example, you may want to use a low-bandwidth codec such as G729ab instead of a high-bandwidth G711 codec. Select a codec in the list, then use the UP and DOWN buttons to set the priority. The BreezeMAX Si 2000 attempts to use the codec highest in the list before trying the next lower one.

## 7.7 Call Block Setting

The BreezeMAX Si 2000 can block certain incoming and outgoing phone numbers from making calls through the unit. You can specify up to 15 incoming and 15 outgoing numbers to block.



### NOTE

The Call Block Setting page is only available in Operator mode

Phone 1 Block Settings		
Phone <input checked="" type="radio"/> 1 <input type="radio"/> 2		
SNo	Outgoing	Incoming
1	123456	112211
2	123456	112233
3	12345566	112244
4		
5		
6		
7		
8		
9		
10		
11		
12		

Figure 7-9: Call Block Settings

- **Phone** – Selects either VoIP port PHONE1 or PHONE2.
- **Outgoing** – Blocks outgoing calls from the listed numbers. (Valid characters 0-9)
- **Incoming** – Blocks incoming calls from the listed numbers. (Valid characters 0-9)

## 7.8 Phone Setting

The BreezeMAX Si 2000 allows a national country setting to be enabled for the region in which you are operating the unit, as well as the telecom service provider currently listed as support by the unit.

The BreezeMAX Si 2000 allows the timings for certain events on the VoIP phone ports to be precisely configured. For example, you can specify how long a phone will ring and how long a dial tone is heard on a phone.

The BreezeMAX Si 2000 also enables the line delay to be specified for each phone so that the caller's voice echo is cancelled.



### NOTE

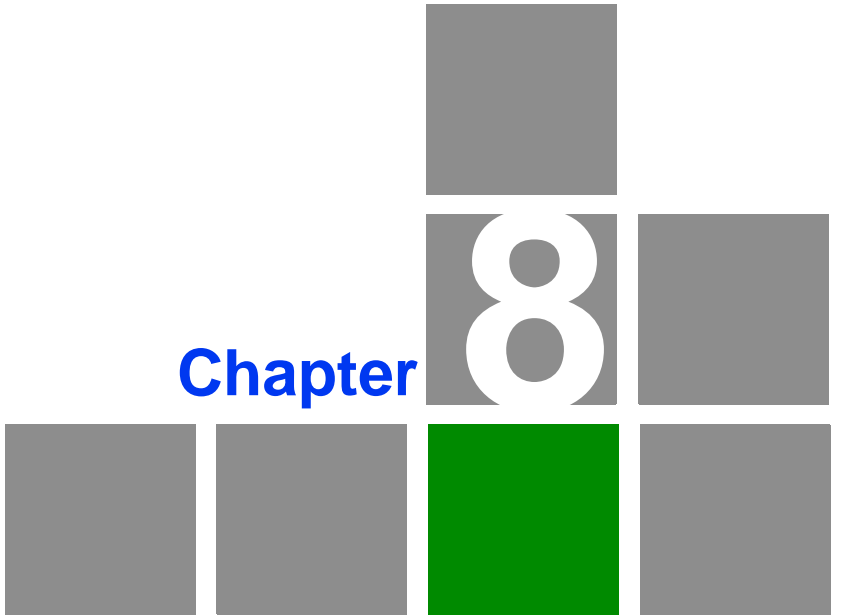
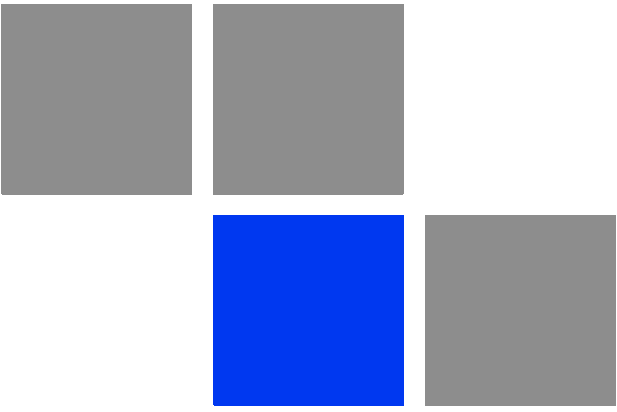
The Phone Setting page is only available in Operator mode

