alvarion®
Your Open WiMAX Choice

BreezeMAX® Si 4000 CPE

Operator Manual

Software Version: 1.0
March 2010
P/N 215634

Document History

Topic	Description	Date Issued
BreezeMAX Si 4000 CPE Manual	This is the document's first release.	March 2010

Legal Rights

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

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

Trade Names

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

All other names are or may be the trademarks of their respective owners.

“WiMAX Forum” is a registered trademark of the WiMAX Forum. “WiMAX,” the WiMAX Forum logo, “WiMAX Forum Certified,”andtheWiMAX Forum Certified logo are trademarks of the WiMAX Forum.

Statement of Conditions

The information contained in this manual is subject to change without notice. Alvarion Ltd. shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or equipment supplied with it.

Warranties and Disclaimers

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

Exclusive Warranty

(a) Alvarion warrants that the Product hardware it supplies and the tangible media on which any software is installed, under normal use and conditions, will be free from significant defects in materials and workmanship for a period of fourteen (14) months from the date of shipment of a given Product to Purchaser (the “Warranty Period”). Alvarion will, at its sole option and as Purchaser's sole remedy, repair or replace any defective Product in accordance with Alvarion' standard R&R procedure.

(b) With respect to the Firmware, Alvarion warrants the correct functionality according to the attached documentation, for a period of fourteen (14) month from invoice date (the “Warranty Period”). During the Warranty Period, Alvarion may release to its Customers firmware updates, which include additional performance improvements and/or bug fixes, upon availability (the “Warranty”). Bug fixes, temporary patches and/or workarounds may be supplied as Firmware updates.

Additional hardware, if required, to install or use Firmware updates must be purchased by the Customer. Alvarion will be obligated to support solely the two (2) most recent Software major releases.

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

Disclaimer

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

(b) PURCHASER'S SOLE REMEDY FOR BREACH OF THE EXPRESS WARRANTIES ABOVE SHALL BE REPLACEMENT OR REFUND OF THE PURCHASE PRICE AS SPECIFIED ABOVE, AT ALVARION'S OPTION. TO THE

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

Limitation of Liability

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

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

Electronic Emission Notices

This device complies with Part 15 of the FCC rules.

Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

FCC Radiation Hazard Warning

To comply with FCC RF exposure requirements in Section 1.1307 and 2.1091 of FCC Rules, the antenna used for this transmitter must be kept at a separation

distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

Radio Frequency Interference Statement

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

R&TTE Compliance Statement

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

Caution

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

Line Voltage

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

Radio

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

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^{6+})	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 manual is delivered subject to the following conditions and restrictions:

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

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

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

About This Manual

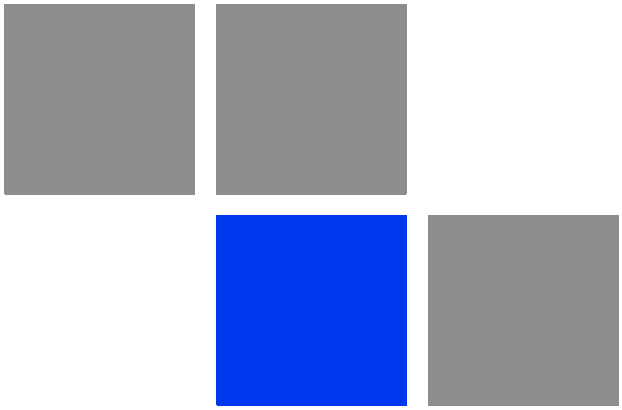
This manual describes the BreezeMAX Si 4000 CPEand details how to install, operate and manage it.

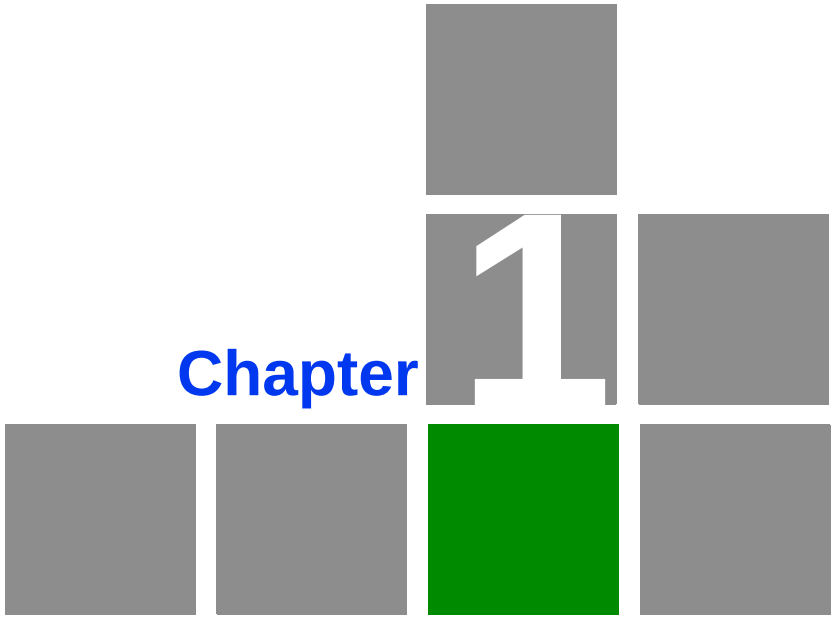
This manual is intended for operators responsible for installing, setting and operating the system, and for system administrators and product experts responsible for managing the system.

This manual contains the following chapters and appendices:

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

Contents





Chapter 1
Product Description

In This Chapter:

1.1 Introducing the BreezeMAX Si 4000

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

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

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

The BreezeMAX Si 4000 is a plug-and-play indoor unit (IDU) that is available in two WiMAX licensed frequency bands: 2.5 GHz and 3.5 GHz (See “The BreezeMAX Si 4000 Family of Products” on page 4). The model you use depends on the frequency band of your service provider’s WiMAX service.

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

The BreezeMAX Si 4000 includes one RJ-45 Ethernet switch port10/100 auto-sensing, auto-MDX) for LAN connection and one RJ-11 Voice over IP (VoIP) phone port. An 802.11b/g Wi-Fi module is included for providing a local WiFi access point service. The BreezeMAX Si 4000 unit also includes built-in omnidirectional WiMAX antennas for WiMAX communication.

Figure 1-1: The BreezeMAX Si 4000 CPE

1.1.1 The BreezeMAX Si 4000 Family of Products

The following table lists the available BreezeMAX Si 4000 models:

Table 1-1: BreezeMAX Si 4000 Models

Frequency Band	Model Number	Ports
2.5 GHz	4M-CPE4000-Si-1D-1V-2.5	■ 1 data port (RJ-45) ■ 1 VoIP phone port (RJ-11)
3.5 GHz	4M-CPE4000-Si-1D-1V-3.5	■ 1 data port (RJ-45) ■ 1 VoIP phone port (RJ-11)
	4M-CPE4000-Si-1D-1V-WiFi-3.5	■ 1 data port (RJ-45) ■ 1 VoIP phone port (RJ-11) ■ 1 WiFi (802.11b/g) port

1.1.2 Product Features

The BreezeMAX Si 4000 supports the following features:

- WiMAX 802.16-2005 Wave2 Standard Compliant Air Interface
- WiFi (for 5.5 GHz models)
- Dynamic Host Configuration Protocol (DHCP)
- Built-in web server for web-based configuration
- Dual image firmware crash protection
- Password protected access and configuration
- Auto-provisioning with remote firmware upgrade
- IEEE 802.3, IEEE 802.3u
- Gateway mode
- Bridge mode for Management and VoIP
- Voice over IP
- VPN pass-through

1.2 Safety Information

CAUTION

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

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

1.3 Specifications

1.3.1 General

Table 1-2: General Specifications

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

1.3.2 WiMAX Radio

Table 1-3: WiMAX Radio Specifications

Item	Description
Radio Type	IEEE 802.16e 2005 WAVE 2
Frequency Band	■ 2.5 GHz - 2485~2690 MHz ■ 3.5 GHz - 3400~3600MHz
Antenna Type	High gain widebeam antenna

Table 1-3: WiMAX Radio Specifications

Item	Description
Channel Bandwidth	2.5GHz - 5.00 and 10.00 MHz 3.5GHz - 5.00, 7.00, and 10.00 MHz
Modulation Technique	■ Scaleable OFDMA employing Time-Division Duplex (TDD) mechanism ■ PRBS subcarrier randomization ■ Contains pilot, preamble, and ranging modulation
FEC Coding Rates	■ Up Link and Down Link: QPSK, 16 QAM, 64 QAM ■ QPSK and 16QAM - 1/2 and 3/4 ■ 64QAM - 1/2, 2/3, 3/4, 5/6
TPL (Transmit Power Level)	27 dBm typical (maximum)
Transmit Power Dynamic Range	45 dB
Channel Step Size	In 250 kHz steps
Synchronization	Shall be referenced to the WiMAX BTS Timing Module
Frequency Accuracy	MRCT Compliant
Air Interface	IEEE 802.16e Wireless MAN-OFDMA
TDD Duty Cycle (Tx/Rx)	Rx up to 75% , Tx up to 50%
SISO or MIMO	MIMO (1TX, 2RX)
Regulatory Compliance	FCC parts 15, 25, 27
Frame Duration	5 msec;
RF Transmitter Specifications	
RF dynamic range	45dB minimum
Transmit Power Control Relative Accuracy	mRCT compliant
Transmit and Receive Switching Gap	50 µS
RF Receiver Specifications	
Impedance	50 ohms nominal
Input return loss	10dBi
RX Sensitivity	Typical 3dB better than mRCT in SISO mode, and 6 dB better in MRC or MIMO mode. -94.5 dBm maximum.

Table 1-3: WiMAX Radio Specifications

Item	Description
Adjacent Channel Rejection	4dB min. Receive signal 64QAM-3/4, 3dB above sensitivity level.
Non-Adjacent Channel Rejection	23dB min Receive signal 64QAM-3/4, 3dB above sensitivity level.
Antenna Specifications	
Antenna Gain	Typical 5dBi
Antenna Connectors	None. Embedded IPEX

1.3.3 WiFi Radio

NOTE

This section only applies to the 4M-CPE4000-Si-1D-1V-WiFi-3.5 model.

Table 1-4: WiFi Radio Specifications

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

1.3.4 VoIP Specifications

Table 1-5: VoIP Specifications

Item	Description
Voice Signalling Protocol	■ SIP v2 (RFC 3261) ■ SDP (RFC2327) ■ RTP/RTCP (RFC 1889/RFC 1890)

Table 1-5: VoIP Specifications

Item	Description
Voice Codecs	■ g711 (a-law and u-law) ■ g729a/b ■ g723 ■ ILBC
Voice Quality	■ VAD (Voice Activity Detection) ■ Echo cancellation (G.168) ■ Adaptive jitter buffer ■ DTMF tone detection and generation
Call Features	■ Call ID ■ Outgoing caller ID block ■ Call transfer (blind/consultive) ■ Call waiting/hold/retrieve ■ Call waiting cancelation ■ Anonymous incoming call blocking ■ T.38 fax relay ■ Dial plan ■ Call forwarding: No Answer/Busy/All ■ Do not disturb ■ Redial/Redial on busy ■ Automatic call return ■ MWI and VMWI - message waiting indication

1.3.5 Configuration and Management

Table 1-6: Configuration and Management

Item	Description
Management options	■ Web-based (HTTP/HTTPS) ■ TR-069

1.3.6 Mechanical

Table 1-7: Mechanical Specifications

Item	Description
Dimensions	232(H)*142(W)*36(D) mm
Weight	0.59 kg
Mounting	Desktop

1.3.7 Electrical

Table 1-8: Electrical Specifications

Type	Details
AC Power Supply	Input: 100-240 VAC, 50-60 Hz, maximum power consumption 0.5A Output: 12 VDC, maximum power consumption 3.4A

1.3.8 Environmental

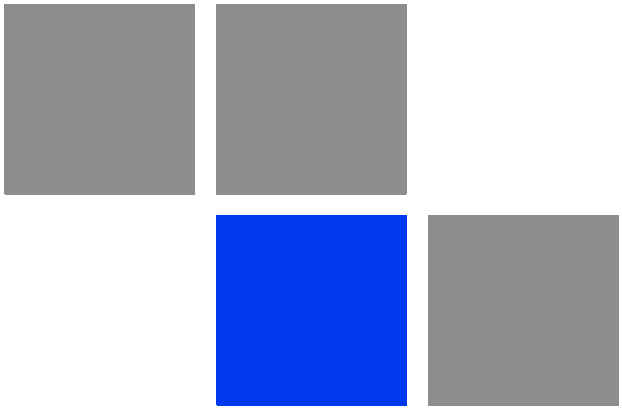
Table 1-9: Environmental Specifications

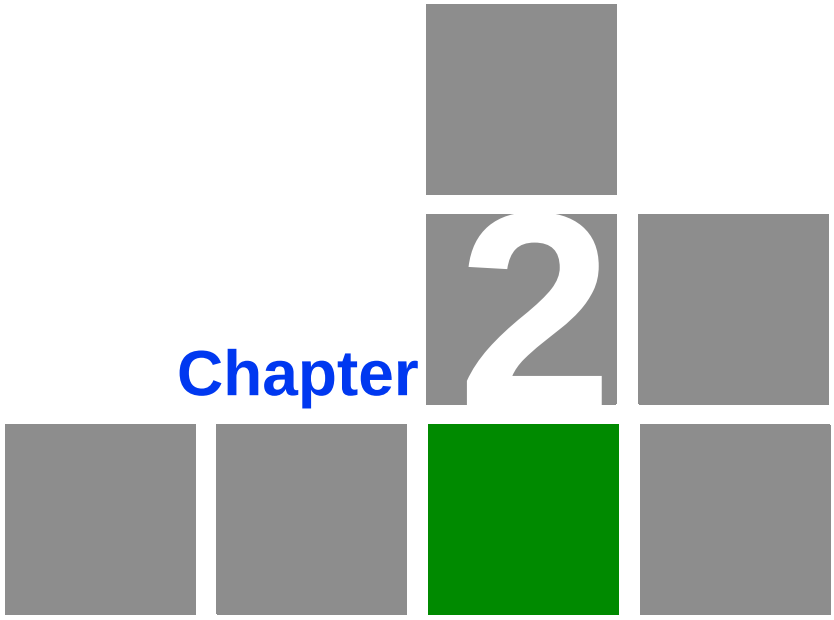
Item	Details
Operating Temperature	0ºC to 40ºC
Storage Temperature	-20 to 55 °C
Humidity	Maximum 95%, non-condensing

1.3.9 Standards Compliance

Table 1-10: Standards Compliance

Type	Standard
EMC	■ FCC Part 15B ■ ETSI EN 301 489
Safety	■ UL 60950-1 ■ IEC 60950-1 ■ EN 60950-1
Radio	■ ETSI EN 302 623 ■ ETSI EN 300 328 ■ FCC 04-135, Part 15,25, 27 ■ EN 302 544
Standards	■ IEEE 802.16e-2005 WAVE 2 ■ IEEE 802.3-2005 10BASE-T and 100BASE-TX ■ IEEE 802.3u ■ IEEE 802.11b and 802.11g





Chapter 2

CPE Installation

In This Chapter:

2.1 Installation Requirements

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

2.1.1 Package Content

The BreezeMAX Si 4000package includes the following components:

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

2.2 Installation Procedure

CAUTION

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

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

2.2.1 Guidelines for Positioning the Unit

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

- Select a cool, dry place, which is out of direct sunlight. To improve overall performance, choose an upper floor location near a window or outside wall.
- Leave adequate space (approximately 2”/5 cm) on all sides for proper air flow.
- Locate the unit near an AC power outlet that provides 100V to 240V.
- Avoid metal obstacles such as furniture, office equipment or metal film anti-glare windows in the transmission path.
- Position the unit at least 6.5 feet/2 meter away from any WiFi device (if used), to avoid interference.

2.2.2 Installing the Unit

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

1. Place the unit on a flat horizontal surface indoors. Use the rotating base to stabilize the device.
2. Connect the power cable to the power jack located on the rear panel of the unit. Connect the other end of the power cord to the AC mains. The unit will take 1-2 minutes to boot up and find a nearby base station signal.

CAUTION

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

3 Observe the Indicator LEDs. When you power on the BreezeMAX Si 4000, verify that the Power LED turns on and that the other LED indicators start functioning as described in Table 2-1 and Table 2-2.

4 Do one or both of the following:

» Connect your PC - Connect a Category 5 or better Ethernet cable to the BreezeMAX Si 4000's LAN port and the other end to the network port of your PC. Alternatively, you can connect the LAN port to an Ethernet switch or other devices. Make sure the length of each cable does not exceed 100 meters (328 ft).

» Connect your PC using WiFi (if available) - Click the WiFi icon  (lower right corner of PC); Click Find WLAN. Click the name of WiFi network and click Connect.