	Phone 1	Phone 2
Line Echo Cancellation	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
VAD/CNG	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

**Figure 7-10: Phone Settings**

- **National Profile** – Choose your country of operation for use of the VoIP settings. Currently only, France, Israel, Japan, Korea, Spain, Taiwan, the UK and the United States are supported.
- **Caller ID** – The telecommunications standard that is supported for the country of chosen operation. (Default: Disabled)
- **Answer Timeout** – The time after which a no answer message is sent to the caller. (Range: 1-300 seconds; Default: 60 seconds)

- **Dial Tone Timeout** – The length of time a dial tone is heard on a connected phone. (Range: 1-300 seconds; Default: 16 seconds)
  
- **Inter Digit Timeout** – The maximum time delay allowed between each dialed digit. When the time is exceeded, a call is made using the dialed digits. (Range: 1-300 seconds; Default: 2 seconds)
  
- **Line Echo Cancellation** – Sets the delay time for voice echo cancellation. A voice echo can be created on some two-wire phone loops, which becomes increasingly louder and annoying when there is a long delay. If voice echo is a problem during a call, you can adjust this parameter to try and reduce or remove it. (Default: Enabled)
  
- **VAD/CNG** – Voice Activity Detection/Comfort Noise Generator. VAD enables the detection of periods of silence in the audio stream so that it is not transmitted over the network. CNG then inserts artificial noise during silent intervals in the audio stream. (Default: Enabled)



Chapter

8

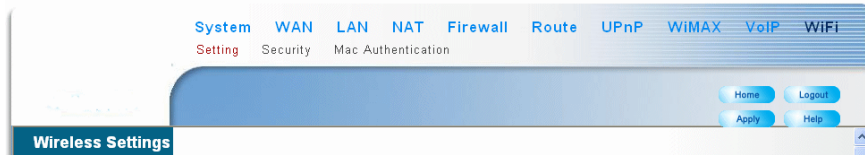
WiFi Settings

## In This Chapter:

- “Introduction” on page 102
- “Wireless Settings” on page 103
- “Wireless Security” on page 107
- “MAC Authentication” on page 110

## 8.1 Introduction

The BreezeMAX Si 2000 model for the 3.5 GHz WiMAX band includes an IEEE 802.11g radio interface for local Wi-Fi communications. The Wi-Fi set up pages include configuration options for the radio signal characteristics and Wi-Fi security.



**Figure 8-1: WiFi Menu**

## 8.2 Wireless Settings

From the Wireless menu, click on Settings to configure the unit's Wi-Fi radio interface. The unit's radio can operate in two modes, IEEE 802.11b & g and 802.11b only.

The IEEE 802.11g standard operates within the 2.4 GHz band at up to 54 Mbps. Note that because the IEEE 802.11g standard is an extension of the IEEE 802.11b standard, it allows clients with 802.11b wireless network cards to associate to an 802.11g access point.

**Figure 8-2: Wireless Settings**

- **Interface Status** – Enables the Wi-Fi radio.
- **Country Code** – Enables to select the parameter set (list of parameters per country regulations) by which various parameters are defined. (Default: United States)
- **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: default)
- **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: 1-11)

**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. Channels 1, 6, and 11, as the three non-overlapping channels in the 2.4 GHz band, are preferred.

- **Auto Channel Select** – Enables the unit to automatically select an available radio channel. (Default: Enabled)
  
- **Working Mode** – Selects the operating mode for the 802.11g radio. (Default: B/G Mixed Mode)
  - » B/G Mixed Mode: Both 802.11b and 802.11g clients can communicate with the unit (up to 54 Mbps).
  - » B Only Mode: Both 802.11b and 802.11g clients can communicate with the unit, but 802.11g clients can only transfer data at 802.11b standard rates (up to 11 Mbps).
  