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

5 Align the unit so that you receive the strongest signal by monitoring the WiMAX LEDs on the front panel of the unit.

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

NOTE

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

6 Connect a standard (analog) telephone set to the BreezeMAX Si 4000's VoIP port using standard telephone cable with RJ-11 plugs.
The BreezeMAX Si 4000 enables VoIP calls to be made through the unit using a standard (analog) telephone set connected to a VoIP port. Standard Session Initiation Protocol (SIP) technology is used to make VoIP calls. You must access the web interface and configure settings for your SIP service provider before you can make VoIP calls. The VoIP service may be configured remotely or locally by web.

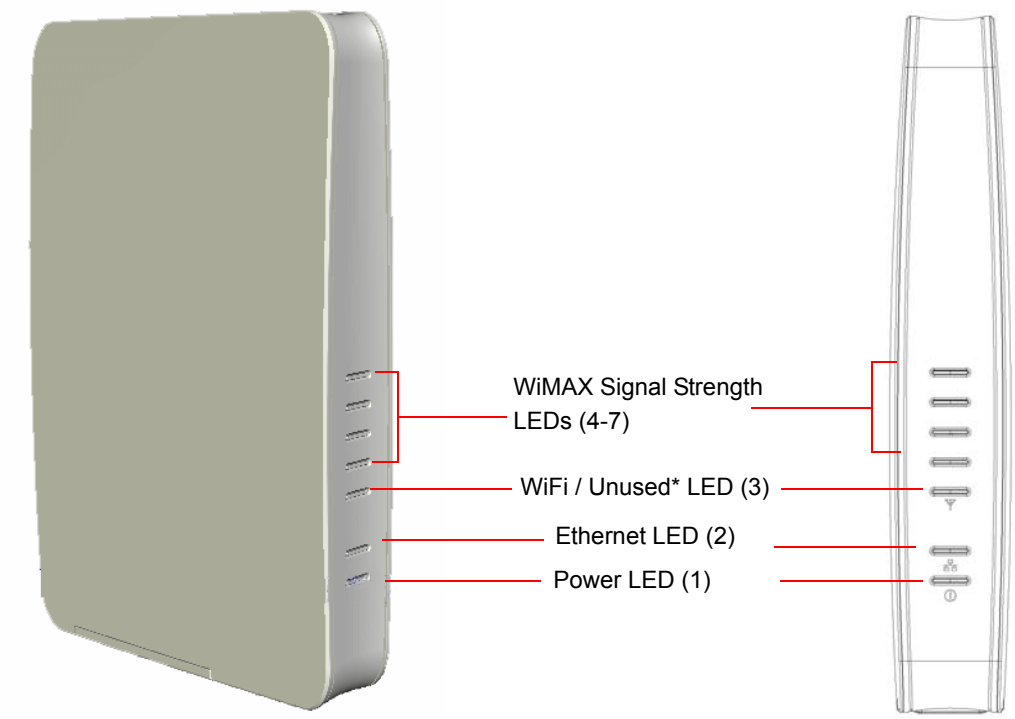
7 If your unit is supplied with a CDROM, insert it to the CDROM drive, run the *CPEAutoConfigTool.exe* program and follow the procedure described in "Configuring the CPE Using the WiMAX Modem Application CD" on page 31.

8 Use your PC's web browser to access the unit's management interface and make any configuration changes. For more information, see "Commissioning" on page 24.

2.3 BreezeMAX Si 4000 Hardware Description

2.3.1 Front Panel

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



* WiFi LED (3) in 3.5 GHz models, unused LED in 2.5 GHz models

Figure 2-1: BreezeMAX Si 4000Front Panel

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

LED	Color	Status	Description
Power (1)	Blue	Off	Power off
		On	Power on

Table 2-1: LEDs Status Indications - 2.5 GHz Models (Continued)

LED	Color	Status	Description
Ethernet (2)	Green	Off	LAN device is disconnected
		On	LAN device is connected
		Blinking	Data packet transmission
Unused LED (3)	Green	N/A	N/A
WiMAX Link Status (4)	Green	On	CPE is connected to a base station
		Off	CPE is not connected to a base station
WiMAX Link Status (5)	Green	On	3≤CINR
WiMAX Link Status (6)	Green	On	9≤CINR
WiMAX Link Status (7)	Green	On	14≤CINR

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

LED	Color	Status	Description
Power (1)	Blue	Off	Power off
		On	Power on
Ethernet (2)	Green	Off	LAN device is disconnected
		On	LAN device is connected
		Blinking	Data packet transmission
Wi-Fi (3)	Green	Off	Wi-Fi disabled
		On	Wi-Fi enabled
WiMAX Link Status (4)	Green	On	CPE is connected to a base station
		Off	CPE is not connected to a base station
WiMAX Link Status (5)		On	3≤CINR
WiMAX Link Status (6)		On	9≤CINR
WiMAX Link Status (7)		On	14≤CINR

2.3.2 Rear Panel

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

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

Table 2-3: BreezeMAX Si 4000 Connectors

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

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

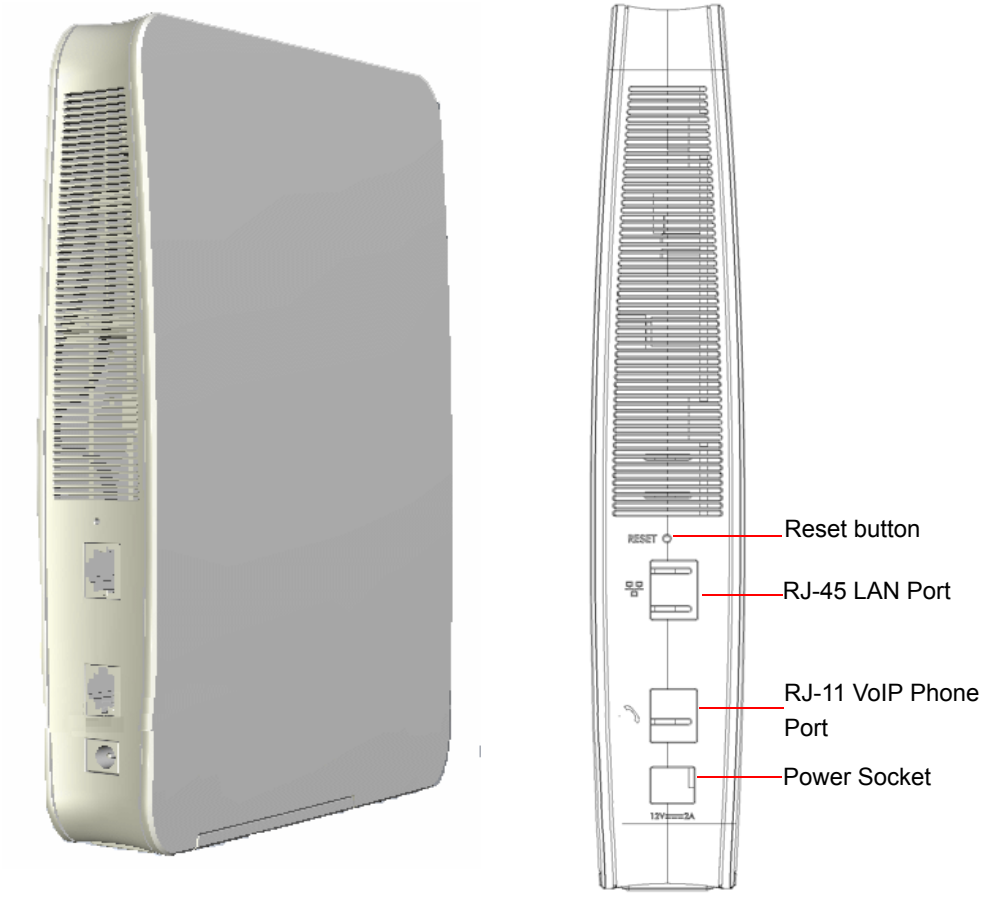


Figure 2-2: BreezeMAX Si 4000 Rear Panel

2.3.3 Reset Button

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

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

2.3.4 WiMAX Antennas

Two built-in omnidirectional antennas are included with the BreezeMAX Si 4000 for WiMAX communications. The omnidirectional antennas transmit and receive signals in all directions equally.

2.3.5 BreezeMAX Si 4000Cables

NOTE

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

Use only Category 5E Ethernet cables from either Alvarion or any of the approved manufacturers, listed in Table 2-4. Consult with Alvarion's specialists on the suitability of other cables.

Table 2-4: Approved Category 5E Ethernet Cables

Manufacturer	Part Number
Superior Cables Ltd. www.superior-cables.com	612098
HES Cabling Systems www.hescs.com	H5E-00481
Teldor www.teldor.com	8393204101

Table 2-4: Approved Category 5E Ethernet Cables

Manufacturer	Part Number
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: eva@south-bay.com.tw	TSM2404A0D
GU-Tech., LLC . - A Member of OVIS GroupTel/Fax : 732 918 8221 Mobile: 718 909 4093 www.OVIS.COM.TW www.GU-TECH.COM	

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

2.3.6 BreezeMAX Si 4000Wi-Fi Option

The BreezeMAX Si 40003.5 GHz model includes the 802.11b/g Wi-Fi option. This unit includes internal antennas for local wireless connections to PCs.

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

Chapter 3

Commissioning

In This Chapter:

3.1 Introduction

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

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

The following methods are available for configuring the BreezeMAX Si 4000:

- The web-based management interface - accessed using a PC/Notebook with a web browser (see "Configuring the CPE Using the Web Management Interface" on page 28).
- An automatic configuration tool provided on a CDROM for the subscribers (see "Configuring the CPE Using the WiMAX Modem Application CD" on page 31).
- Upgrading the CPE using an auto-configuration file, or IPKG (in **.ipk* format) (see "Configuring the CPE Using the IPKG Upgrade" on page 35).

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

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

Table 3-1: Basic Parameters

Item	Default Value	Comment
User Name (WiMAX)	WAN mac address and WiMax.com realm, e.g: 0026824EE12C@WiMax.com	Should be supplied by system administrator. Configured in the Internet> Security> Authentication window
WiMAX Password	quickynikynyoky	
Domain	wimax.com (also Eng > WiMAX Config > Realm	
Frequency		Should be supplied by system administrator.

Table 3-1: Basic Parameters

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

3.2 Configuring the CPE Using the Web Management Interface

The BreezeMAX Si 4000 supports multi-user permissions: Operator and Subscriber modes are available by downloading different configuration files (IPKGs) from the web and upgrading the unit. Each level has different permissions to access various pages for configuration.

3.2.1 Accessing the Web Management Interface

BreezeMAX Si 4000has the default IP address 192.168.254.251 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 4000 (that is, the PC's IP address starts with 192.168.254.x).

To log in:

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

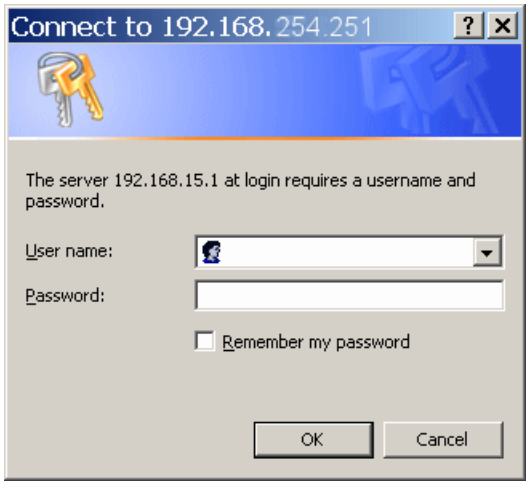


Figure 3-1: Login Window

2 Enter the user name and password, and click **Login**. The default credentials are:

- Username: subscriber
- Password: alvarion

The Status - Device Status page is displayed.

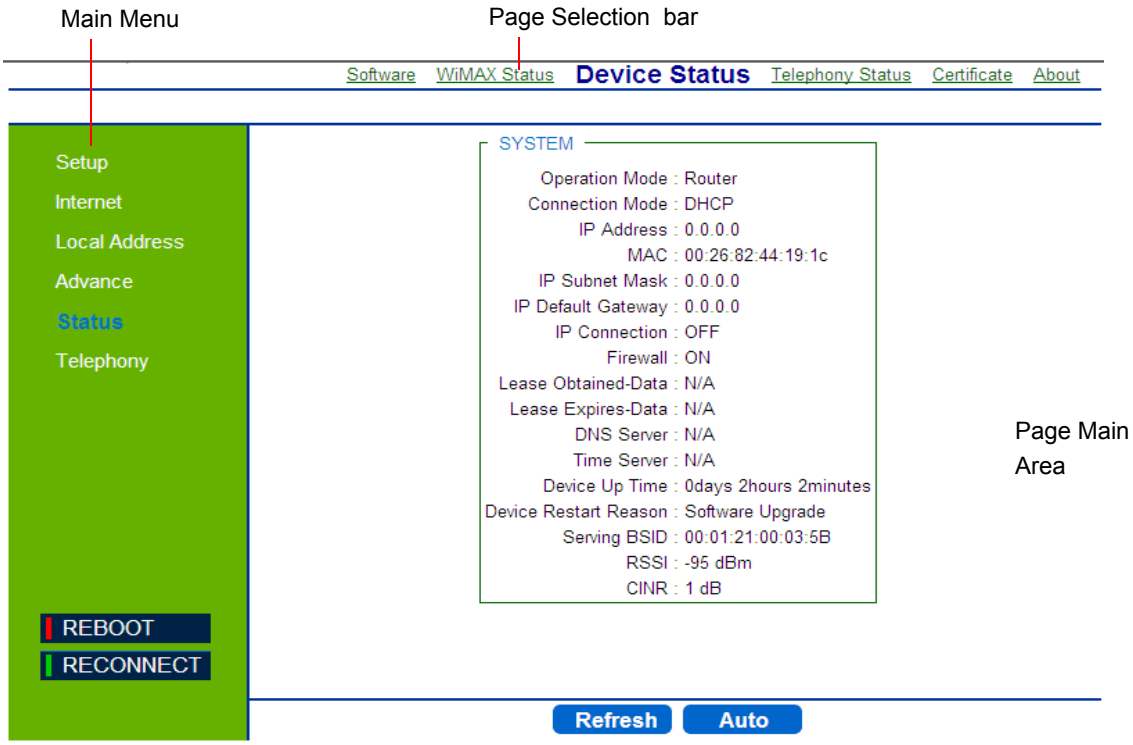


Figure 3-2: Main Window (Device Status)

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

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

In Operator mode only, additional parameters are available in the Engineering menu item, for more detailed configuration. The Engineering features are available in a software package, and can only be activated after uploading it to the system from the Status page See “Software Status” on page 74.

3.2.2 Applying Changes

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

- **Apply** - Click this button to save the changes you have made in each page of the device system.
- **Undo** - Click this button to clear the input data in the specific window.
- **Reboot** - Click this button to restart your unit. The device returns to the last applied settings.
- **Reconnect** - click this button to attempt reconnecting the device to the Base Station. This step is normally not required, unless suspecting that connection is problematic.

3.3 Configuring the CPE Using the WiMAX Modem Application CD

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

To configure the unit using the Auto-Configuration tool:

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

Figure 3-3: Installation Setup Wizard Window

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

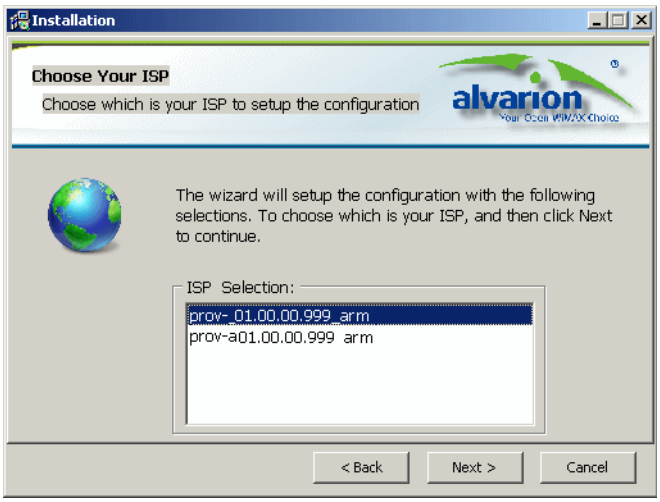


Figure 3-4: Choose Your ISP Window

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

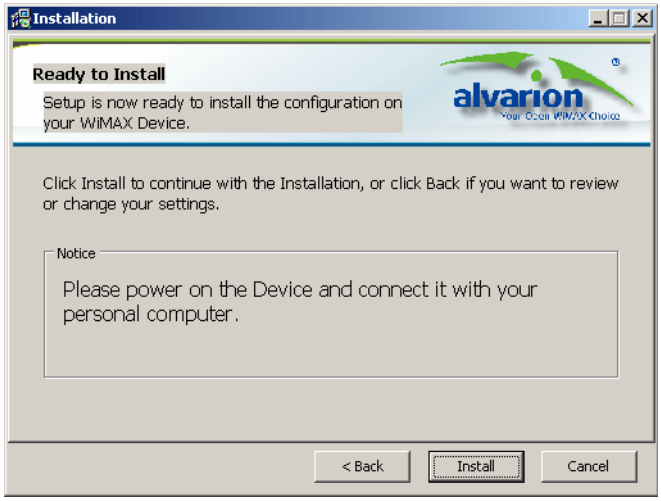


Figure 3-5: Ready To Install Window

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

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

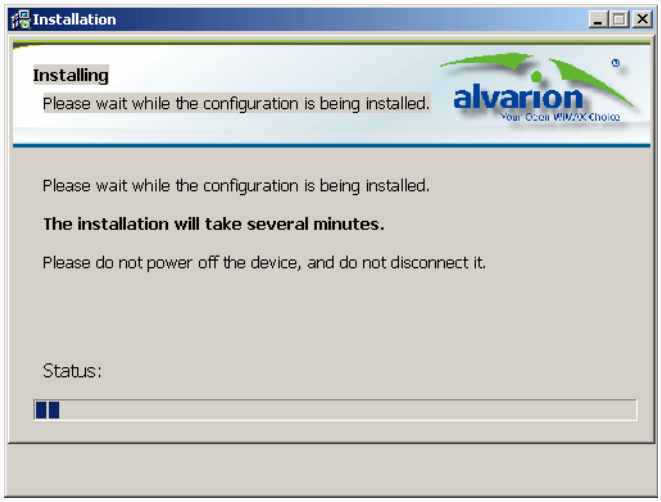


Figure 3-6: Installing Window

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

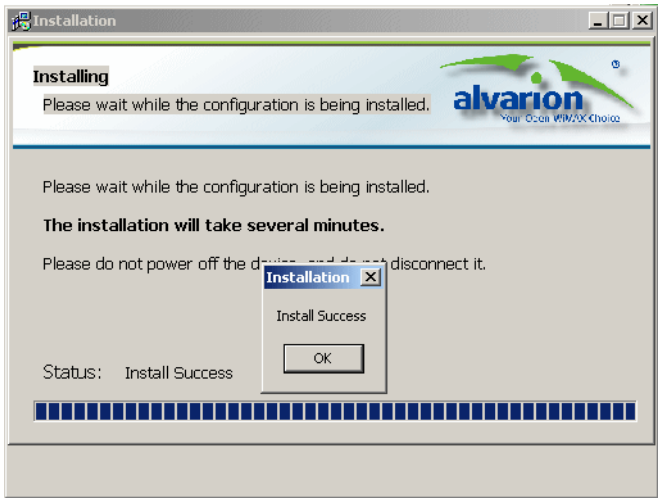


Figure 3-7: Installation Succeeded

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

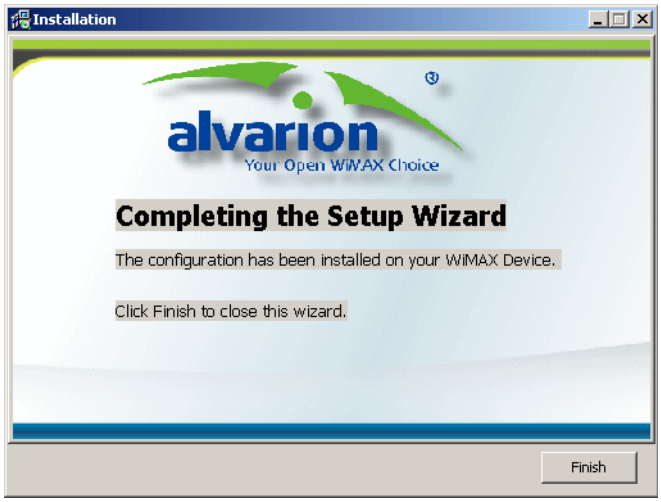


Figure 3-8: Installation Complete

3.4 Configuring the CPE Using the IPKG Upgrade

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

To upgrade the unit using the IPKG:

1. From the main menu at the left pane select **Status** and open the **Software** page (Figure 3-9).
2. Click **Browse** to upload the **ipk* file provided for this unit.
3. Click **Upgrade** to apply all the parameters in the IPKG file to this unit.

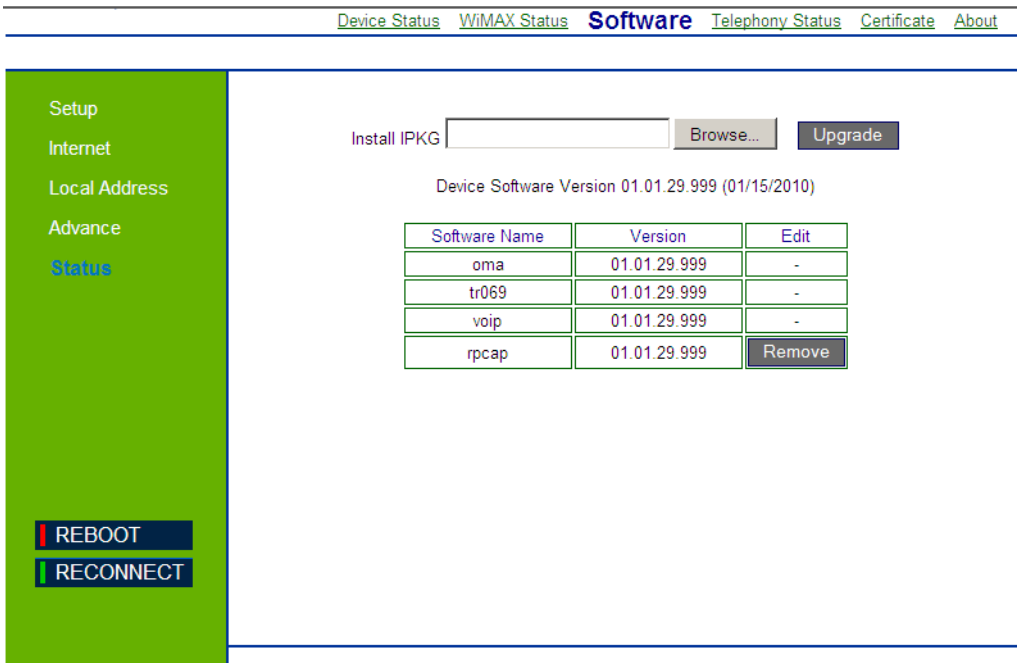


Figure 3-9: Status - Software Page

3.5 Creating a Default Configuration File

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

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

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

To create a configuration **.tar* file:

1. Choose a CPE from which to create the default configuration file.
2. Configure the settings of the CPE as described in this manual.
3. Select **Engineering** from the main menu and open the **Dev Config** page (Figure 3-10).
4. Double-click **Export**. A **.tar* file is created and you can save it for later auto-configuration of additional CPEs.

Figure 3-10: Engineering - Dev Config Page

To generate an ipk file:

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

- *Generate_Provision_V1.8.rar* (provided on a CDROM)
- The **.tar* file created previously.

2 Extract the *Generate_Provision_V1.8.rar* and run the CPE Auto Configuration Tool: *generate_provision_1.8.exe*; The Generate IPKG Tool window is displayed.

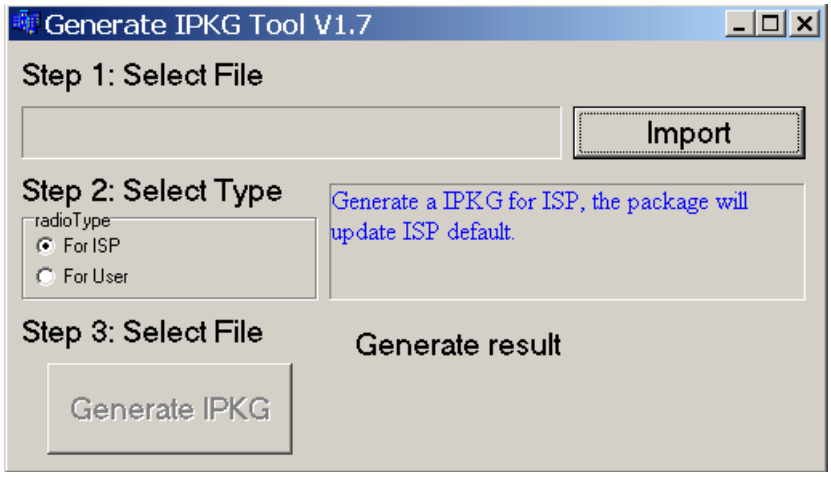


Figure 3-11: Generate IPKG Tool

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

4 Select the type of IPKG to generate:

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

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

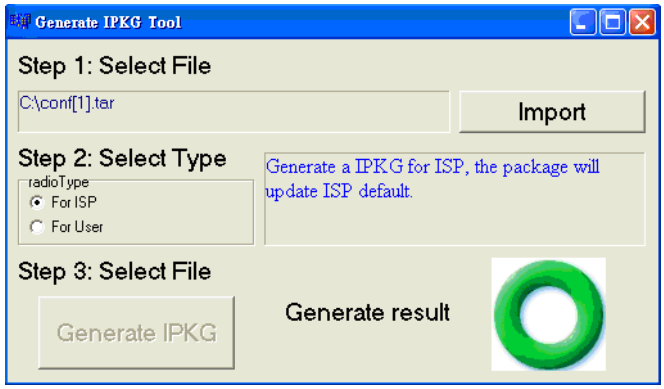


Figure 3-12: Generation Results

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

3.6 Operation Verification

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

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

Chapter 4

Configuring Setup Parameters

In This Chapter:

4.1 Introduction

The BreezeMAX Si 4000's Setup menu allows you to perform general management functions for the unit, including setting the connection modes, the system time zone, configuring an access password, and restore settings to factory defaults.

NOTE

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

The default IP address of the BreezeMAX Si 4000is 192.168.254.251. The unit operates by default in DHCP mode.

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

When applying Factory Defaults, a Rebooting message and the 60 seconds countdown are displayed.

4.2 Setting Basic Parameters

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

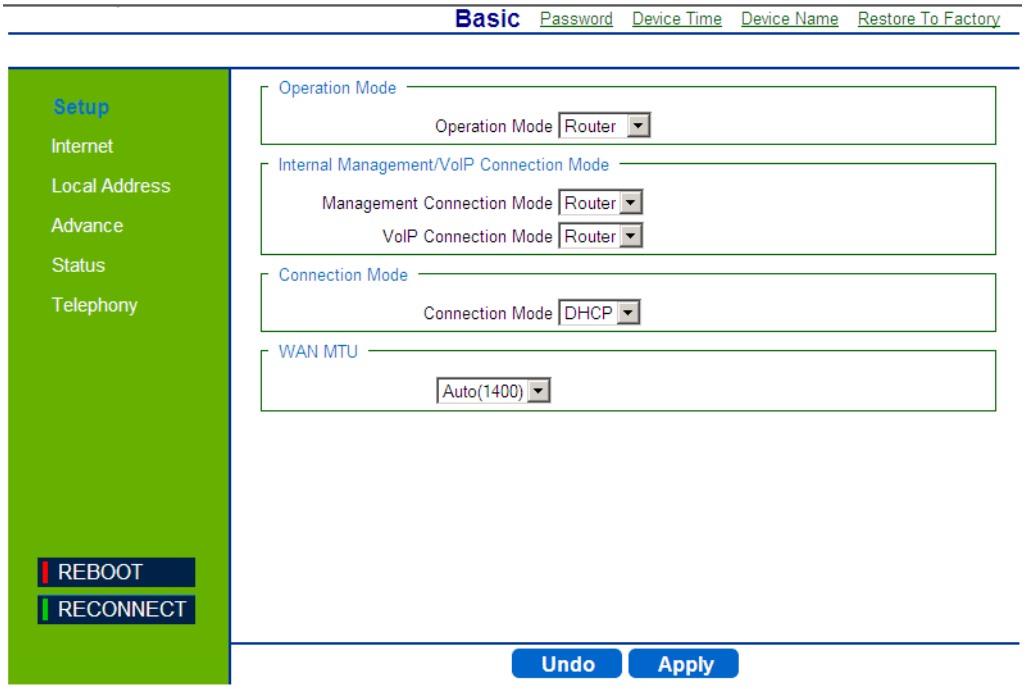


Figure 4-1: Setup - Basic Parameters

- **Operation Mode** - Specifies the mode for forwarding data packets from the service provider's WiMAX network to the local network. Router is the only option, unless differently configured by Alvarion.

- **Internal Management/VoIP Connection Mode**

  - Management Connection Mode - Sets the forwarding mode for sending management packets to the WiMAX network:

    - Bridge mode forwards packets based on Layer 2 MAC addresses. Bridge mode means that management connection will have a different (second)

IP than data connection. This IP will be used for communication with the management server, for web access from WAN, ping, etc.

- ◊ Router mode forwards packets based on Layer 3 IP addresses.

» VoIP Connection Mode - Sets the forwarding mode for sending VoIP packets to the WiMAX network:

- ◊ Bridge mode forwards packets based on Layer 2 MAC addresses. Bridge mode means that voice connection will have different IP than data or management connections. This IP will be used only for SIP/RTCP and RTP messages sent and received by the device's POTS (plain old telephone service) lines.
- ◊ Router mode forwards packets based on Layer 3 IP addresses.
- ◊ None - No forwarding

■ **Connection Mode -** sets the connection type for the unit

» DHCP - The system will assign IP addresses to the unit on the local area network.

» Static - The IP address is predefined and fixed. When you select this option new menu items are displayed for configuration:

- ◊ WAN IP Address
- ◊ WAN Subnet Mask
- ◊ WAN Gateway Address
- ◊ DNS1- Domain Name System
- ◊ DNS2

■ **WAN MTU** - Sets the WAN maximum transmission unit (MTU) size in bytes

» Auto (1400) - transmission unit size is 1400 bytes

» Manual - enter the value for transmission unit size (Range: 576-1500)

4.3 Setting Password

The Password page enables you to change the default password for management access to the BreezeMAX Si 4000.

NOTE

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

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

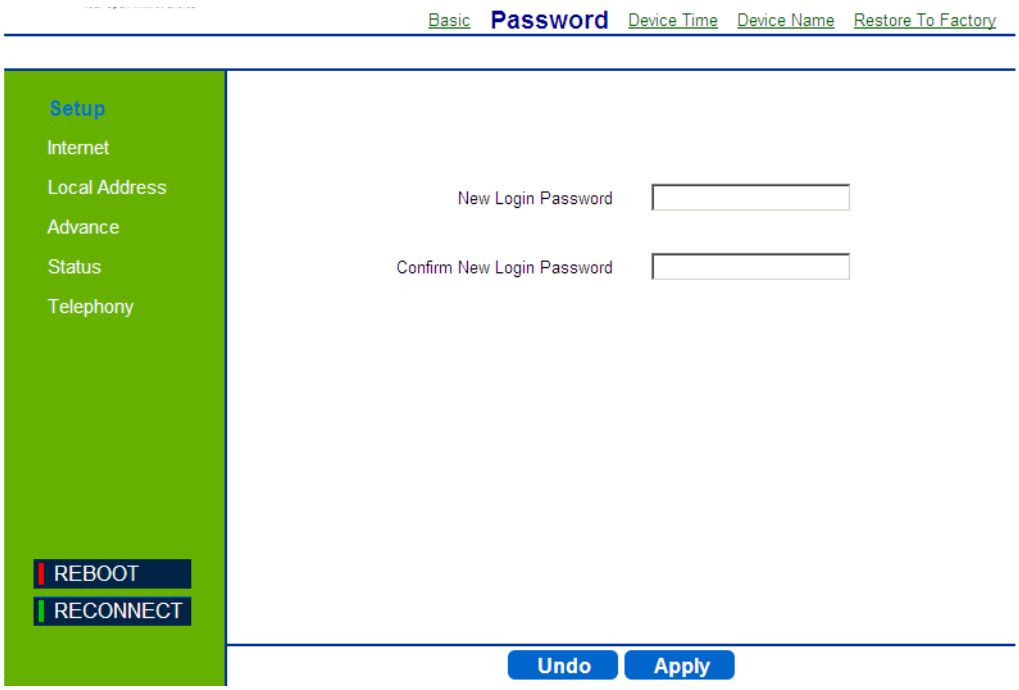


Figure 4-2: Setup - Password

To change the login password:

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

4.4 Setting Device Time Zone

The BreezeMAX Si 4000 uses the Simple Network Time Protocol (SNTP) to set its internal clock based on periodic updates from a time server. Maintaining an accurate time on the device enables the system log to record meaningful dates and times for event entries.