- **Transmit Power** – Adjusts the power of the radio signals transmitted from the unit. The higher the transmission power, the farther the transmission range. Power selection is not just a trade off between coverage area and maximum supported clients. You also have to ensure that high-power signals do not interfere with the operation of other radio devices in the service area. (Options: Auto, Full, Min; Default: Auto)
  
- **Tx Data Rate** – The maximum data rate at which the unit transmits unicast packets on the Wi-Fi interface. The maximum transmission distance is affected by the data rate. The lower the data rate, the longer the transmission distance. (Default: Auto)
  
- **RTS Threshold (256~2432)** – Sets the packet size threshold at which a Request to Send (RTS) signal must be sent to a receiving station prior to the 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 Protection 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 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 2000. (Default:CTS Only)
  - » **Disable:** If there are no 802.11b clients in the network, the protection mode can be disabled.
  - » **CTS Only:** The transmitting client sends only 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.
  - » **RTS/CTS:** 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 (96 microseconds) instead of a long preamble (192 microseconds) can increase data throughput on the unit, but requires that all clients can support a short preamble. (Default: Short)
  - » **Short:** Sets the preamble to short for increased throughput.
  - » **Long:** Sets the preamble to long. Using a long preamble ensures the unit can support all 802.11b and 802.11g clients.
  
- **SSID Suppress** – When enabled, the BreezeMAX Si 2000 stops broadcasting the configured SSID in its beacon signal. 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 2000. 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 2000.

- **Factory Default** – Click the Reset button to set all the Wi-Fi settings to their factory default values.

## 8.3 Wireless Security

The BreezeMAX Si 2000 Wi-Fi interface 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 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.
- Traffic Encryption – Data passing between the unit and clients must be protected from interception and eavesdropping.

For a more secure network, the BreezeMAX Si 2000 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.

To configure wireless security click on Security.

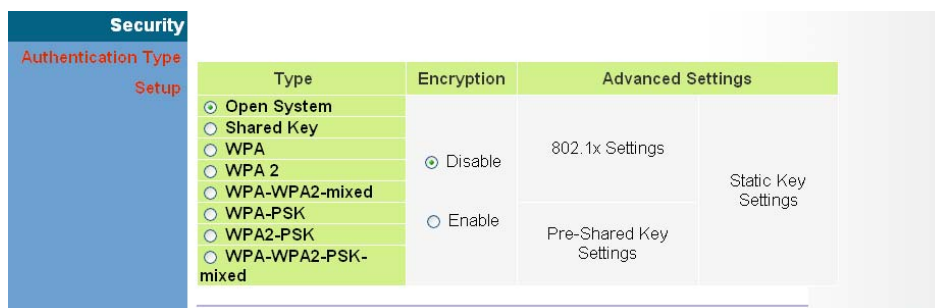


Figure 8-3: Wireless Security

### 8.3.1 Wireless Security

There are eight security options available. When you select the security type in the table, 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.

The following sections describe the security options available for the BreezeMAX Si 2000 Wi-Fi network.

## 8.3.2 WEP Shared Key Security

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 2000. 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

**Security**

**Authentication Type Setup**

Type	Encryption	Advanced Settings
<input type="radio"/> Open System	<input type="radio"/> Disable	802.1x Settings
<input checked="" type="radio"/> Shared Key		
<input type="radio"/> WPA	<input checked="" type="radio"/> Enable	Pre-Shared Key Settings
<input type="radio"/> WPA 2		
<input type="radio"/> WPA-WPA2-mixed		
<input type="radio"/> WPA-PSK		
<input type="radio"/> WPA2-PSK		
<input type="radio"/> WPA-WPA2-PSK-mixed	<a href="#">Static Key Settings</a>	