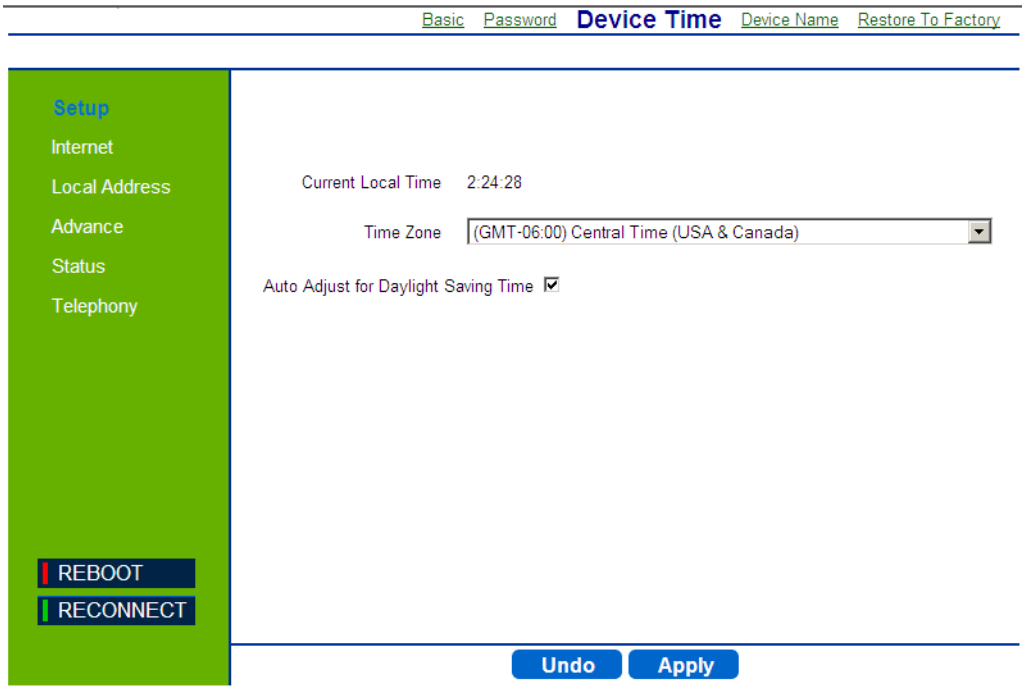


Figure 4-3: Setup - Device Time

The Device Time page displays the following information:

- **Current Local Time (hh:mm:ss)** – Displays the current time of the system clock.
- **Time Zone** – SNTP uses Greenwich Mean Time, or GMT (also known as Universal Time Coordinated, or UTC) based on the time at the Earth's prime meridian, zero degrees longitude. To display a time corresponding to your local time, select your time zone from the pull-down list. The default is GMT-06.00, for Central Time (USA and Canada.)

- **Auto Adjust for Daylight Saving Time** - Select this check-box to set the daylight saving time if the unit operates in a region that observes daylight saving time. The default is Enabled.

4.5 Setting Device Name

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

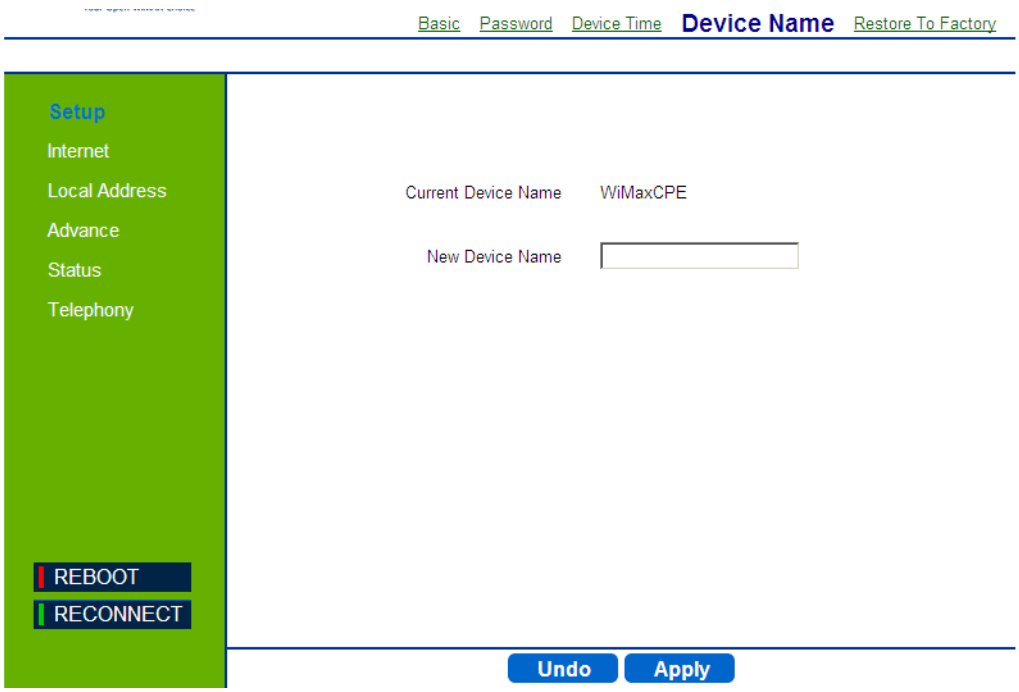


Figure 4-4: Setup - Device Name

The Device Name page displays the following information:

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

4.6 Restore to Factory Default Configuration

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

All the changes from the default factory settings will be lost, including WiFi and Voice settings. Voice settings can be reconfigured by contacting Customer Support.

Figure 4-5: Setup - Restore to Factory Warning

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

Chapter 5

Configuring Internet Parameters

In this chapter:

5.1 Introduction

BreezeMAX Si 4000's Internet menu allows you to set general Internet management functions for the unit, including authentication method selection, security parameters, and setting a Dynamic DNS (Domain Name System) provider.

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

5.2 Authentication

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

IMPORTANT

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

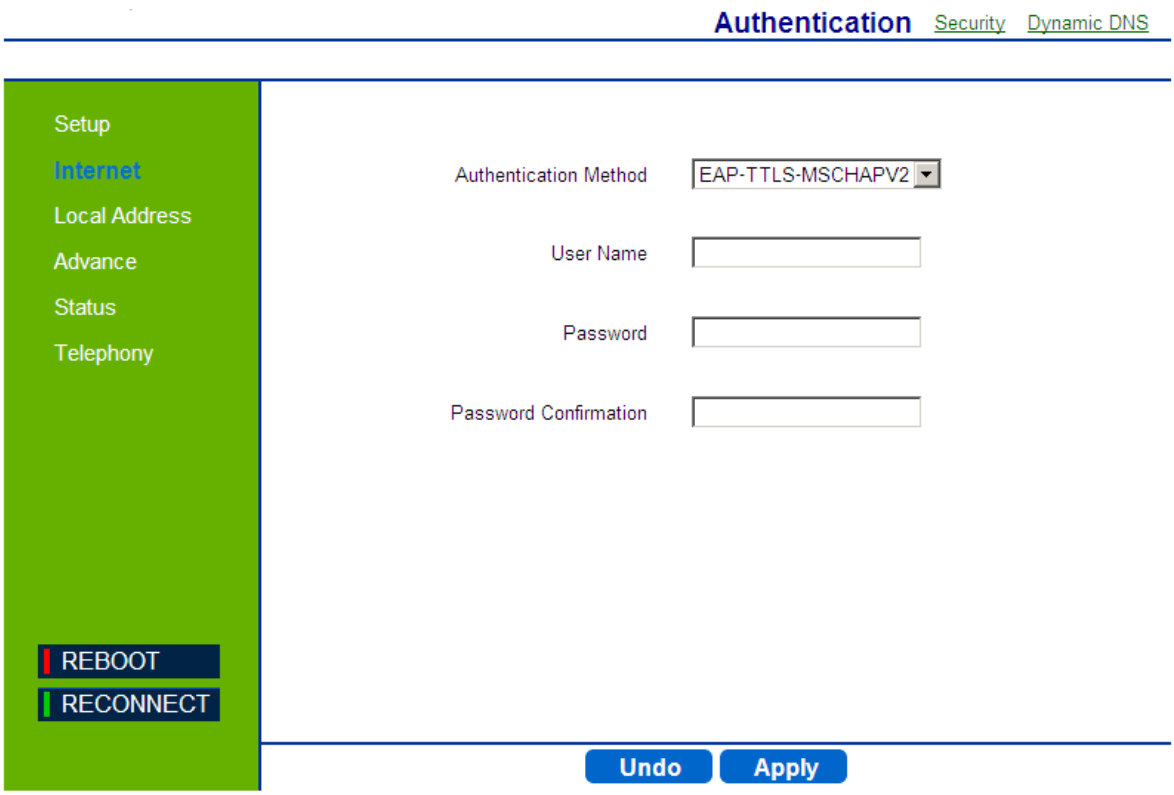


Figure 5-1: Internet - Authentication

The Authentication page includes the following parameters:

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

When Authentication is enabled, set the following parameters:

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

5.3 Security

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

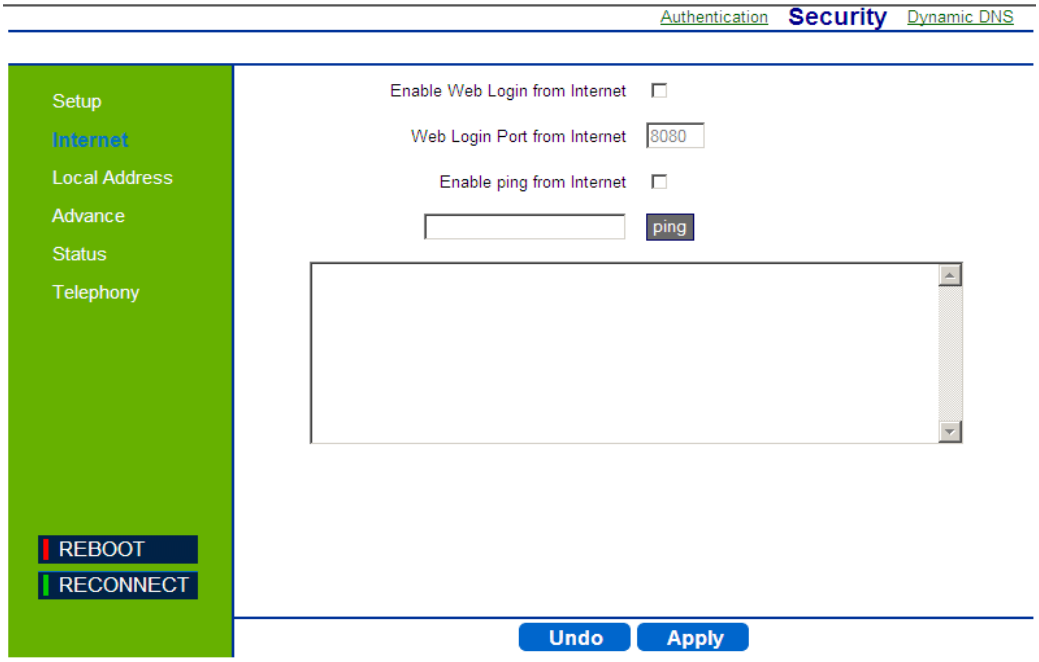


Figure 5-2: Internet - Security

The Security page includes the following parameters:

- **Enable Web login from Internet** - Select this check-box to access the device from other networks. When web login is enabled and a port is defined, you can access the device from another network Simply by opening a browser and entering the address of the device (Default: Disabled)

- **Web Login Port from Internet** - Define a specific port number for security access control (the default port number is 8080). Available only if Web Login from Internet is enabled.

- **Enable ping from Internet** - Enables to set the unit to respond to ping commands for troubleshooting purposes.

NOTE

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

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

To issue a Ping command from internet, enter the destination address (either your PC or another PC as required and click **Ping**. The response will be displayed in the area below the Ping button.

5.4 Dynamic DNS

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

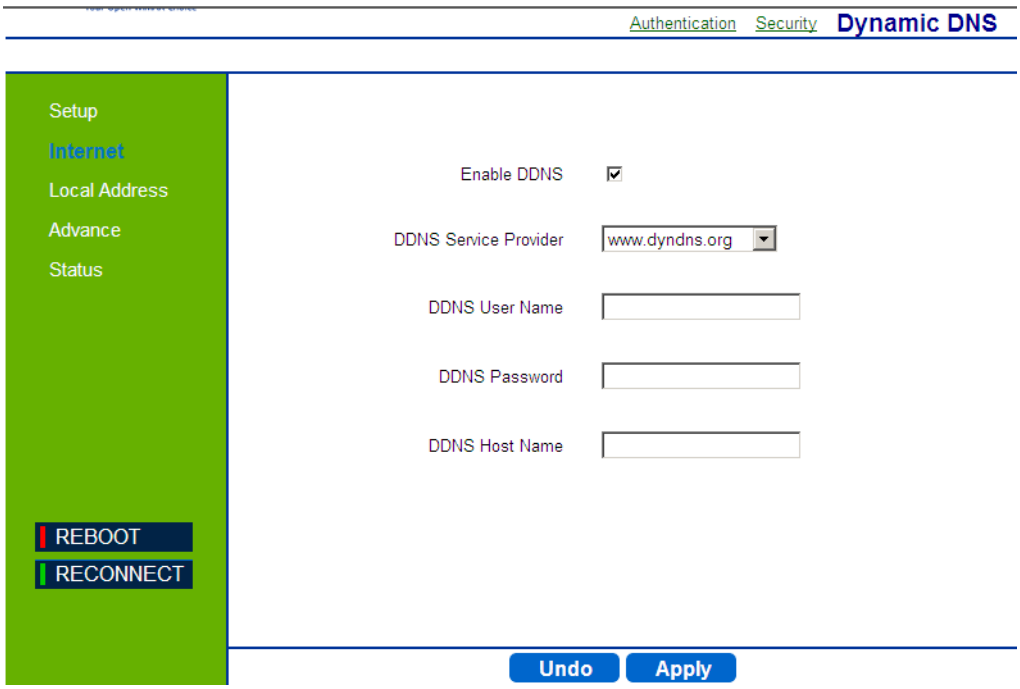


Figure 5-3: Internet - Dynamic DNS

The Dynamic DNS page includes the following parameters:

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

  When DDNS is enabled, configure the following parameters:

  - DDNS User Name
  - DDNS Password
  - DDNS Host Name

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

5.5 WiFi

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

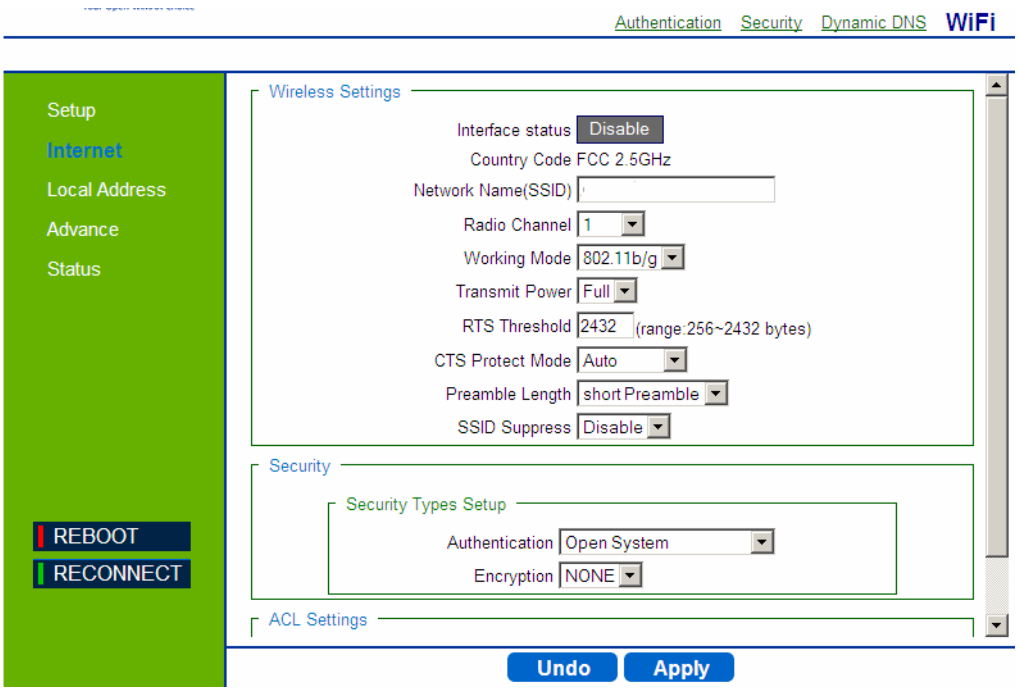


Figure 5-4: Internet WiFi

5.5.1 Wireless Settings

The Wireless Settings page includes the following parameters:

- **Interface status** - Enables/disables the Wi-Fi radio
- **Country Code** –The parameter set (list of parameters per country regulations) by which various parameters are defined (Read-only).
- **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: 1-14, Auto).

NOTE

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

- **Working mode** - The 802.1x authentication is an addition to the WLAN security methods. It provides a method to protect the network behind the access point from intruders as well as provide dynamic keys and strengthen WLAN encryption. (Range: 802.11b, 802.11g, 802.11b/g, Default:802.11b/g)

- **Transmit Power** – The power of the radio signals transmitted from the unit. The higher the transmission power, the farther the transmission range. Only Full power is available.