**Static Key Settings**

Key Number	Key 1	Key 2	Key 3	Key 4
<b>Key Type</b>	<input checked="" type="radio"/> hex <input type="radio"/> ascii			
<b>Key Length</b>	<input checked="" type="radio"/> 64bits <input type="radio"/> 128bits <input type="radio"/> 152bits	<input checked="" type="radio"/> 64bits <input type="radio"/> 128bits <input type="radio"/> 152bits	<input checked="" type="radio"/> 64bits <input type="radio"/> 128bits <input type="radio"/> 152bits	<input checked="" type="radio"/> 64bits <input type="radio"/> 128bits <input type="radio"/> 152bits
<b>Key</b>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Hex: For 64 Bits enter 10 digits, for 128 Bits enter 26 digits, for 152 Bits enter 32 digits  
 Ascii: For 64 Bits enter 5 characters, for 128 Bits enter 13 characters, for 152 Bits enter 16 characters

**Default Key Setting**

Key 1    Key 2    Key 3    Key 4

**Figure 8-4: WEP Shared Key Security**

■ **Key 1 ~ Key 4** – Sets WEP key values. 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, 64 bits, no preset value)

- » **Key Type:** Specifies keys as either ASCII or Hexadecimal values.
- » **Key Length:** WEP keys can be set as 64, 128, or 152 bits in length.
- » **Key:** Specify keys as either 5, 13, or 16 alphanumeric characters, or 10, 26, or 32 hexadecimal digits, depending on the selected key length.

- **Default Key Setting** – Sets the WEP key used for authentication and encryption. (Range: 1-4; Default: 1)

### 8.3.3 WPA/WPA2 Security

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.

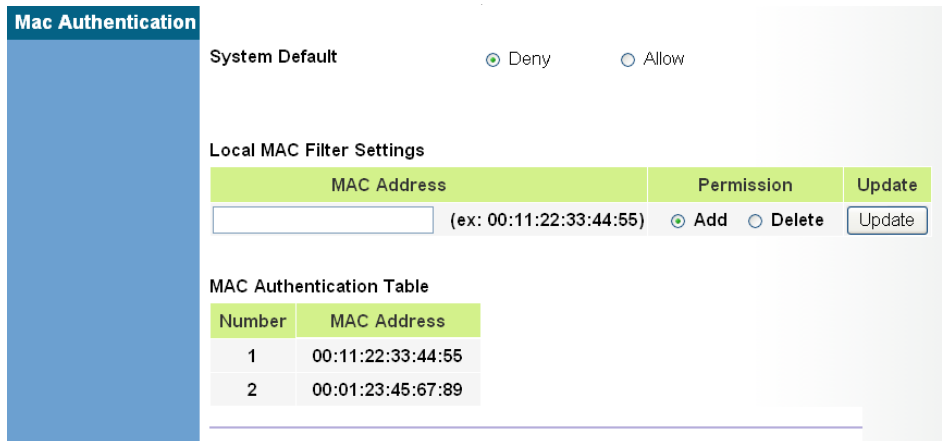
The screenshot shows the 'Security' configuration page. On the left, there is a sidebar with 'Authentication Type Setup' and 'Pre-Shared Key Settings'. The main content area is divided into three columns: 'Type', 'Encryption', and 'Advanced Settings'. Under 'Type', several radio buttons are listed, with 'WPA-WPA2-PSK-mixed' selected. Under 'Encryption', the 'Enable' radio button is selected. The 'Advanced Settings' column contains links for '802.1x Settings', 'Static Key Settings', and 'Pre-Shared Key Settings'. Below this, the 'WPA Pre-Shared Key' section features a text input field and instructions: 'Hex: Enter 64 digits' and 'Ascii: Enter between 8 and 63 characters'.

Figure 8-5: WPA/WPA2 PSK Security

- **WPA Pre-Shared Key** – The key required for WPA-PSK, WPA2-PSK, and WPA-WPA2-Mixed-PSK modes. There are two methods for key entry: An ASCII string of 8~63 characters in length (0~9, A~F, including spaces), or 64 hexadecimal digits.

## 8.4 MAC Authentication

Wireless clients can be authenticated for network access by checking their MAC address against a local database configured on the BreezeMAX Si 2000. You can configure a list of up to 32 wireless client MAC addresses in the filter list to either allow or deny network access.