- **RTS Threshold** – Sets the packet size threshold at which a Request to Send (RTS) signal must be sent to a receiving station prior to sending the data frame. The unit sends RTS frames to a receiving station to negotiate the sending of a data frame. After receiving an RTS frame, the station sends a CTS (clear to send) frame to notify the unit that it can start sending data. If a packet size equals or exceeds the RTS threshold, the RTS/CTS (Request to Send/Clear to Send) mechanism will be enabled. Units contending for the medium may not be aware of each other, and the RTS/CTS mechanism can solve this “Hidden Node Problem.” (Range: 256-2432 bytes: Default: 2432 bytes)

- **CTS Protect Mode** – When 802.11g and 802.11b clients operate together in the same Wi-Fi network, there needs to be a mechanism that prevents 802.11b clients from interfering with 802.11g transmissions. This is achieved by sending 802.11b-compatible CTS (Clear to Send) or RTS/CTS (Request to Send / Clear to Send) frames before each transmission. This mechanism decreases the performance of 802.11g clients, but ensures that 802.11b clients can communicate with the BreezeMAX Si 4000. (Default: Auto)

  - **Always off**: If there are no 802.11b clients in the network, the protection mode can be disabled.
  - **Always on**: The transmitting client sends a CTS frame to prevent others from accessing the medium. This mechanism is effective for most networks with mixed 802.11g and 802.11b clients.
  - **Auto**: Both RTS and CTS frames must be exchanged before a client can send data. There may be 802.11b clients in some networks that do not detect the CTS frames from other stations. The full RTS/CTS exchange should solve most connection problems, but it also has the greatest impact on network performance.

- **Preamble Length** – All IEEE 802.11 frames begin with an alternating pattern of 1s and 0s called the preamble, which tells receiving stations that a frame is arriving. This provides time for the receiving station to synchronize to the incoming data stream. This parameter sets the length of the signal preamble that is used at the start of a data transmission. Using a short preamble instead of a long preamble can increase data throughput on the unit, but requires that all clients can support a short preamble. (Default: Short)

  - **Short**: Sets the preamble to short (96 microseconds) for increased throughput.
  - **Long**: Sets the preamble to long (192 microseconds. Using a long preamble ensures the unit can support all 802.11b and 802.11g clients.

- **SSID Suppress** – The unit is configured by default as an “open system,” which broadcasts a beacon signal including the configured SSID. Wireless clients with a configured SSID of “ANY” can read the SSID from the beacon, and automatically set their SSID for immediate connection to the BreezeMAX Si 4000. When enabled, the unit does not include its SSID in beacon messages. This provides a basic level of security, since wireless clients must be configured with the SSID to connect to the BreezeMAX Si 4000.

5.5.2 Wireless Security

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

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

- **Authentication** – It must be verified that clients attempting to connect to the network are authorized users. (Default mode is WPA-PSK, see “WPA/WPA2 Security” on page 62)
- **Traffic Encryption** – Data passing between the unit and clients must be protected from interception and eavesdropping.

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

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

The following sections describe the security options available for the BreezeMAX Si 4000Wi-Fi network.

5.5.2.1 802.1x

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

You can set the following:

- Rekey Interval - Interval in seconds between renewals of authentication key (Default: 3600)
- RADIUS Server
- RADIUS Port (Default: 1812)

- RADIUS Key (Default: radius_key)

5.5.2.2 Shared Key (WEP)

Wired Equivalent Privacy (WEP) provides a basic level of security, preventing unauthorized access to the network and encrypting data transmitted between wireless clients and the BreezeMAX Si 4000. WEP uses static shared keys (fixed-length hexadecimal or alphanumeric strings) that are manually distributed to all clients that want to use the network.

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

Default Key (1 ~ 4) – Sets WEP key values for authentication and encryption. The user must first choose between ASCII or Hexadecimal keys. At least one key must be specified. Each WEP key has an index number. The selected key is used for authentication and encryption on the Wi-Fi interface. Enter key values that match the key type and length settings. (Default: Hex, 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.

5.5.2.3 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.

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

You can set the following:

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

5.5.3 ACL (Access Control List) Settings

In this section you can add MAC addresses of clients which are authorized to access the system.

Click **Insert** to add a MAC address to the list, and specify the details.

Chapter 6

Displaying Status Details

In this chapter

6.1 Introduction

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

6.2 Device Status

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

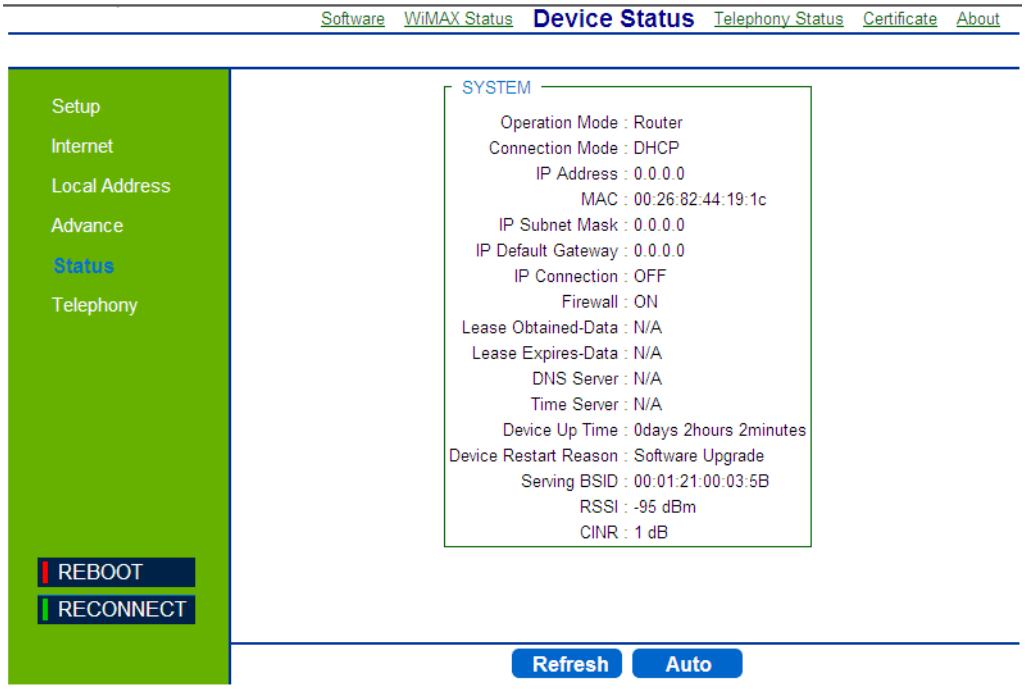


Figure 6-1: Status - Device Status

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

Table 6-1: Device Status Parameters

Item	Description
Operation Mode	The mode for forwarding data packets from the service provider's WiMAX network to the local network, as defined in "Setting Basic Parameters" on page 43. Available option: Router.
Connection Mode	Connection type for the unit, as defined in "Setting Basic Parameters" on page 43. Available options: DHCP, Static

Table 6-1: Device Status Parameters (Continued)

Item	Description
IP Address	WAN IP address, if the Static connection mode was selected, as defined in "Setting Basic Parameters" on page 43. For DHCP mode - IP address acquired on the WAN interface is displayed. Otherwise it is 0.0.0.0
MAC	WAN MAC Address
IP Subnet Mask	The IP subnet mask, if the Static connection mode was selected, as defined in "Setting Basic Parameters" on page 43, For DHCP mode - IP address acquired on the WAN interface is displayed. Otherwise it is 0.0.0.0
IP Default Gateway	The IP Default Gateway, if the Static connection mode was selected, as defined in "Setting Basic Parameters" on page 43. For DHCP mode - IP address acquired on the WAN interface is displayed. Otherwise it is 0.0.0.0
IP Connection	IP is connected to the network (On/Off)
Firewall	Firewall enabled or disabled (on/off), as set in "Firewall" on page 90.
Lease Obtained-Data	Date of obtaining the device leasing.
Lease Expires-Data	Date of device leasing expiration.
DNS Server	The Domain Name Server address
Time Server	The NTP (Network Time Protocol) server address
Device Up Time	Duration of device function (xdays yhours zminutes)
Device Restart Reason	The reason for last device reebot (e.g. Software Upgrade)
Serving BSID	Base Station ID number (e.g. 00:01:21:00:03:5A)
RSSI	Currently received signal strength indication (e.g. 78 dBm)
CINR	Carrier to Interference-plus-Noise Ratio [in decibels (dB)] (e.g. 13 dB). This value should be maximized for best signal quality.

6.3 WiMAX Status

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

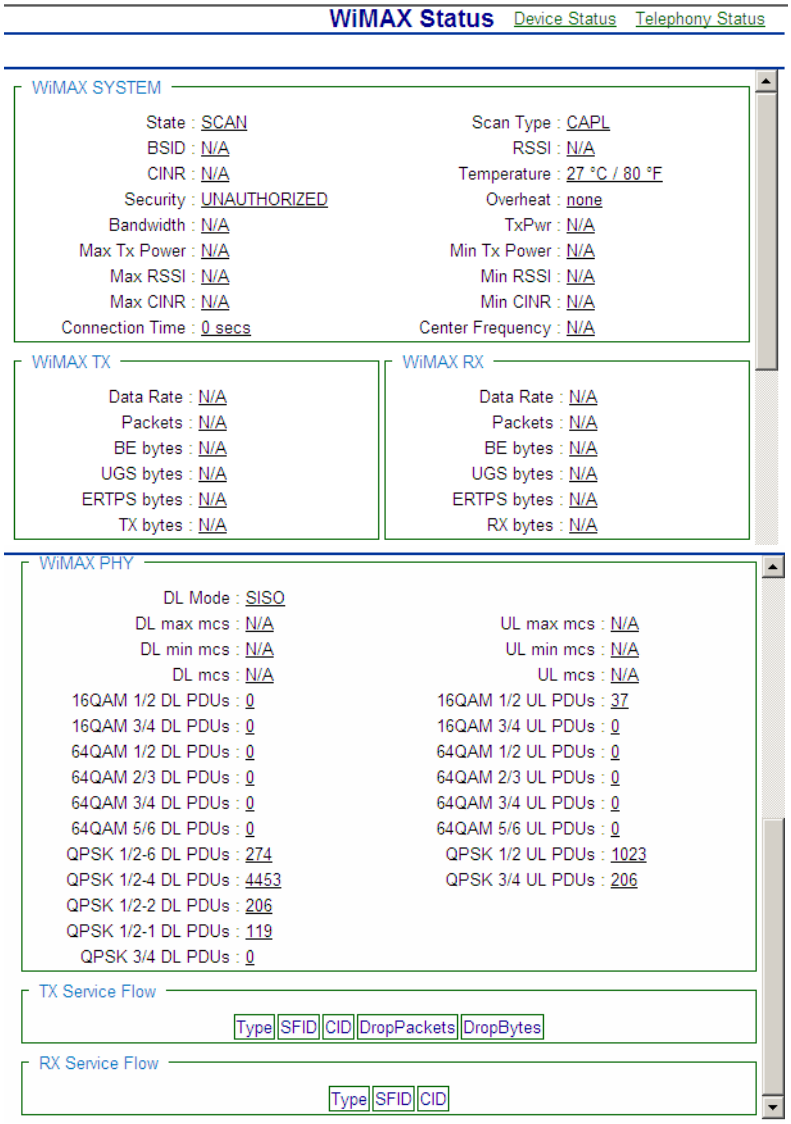


Figure 6-2: Status - WiMAX Status

- Click **Refresh** to display the current WiMAX connection status.
- Click **Auto** to update the status information periodically (every 10 seconds)

The following table describes the WiMAX Status parameters:

Table 6-2: WiMAX System Parameters

Parameter	Description	Possible values
WiMAX System		
State	The status of WiMAX connection.	■ Network Entry - the unit has just been connected to the network ■ Operational - the unit is functional ■ Scan - the unit scans the network ■ Idle - the unit is de-registered from the network, however will continue to scan the network and keep track of its location
BSID	Base Station ID	Depends on the BS to which the unit is connected
CINR	Carrier to Interference-plus-Noise Ratio [in decibels (dB)] - a measurement of signal effectiveness. A greater value will improve the connection speed.	0-35 dB
Security	Network security technologies and protocols status	Authorized - has authentication settings Unauthorized - without authentication setting
Bandwidth		Depending on unit model: 5000, 7000, or 10000
Max Tx Power	Maximum uplink transmit power	
Max RSSI	Maximum received signal strength indication	-35 to -100 dBm
Max CINR	Maximum Carrier to Interference-plus-Noise Ratio	
Connection Time	Time (in seconds) during which the unit is connected to the BS	

Table 6-2: WiMAX System Parameters (Continued)

Parameter	Description	Possible values
Scan Type	The method by which the network is scanned	■ Fullband - The system will try to scan the whole frequency band. ■ CAPL - Channel Allocation Priority Level. The system allocates priority to channels for scanning order. ■ Neighbor - The system will try to scan the neighbor BS to the previous BS defined in “Last good BS”. The neighbor BS details will appear in the table of this section. ■ History - The system will try to scan with the previous good BS to speed up the scan duration. A “good BS” is defined as one with which the unit can get an IP address.
RSSI	Currently received signal strength indication	-35 to -100 dBm
Temperature	Unit’s temperature	
Overheat	Indication of temperature higher than 40°	
TxPwr	Current uplink transmit power	
Min Tx Power	Minimum uplink transmit power	
Min RSSI	Minimum received signal strength indication	
Min CINR	Minimum Carrier to Interference-plus-Noise Ratio	
Center Frequency	The middle frequency of the bandwidth of a channel.	
WiMAX TX		
Data Rate	The level of available data throughput that can actually be provided to an end-user.	
Packets	Number of carried blocks of data	
BE bytes	Total number of bytes sent on Best Effort connection	
UGS bytes	Total number of bytes sent on Unsolicited Grant Service connection	

Table 6-2: WiMAX System Parameters (Continued)

Parameter	Description	Possible values
ERTPS bytes	Total number of bytes sent on ERTPS - Extended Real-time Polling Service data packets.	
TX bytes	Total of uplink transmitted bytes	
WiMAX RX		
Data Rate	The level of available data throughput that can actually be provided to an end-user.	
Packets	Number of carried blocks of data	
BE bytes	Total number of bytes sent on Best Effort data packets	
UGS bytes	Total number of bytes sent on Unsolicited Grant Service data packets	
ERTPS bytes	Total number of bytes sent on Extended Real-time Polling Service data packets	
RX bytes	Total of downlink transmitted bytes	
WiMAX PHY		
DL Mode	Downlink connection mode	SISO, MIMO, MiMO A, MIMO B
DL max mcs	Maximum modulation reached	
DL min mcs	Minimum modulation reached	
DL mcs	Current modulation	
UL max mcs	Maximum modulation reached	
UL min mcs	Minimum modulation reached	
UL mcs	Current modulation	
List of various modulations: ■ QPSK DL/UL PDUs ■ 16QAM DL/UL PDUs ■ 64QAM DL/UL PDUs	Number of packets in this modulation	
TX Service Flow / Rx Service Flow		
Type	The service flow type	Best effort, ERT, NRT, UGS
SFID	Service flow ID	
CID	Connection ID	

Table 6-2: WiMAX System Parameters (Continued)

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

6.4 Software Status

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

NOTE

Use this page only upon instructions from Alvarion.

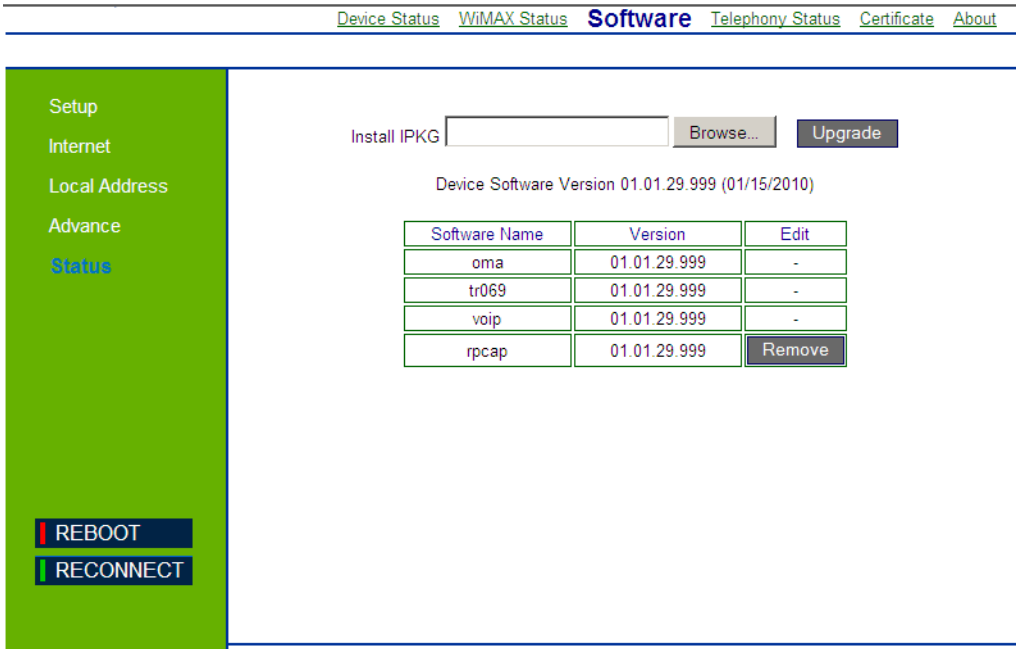


Figure 6-3: Status - Software

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

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

6.5 Telephony Status

This page displays information on the telephone line status.

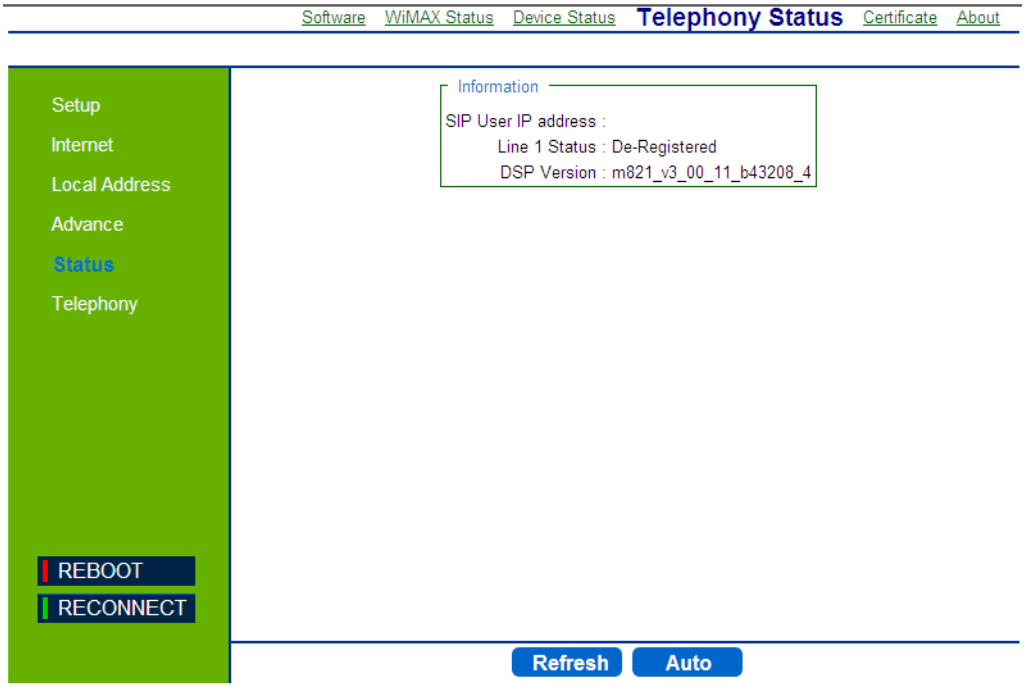


Figure 6-4: Status - Telephony Status

The information displayed in this window is:

- **SIP User IP address** - IP address of the Session Initiation Protocol, an application-layer control protocol that can establish, modify, and terminate multimedia sessions such as Internet telephony calls (VOIP).
- **Line 1 Status** - Registered or De-registered in the SIP server
- **DSP Version** - current version of the voice chip in the Data Signal Processor (DSP).
- Click **Refresh** to display the current telephony status.
- Click **Auto** to update the status information periodically (every 10 seconds).

6.6 Certificate Status

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

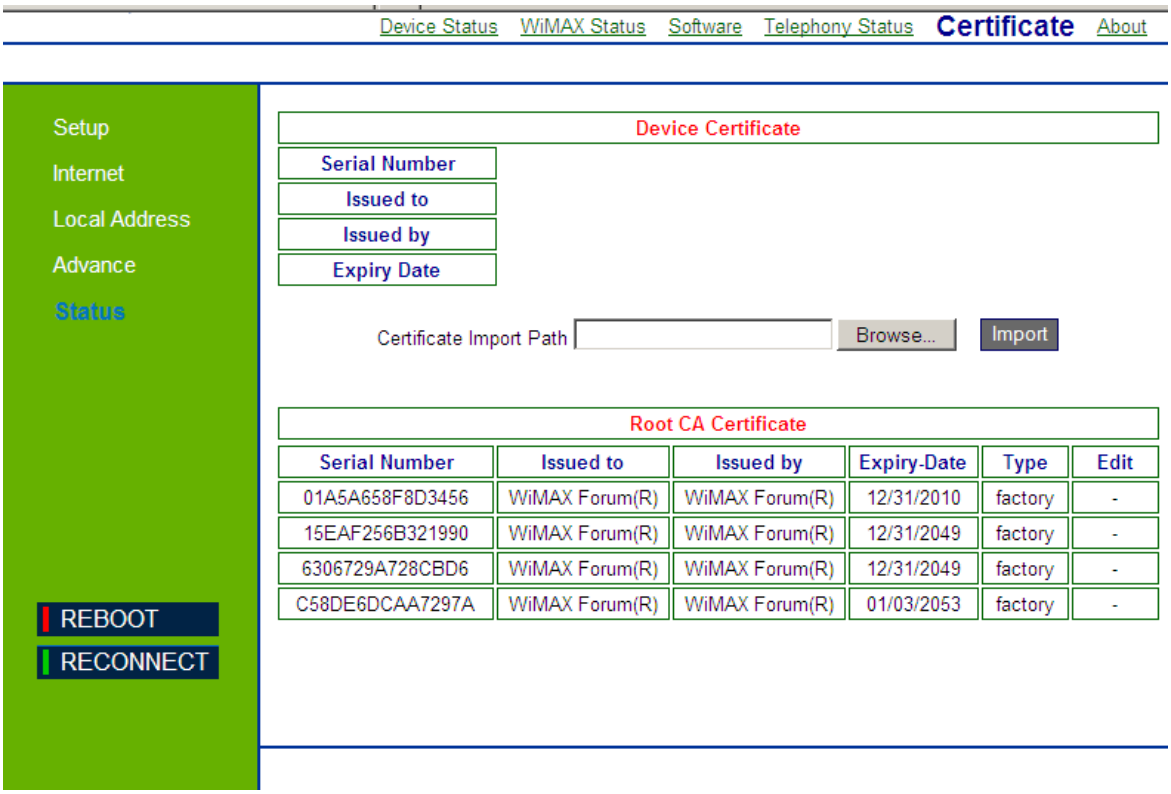


Figure 6-5: Status - Certificate

The page displays the following information in a table:

- Certificate Serial Number
- Issued to
- Issued by
- Expiry Date - the date for certificate expiration. The format is mm/dd/yyyy.
- Certificate type
- Edit - option to remove a certificate from the list

NOTE

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

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

6.7 About

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

The information includes:

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

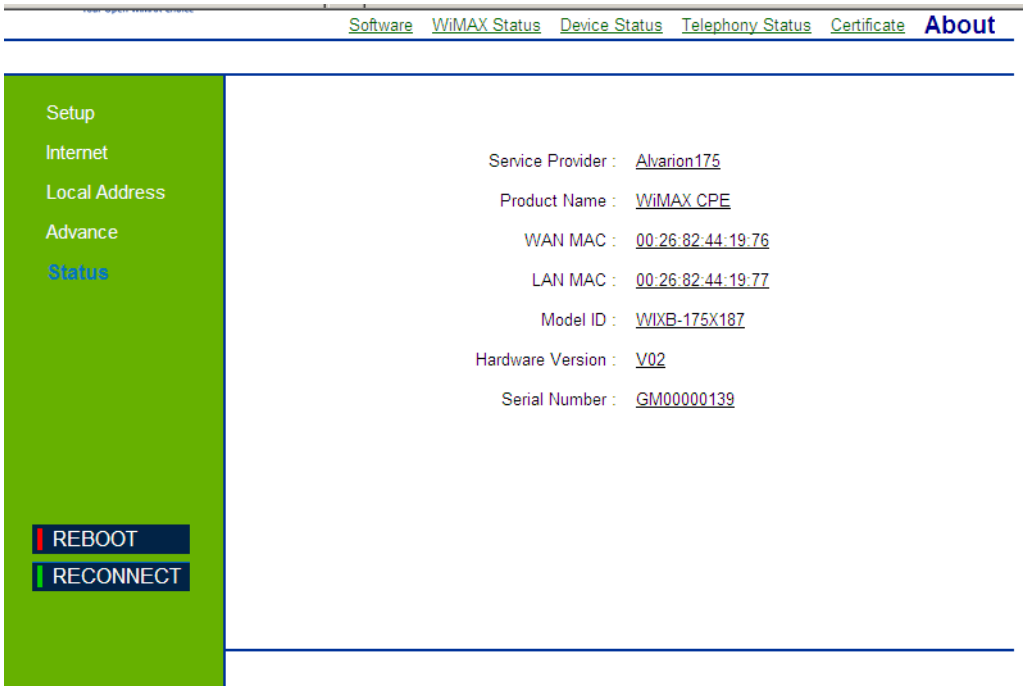
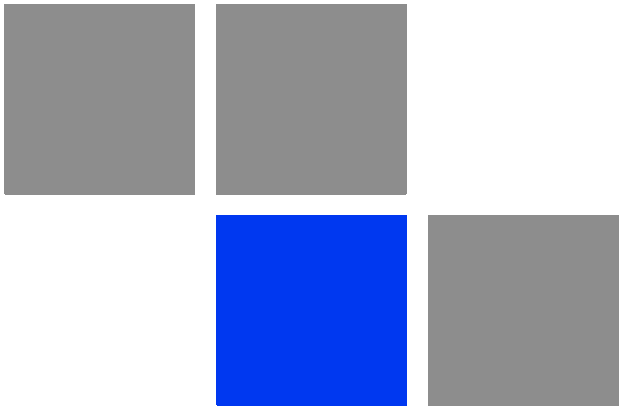


Figure 6-6: Status - About



Chapter 7

Configuring Local Address Parameters

In this chapter:

7.1 Introduction

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

NOTE

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

7.2 DHCP Server

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

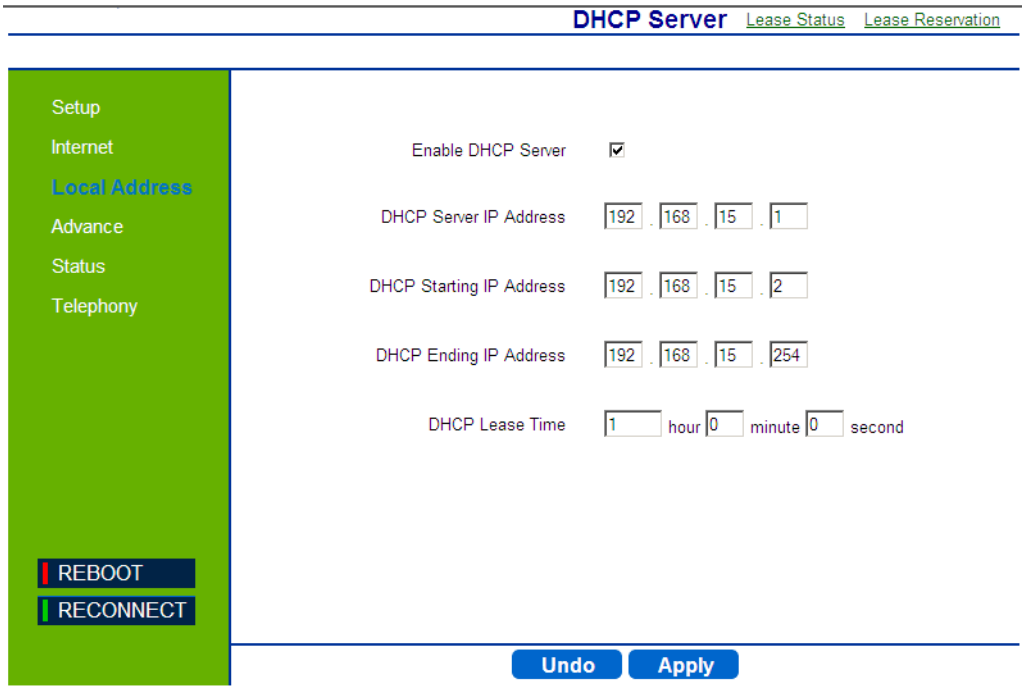


Figure 7-1: DHCP Server

- **Enable DHCP Server** - Select this check-box dynamically assign a leased IP address to clients that connect to the device from the local network. This option is applicable to IP CS modes only. For Bridge (Eth CS) this option is disabled.

- **DHCP Server IP Address** - Enter a DHCP server IP address. The default address is 192.168.254.251.

- **DHCP Starting IP Address** - Enter the first IP address assigned by the DHCP server. The default address is 192.168.254.1.

- **DHCP Ending IP Address** - Enter the last IP address assigned by the DHCP server. The default address is 192.168.254.5.

- **DHCP Lease Time** - Set the time for renewing the IP Lease. Default: 15minutes.

7.3 Lease Status

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

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

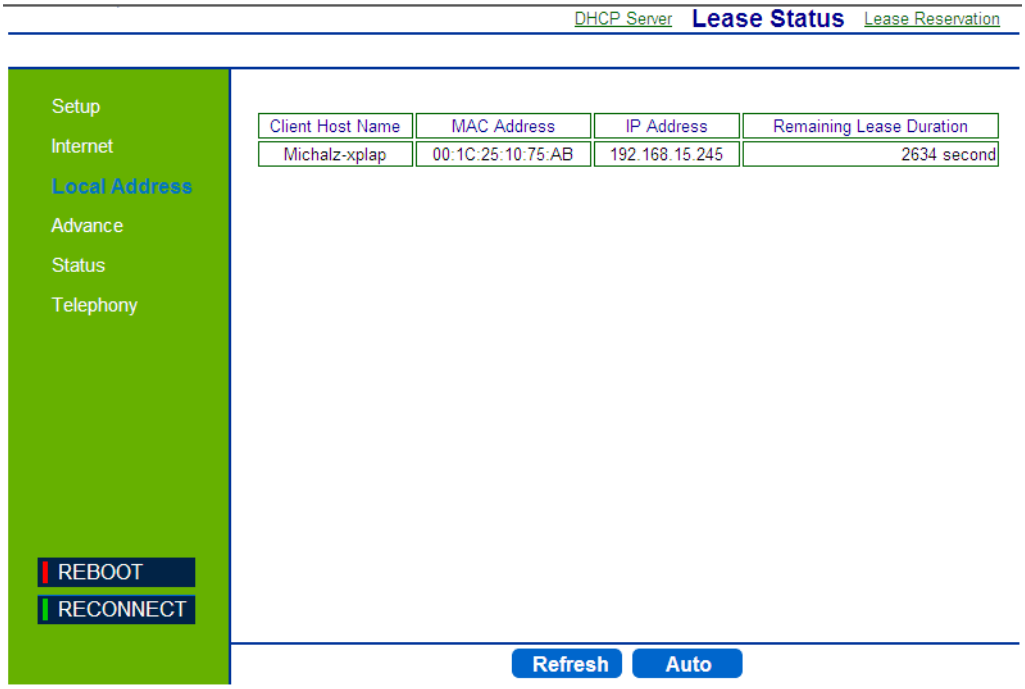


Figure 7-2: Lease Status

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

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

7.4 Lease Reservation

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

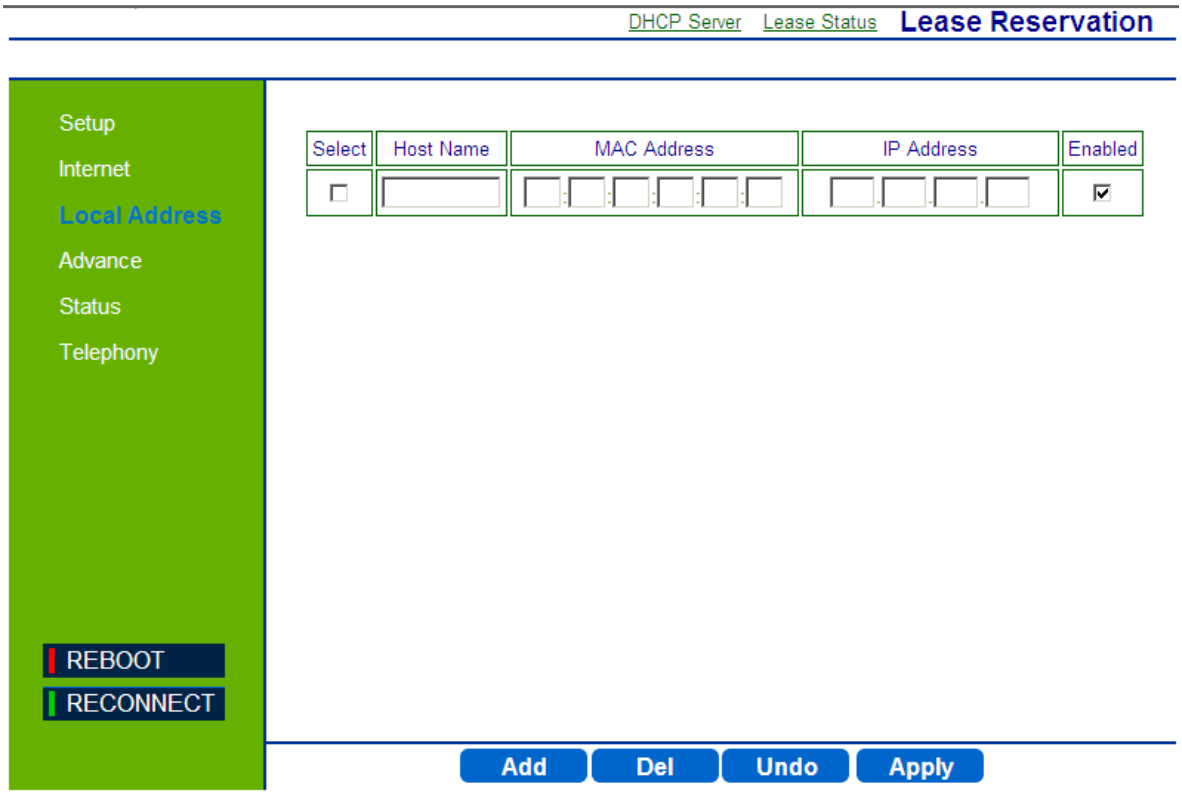


Figure 7-3: Lease Reservation

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

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

Chapter 8

Setting Advanced Parameters

In this chapter:

8.1 Introduction

This chapter describes how to configure advanced parameters, such as: Firwall protection, filters for blocking the access of unauthorized clients, port forwarding and triggering, and also the service line parameters.