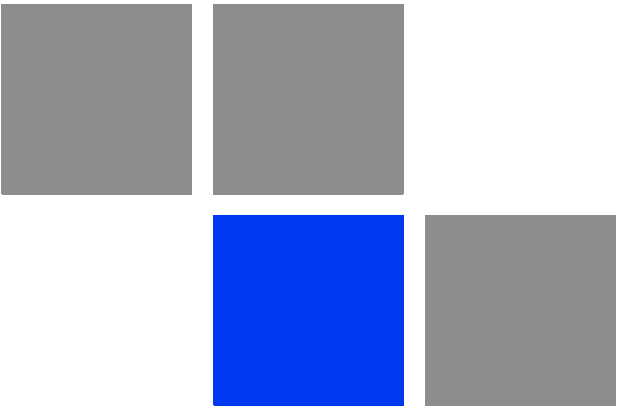


**Figure 8-6: MAC Authentication**

- **System Default** – Specifies the action for MAC addresses listed in the local MAC Authentication Table.
  - » **Deny:** Blocks access for all MAC addresses listed in the MAC Authentication Table. Clients with MAC addresses not listed in the table are permitted access.
  - » **Allow:** Permits access for all MAC addresses listed in the MAC Authentication Table. Clients with MAC addresses not listed in the table are denied access.

- **Local MAC Filter Settings** – Adds new MAC addresses to the MAC Authentication Table, or removes addresses currently listed in the table.
  - » **MAC Address:** Physical address of a client. Enter six pairs of hexadecimal digits separated by colons; for example, 00:90:D1:12:AB:89.
  - » **Permission:** Select Add to list a new specified MAC address in the MAC Authentication Table. Select Delete to remove the specified MAC address from the table.
  - » **Update:** Performs the Add or Delete action on the specified MAC address.
  
- **MAC Authentication Table** – Displays current entries in the MAC filter database.





## In This Chapter:

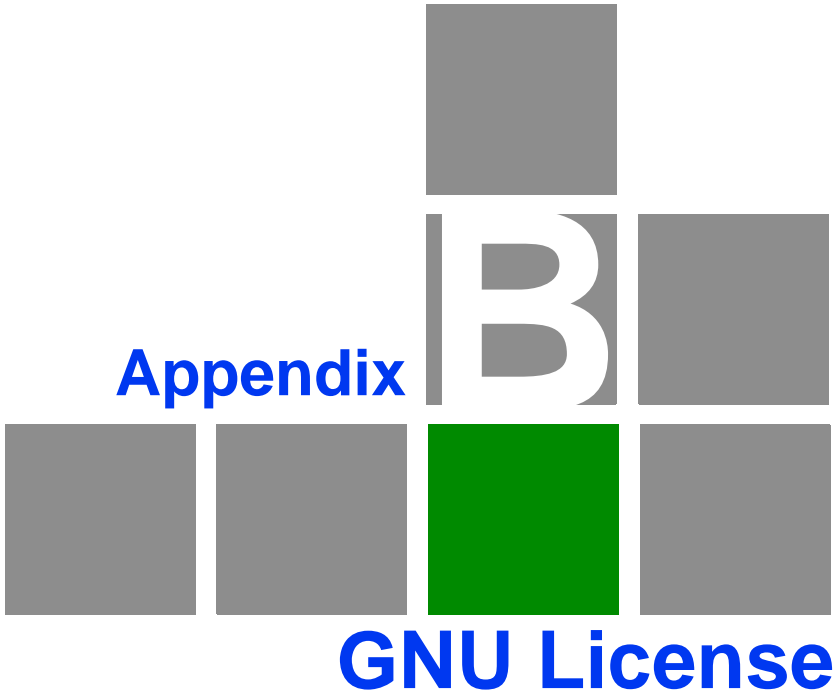
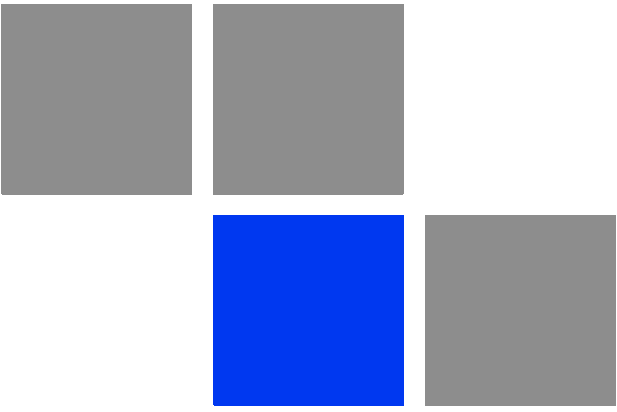
This section provides a lists of things to check in case of problems before contacting local Technical Support.

Check the following before you contact local Technical 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 back panel for 5 seconds or more. Then use the default password “admin” to access the management interface.
- 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 back panel for 5 seconds or more. Then use the default password “admin” to access the management interface.

Table A-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>■ Power LED is Red</li></ul>	<ul style="list-style-type: none"><li>■ The unit has detected a system error. Reboot the unit to try and clear the condition.</li><li>■ If the condition does not clear, contact your local dealer for assistance.</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 LEDs are Off</li></ul>	<ul style="list-style-type: none"><li>■ Move the location of the unit.</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>



## In This Chapter:

This product includes copyrighted third-party software subject to the terms of the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other related free software licences. The GPL code used in this product is distributed WITHOUT ANY WARRANTY and is subject to the copyrights of one or more authors. For details, refer to the section “The GNU General Public License” below, or refer to the applicable licence as included in the source-code archive.

This section summarizes the terms and conditions of use of the GNU license that applies to the software on the BreezeMAX Si 2000.

## B.1 The GNU General Public License

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

### B.1.1 Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

## B.1.2 GNU General Public License Terms and Conditions for Copying, Distribution and Modification

This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.



You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted

herein. You are not responsible for enforcing compliance by third parties to this License.

If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of

any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

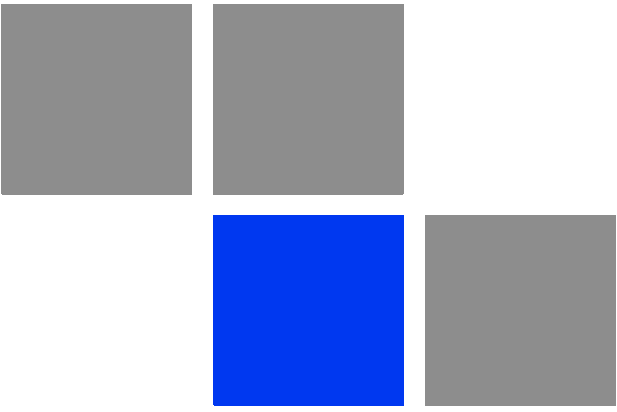
If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

#### NO WARRANTY

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS



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>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>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>Customer Premise Equipment (CPE)</b>	Customer Premise Equipment: Communications equipment that resides on the customer's premises.
<b>Domain Name System (DNS)</b>	A system used for translating host names for network nodes into IP addresses.
<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>Ethernet</b>	A popular local area data communications network, which accepts transmission from computers and terminals.
<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>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>IEEE 802.16e</b>	A standard that provides mobile broadband wireless access using Scalable Orthogonal Frequency Division Multiple Access (SOFDMA).
<b>Local Area Network (LAN)</b>	Local Area Network: A group of interconnected computer and support devices.
<b>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>Network Time Protocol (NTP)</b>	NTP provides the mechanisms to synchronize time across the 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>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>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>RTS Threshold</b>	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.
<b>Service Set Identifier (SSID)</b>	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).
<b>Session Key</b>	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.
<b>Shared Key</b>	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.
<b>Simple Network Management Protocol (SNMP)</b>	Simple Network Management Protocol: The application protocol in the Internet suite of protocols which offers network management services.
<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>Subscriber Station</b>	A general term for a customer’s WIMAX terminal equipment that provides connectivity with a base station.
<b>Trivial File Transfer Protocol (TFTP)</b>	Trivial File Transfer Protocol: A TCP/IP protocol commonly used for software downloads.
<b>UTP</b>	Unshielded twisted-pair cable.
<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.