8.2 Firewall

The BreezeMAX Si 4000 provides extensive firewall protection by restricting connection parameters to limit the risk of intrusion and defending against a wide array of common hacker attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a demilitarized zone (DMZ).

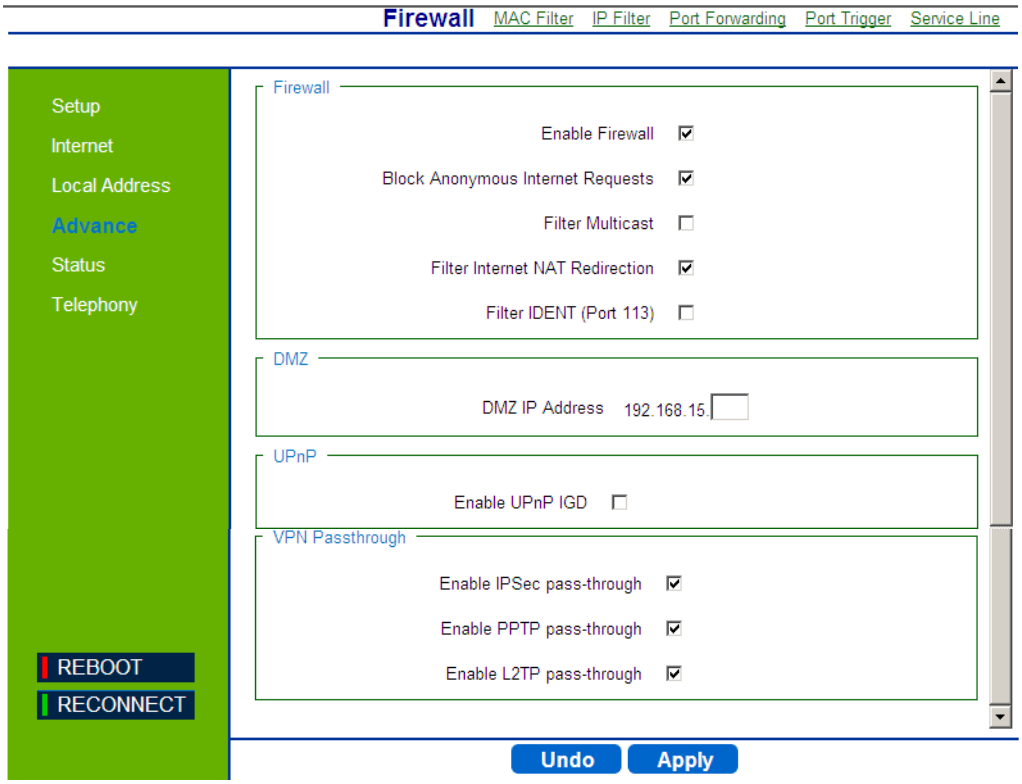


Figure 8-1: Advance - Firewall

The following configuration parameters are available:

- **Firewall** settings
  - **Enable Firewall** - Select this check-box to enable or disable firewall
  - **Block Anonymous Internet Requests** - Select this check-box to reject anonymous Internet requests.
  - **Filter Multicast** - Select this check-box to filter out mutlicast packets.
  - **Filter Internet NAT Redirection -** NAT Redirection is used to block access to the local server from the local PC via unit's WAN IP. If this feature is enabled, local PC can only access the local server via unit's LAN IP.
  - **Filter IDENT (Port 113)** - Select this check-box to drop incoming packets from the unit WAN side with destination port 113.
- **DMZ** - DMZ IP Address. Set a server that acts as a "neutral zone" (DMZ stands for "Demilitarized Zone") and separates an internal network from a public one in order to prevent outside access to private data. The DMZ forwards the network traffic to specific hosts based on the protocol and port number.
- **UPnP** - **Enable UPnP IGD** - Select this check-box to enable/disable Universal Plug and Play Internet Gateway Device - a protocol that simplifies device connection and network implementation. When this option is enabled, certain Windows applications would setup the port forwarding rule dynamically.
- **VPN Passthrough -** Select one of the following security protocols to define the Virtual Private Network traffic sessions.
  - **Enable IPSec pass-through** - Internet Protocol Security. IPSec provides encrypted security services at the IP layer, and enables to use encrypted tunnels /traffic between two hosts.
  - **Enable PPTP pass-through** - Point to Point Tunneling Protocol. This protocol enables the transfer of data packets of TCP / IP through a foreign network that is not based on these protocols (by marking the packet with an address suited to the foreign network)
  - **Enable L2TP pass-through** - Layer 2 Tunneling Protocol, an open standard with mutlivendor interoperability and acceptance.

8.3 MAC Filter

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

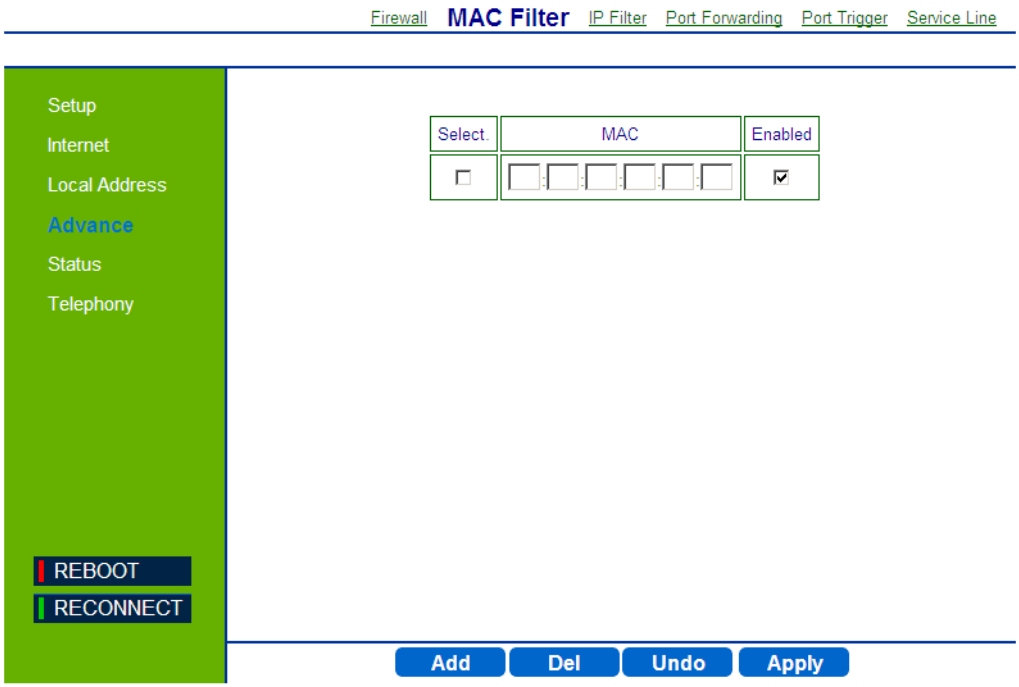


Figure 8-2: Advance - MAC Filter

The following configuration parameters are available:

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

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

8.4 IP Filter

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

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

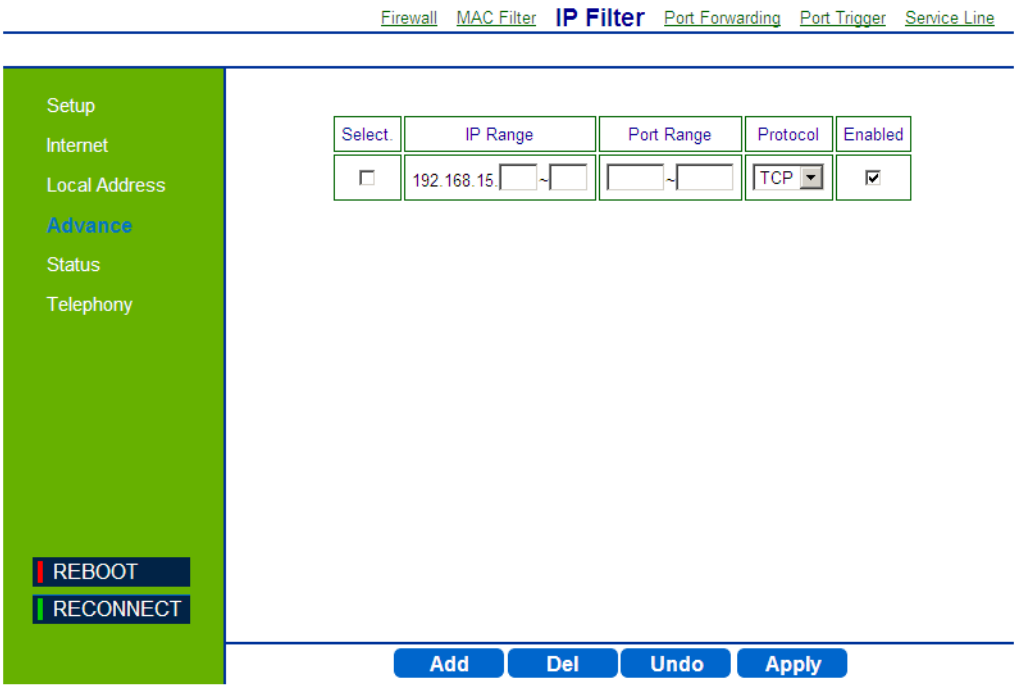


Figure 8-3: Advance - IP Filter

The following configuration parameters are available:

- **Select** - Select this check-box to add this client to the filtered group
- **IP Range** - Specify an IP address or range on the local network. (Range: 192.168.254.251 to 192.168.254.254)
- **Port Range** - Enter the port range to be filtered
- **Protocol** - set the protocol to be filtered: TCP (default) or UDP.

- **Enabled** - Select this check-box to enable or disable (default) filtering for the specific table entry.

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

8.5 Port Forwarding

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

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

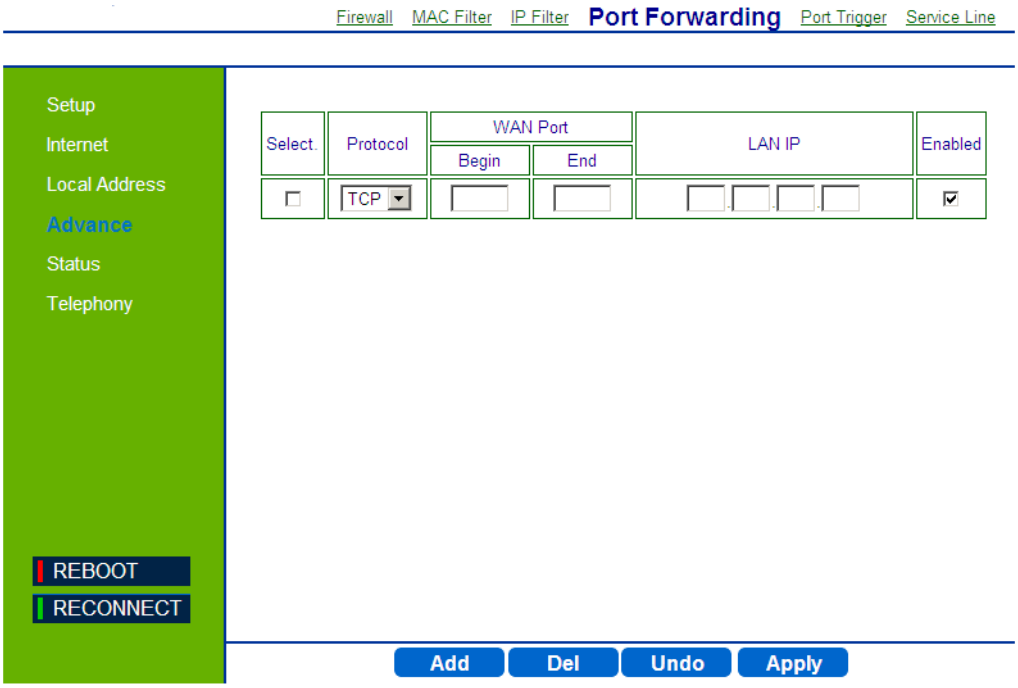


Figure 8-4: Advance - Port Forwarding

The following configuration parameters are available:

- **Select** - Select this check-box to add this row to the selection group
- **Protocol** - Set the protocol for port forwarding: TCP or UDP
- **WAN Port** - Enter the range (begin and end ports) for the WAN
- **LAN IP** - Enter the IP address that identifies the IP subnet of the remote network.

- **Enabled** - Select this check-box to enable/disable port forwarding for the specific IP

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

8.6 Port Trigger

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

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

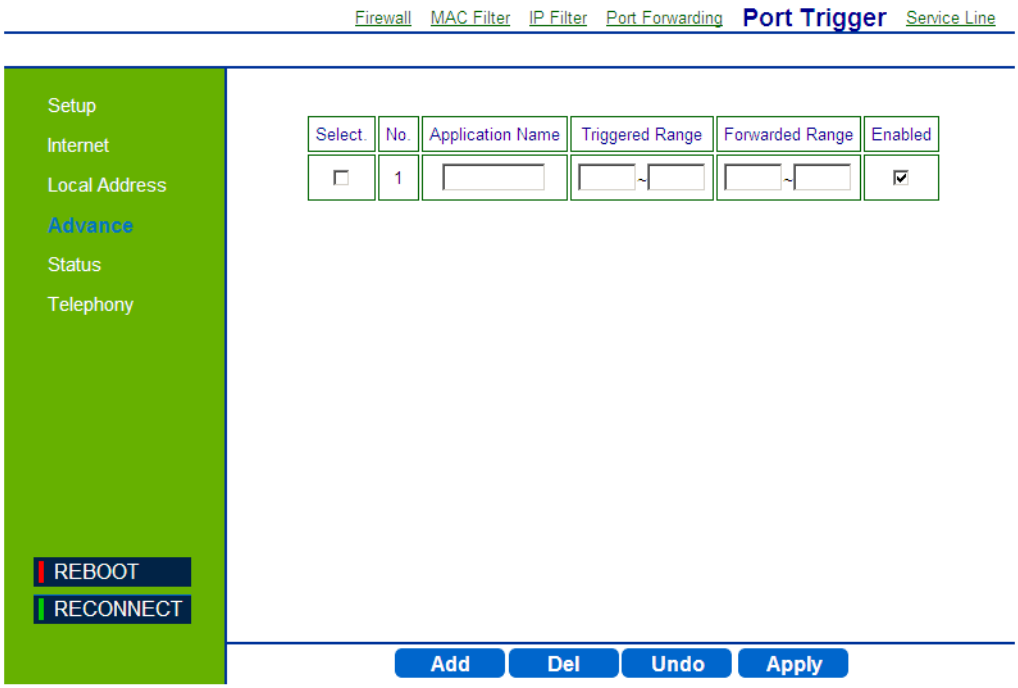


Figure 8-5: Advance - Port Trigger

The following configuration parameters are available:

- **Select** - Select this check-box to add this row to a selection group
- **No**. - Display the number of the port trigger rule

- **Application Name** - Enter a name for identifying this port trigger protocol.
- **Triggered Range** - Enter the trigger range (1~65535)
- **Forwarded Range** - Enter the forwarded range (1~65535)
- **Enabled** - Select this check-box to enable/disable port trigger for the specific application

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

8.7 Service Line

In the Service Line page you set the rules for data traffic. You can configure rules for Ethernet LAN ports, for Wireless LAN or for both.

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

A rule with Marking enabled must have the same value for the start and stop DSCP. For uplink traffic, when a rule with marking enabled is encountered then the traffic is marked with the corresponding DSCP value, regardless of the existing DSCP value. For downlink traffic, packets coming from WAN are forwarded to the configured LAN port only if they have the configured DSCP value. The value of the DSCP field of the first incoming packet from the specified LAN port will be used to mark all the reply packets towards LAN. For example, if the first coming packet from Ethernet LAN has the DSCP value 3, the second 5 and so on, and the Service Line rule is configured to mark the Ethernet LAN packets with 10 - all the reply packets coming from WAN with the DSCP 10 will be forwarded to LAN with DSCP 3.

The set of rules are verified one by one until a match is found. If a match is found the other rules are not checked anymore. The default rule permits all the traffic (DSCP value between 0 and 63 and both ports – ETH and WiFi).

You cannot configure a rule with a range of DSCPs that contains one of the DSCPs reserved for SIP, RTP/RTCP, or MGMT.

Only IP-CS (IP Conversion Sublayer) service line is available.

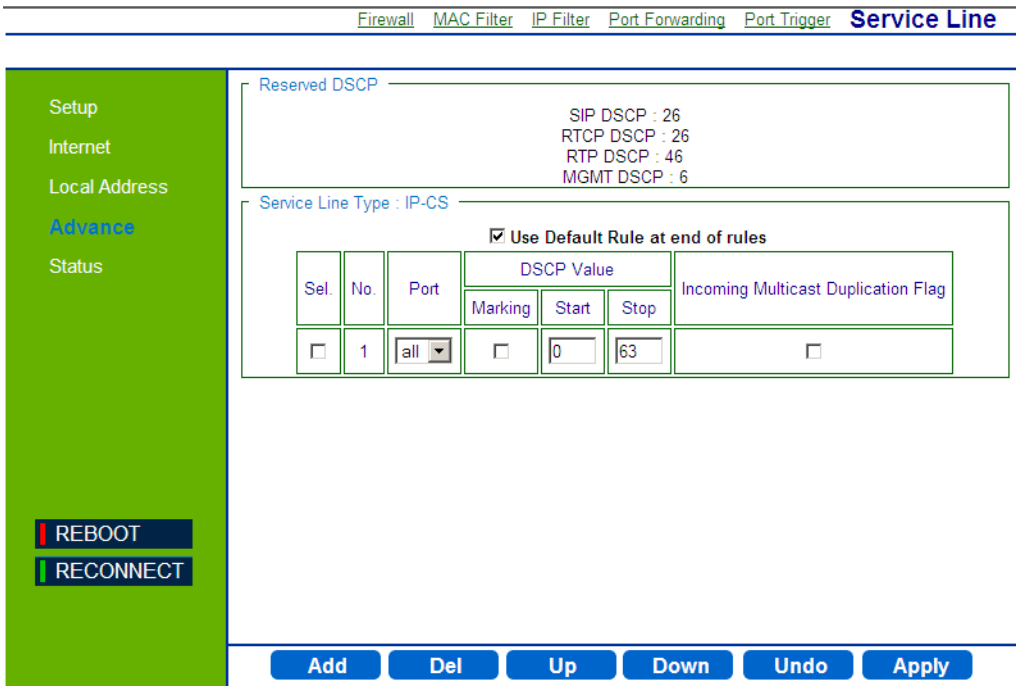


Figure 8-6: Advance - Service Line

The following information is displayed:

Reserved DSCP - You cannot configure a rule with a range of DSCPs that contains one of the DSCPs reserved for SIP, RTP/RTCP, or MGMT. For example, if the values for SIP, RTP/RTCP, MGMT are 26/46/6, you cannot configure a rule that contains one of these values (DSCP start 4, DSCP stop 7 or DSCP start 20, DSCP stop 50). Also you cannot configure a rule to mark packets with one of these values. (See also "Function Settings" on page 121).

The following configuration parameters are available:

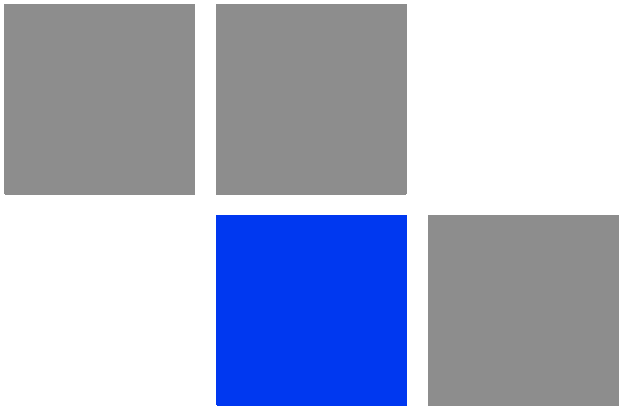
Table 8-1: Service Line Parameters (IP-CS)

Parameter	Description
Use Default Rule at end of rules	The default rule permits all the traffic (DSCP value between 0 and 63 and both ports – ETH and WiFi).If the default rule is enabled and none of the configured rules can be applied to the traffic, the default rule is applied. If the default rule is disabled and none of the rules matches the packets, then the packets are discarded.
Sel.	Select this check-box to add this row to a selection group
No.	Display the number of this rule

Table 8-1: Service Line Parameters (IP-CS) (Continued)

Parameter	Description
Port	Set the port for IP-CS: 1(data), 2(voice), WiFi or All
DHCP Value	■ Marking - Select this check-box to tag packets in this line for classification ■ Start /Stop - Internal Management, internal VoIP SIP and RTP DSCP shall not be allowed specifically. If they are in the range between start and stop, outgoing packets with these values will be dropped. If DSCP marking is enabled, the DSCP values of start=stop. Default: start=0, stop=63. Range: 0-63.
Incoming Multicast Duplication Flag	Select this check-box to enable duplication of multicast (VoIP, Data) packets.

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



Chapter 9

Engineering

In this chapter:

9.1 Introduction

The Engineering menu item is accessible to the Operator only and provides advanced CPE configuration parameters. The Engineering mode is available in a software package that is uploaded from the Status page; See “WiMAX Status” on page 69).

For detailed description of terms and abbreviations, refer to the “Glossary” on page 127.

9.2 WiMAX Configuration

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

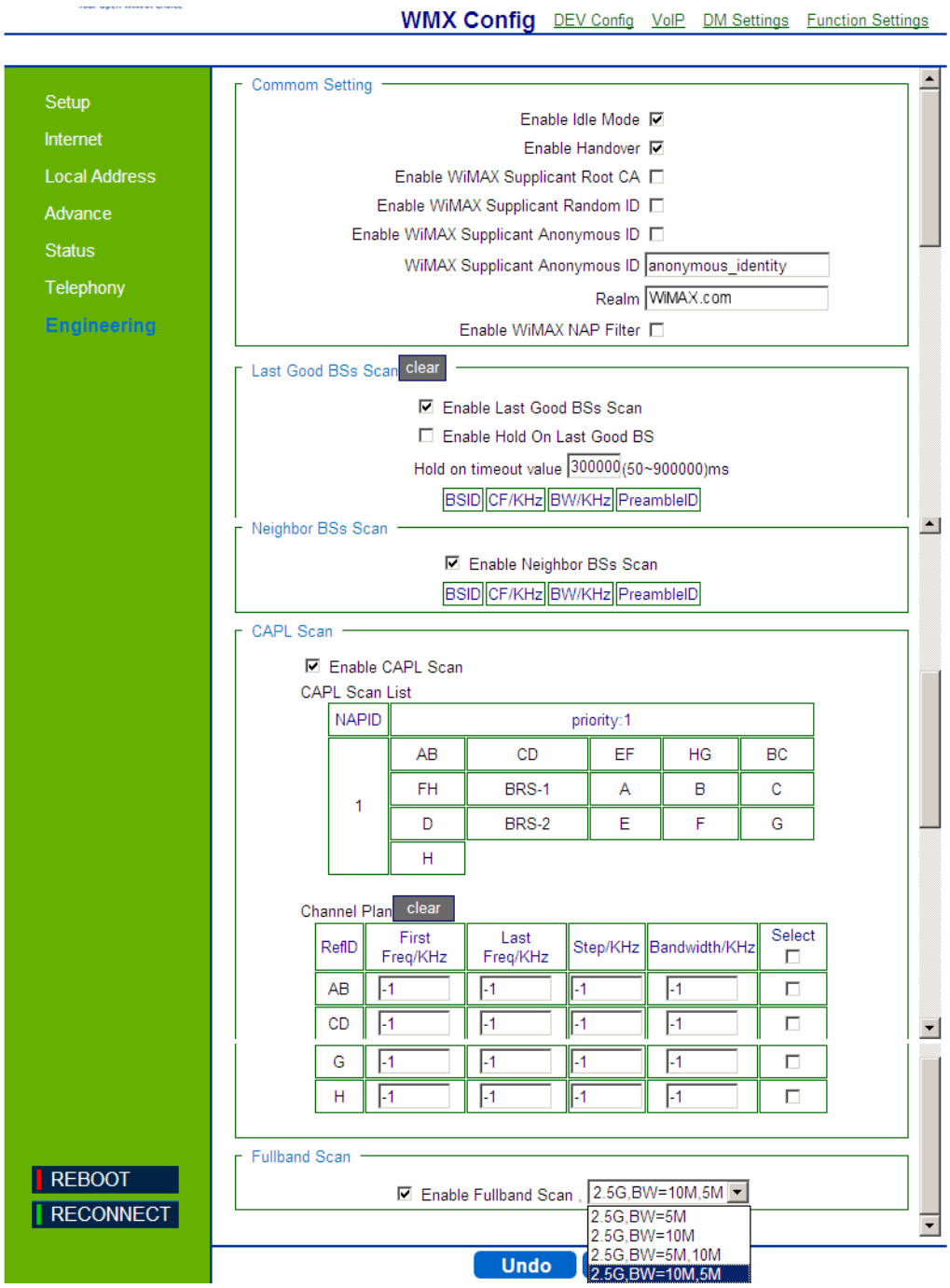


Figure 9-1: Engineering - WiMAX Config.

The following table describes the WMAX Configuration parameters:

Table 9-1: WMAX Config. Settings

Parameter	Description	Default	Possible Values
Common Settings			
Enable Idle Mode	Select this checkbox to enable Idle Mode -the CPE is completely deregistered from the network, however will continue to scan the network and keep track of its location	Enable	Enable/disable
Enable Handover	Select this checkbox to enable Handover - transfer to another BS during mobility	Enable	Enable/disable
Enable WiMAX Supplicant Root CA	IOT AAA root certificates are predefined in the CPE. Select this checkbox to allow the CPE to verify BS's certification.	Disable	Enable/disable
Enable WiMAX Supplicant Random ID	Select this checkbox to assign a random ID to the Supplicant. If disabled - the ID is the MAC_Address@realm.	Enable	Enable/disable
Enable WiMAX Supplicant Anonymous ID	If enabled, the unit will use "WiMAX Supplicant Anonymous ID" as anonymous identity, else the unit will use MAC_Address@realm instead.	Disable	Enable/disable
WiMAX Supplicant Anonymous ID	Enter the WiMAX Supplicant Anonymous ID to be used.	anonymous _identity	Up to 128 characters
Realm	The WiMAX domain	WiMax.com	
Enable WiMAX NAP Filter	Enables filtering Network Access Provider. If it is enabled - network provider ID will be checked for network entry.	Disable	Enable/disable

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

Parameter	Description	Default	Possible Values
Last Good BS Scan			
Table of Last Good BSs	Define the following: ■ BSID -Base Station ID ■ CF/KHz - Channel Frequency ■ BW/KHz - Bandwidth in KHz ■ PreambleID - The Preamble ID of the BS Use the **Clear** button to delete a saved last good BS from the list.	N/A	N/A
Enable Last Good BSs Scan	The system will try to scan with the previous good BS to speed up the scan duration. A “good BS” is defined as one with which the CPE can get an IP address.	Enable	Enable/disable
Enable Hold On Last Good BS	Save the ID for the next scan	Disable	Enable/disable
Hold on timeout value	Enter the period of time (in miliseconds) to keep referring to this BS as the Last Good BS when connection is not optimal.	300,000	50~900,000 ms
Neighbor BS Scan			
Enable Neighbor BS Scan	The system will try to scan the neighbor BS to the previous BS defined in “Last good BS”. The neighbor BS details will appear in the table ofthis section.	Enable	Enable/disable
CAPL BS Scan (Channel Allocation Priority Level)			
Enable CAPL BS Scan	Channel Allocation Priority Level - The CAPL scan list is defined by the customer provisioned list. Priority is the customer defined priority scan order. Higher priority will be scanned first.	Enable	Enable/disable
Channel Plan	Define the channel plan by adding the Ref IDs, in order to map the IDs into a scan list.	N/A	

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

Parameter	Description	Default	Possible Values
Fullband Scan			
Enable Fullband Scan	The system will try to scan the whole frequency band (125kHz for the frequency step) with user specified bandwidth as follows: ■ For 2.xGHz: 5 MHZ, 10 MHz, or Auto (5, 10 or 10,5) MHz ■ For 3.xGHz: 5 MHz, 7 MHz, 10 MHz, or Auto (10, 5, 7) MHz	Enable	Enable/disable

9.3 Device Configuration

In this page you save and export all the parameters currently set on the device, packed in a file, to your PC. This file will be used as a configuration template in order to apply the same settings to other CPEs. The format of the exported file is **.tar*, which will have to be converted into an **.ipk* file format using the Auto-configuration tool (see "Configuring the CPE Using the WiMAX Modem Application CD" on page 31).

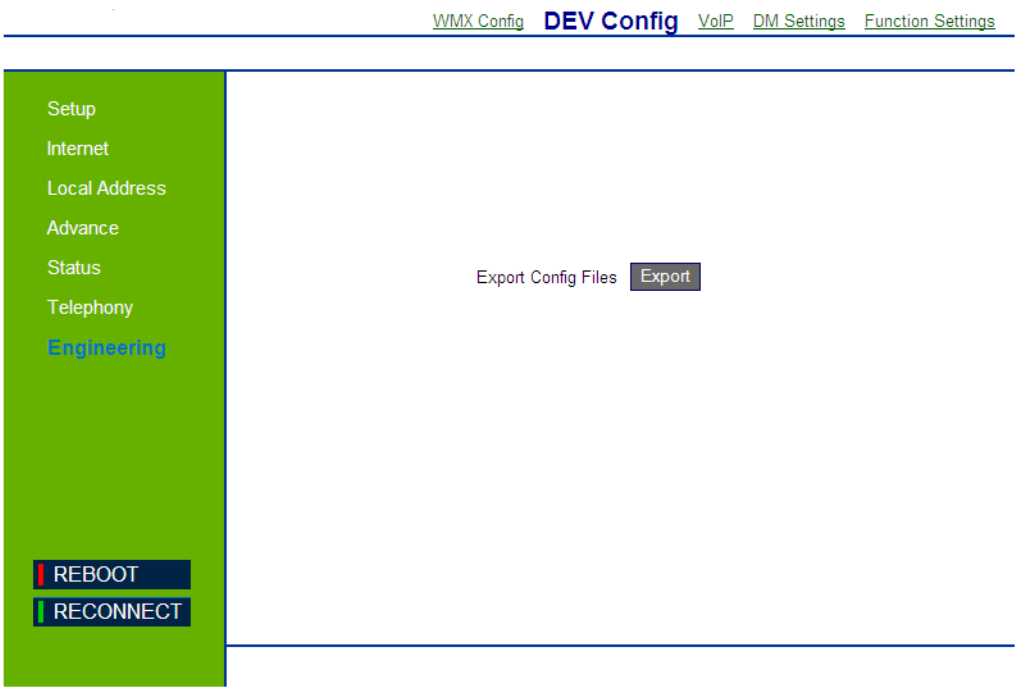


Figure 9-2: Engineering - DEV Config.

To save and export the current device settings:

1. Set the device parameters as required in each of the application pages. Be sure to click **Apply** to activate your changes.
2. In the Dev Config page click **Export** to save the current settings and export as a conig file.
3. Save the file (.*tar format) for mass CPE configuration (see "Creating a Default Configuration File" on page 36).

9.4 VoIP Configuration

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 a analog signal (your voice) into a digital signal (data packets) and then back into an analog signal.

The BreezeMAX Si 4000 CPE uses Session Initiation Protocol (SIP) as the control mechanism that sets up, initiates, and terminates calls between a caller and a called party. The SIP messaging makes use of “Proxy,” “Redirect,” and “Registration” servers to process call requests and find the location of called parties across the Internet. When SIP has set up a call between two parties, the actual voice communication is a direct peer-to-peer connection using the standard Real-Time Protocol (RTP), which streams the encoded voice data across the network.

You can make VoIP calls by connecting a regular phone to one of the BreezeMAX Si 4000 CPE’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 4000 CPE, you must have an account with a SIP service provider and configure the required parameters through the web interface. The BreezeMAX Si 4000 CPE allows the two RJ-11 Phone ports to be configured separately with different settings.

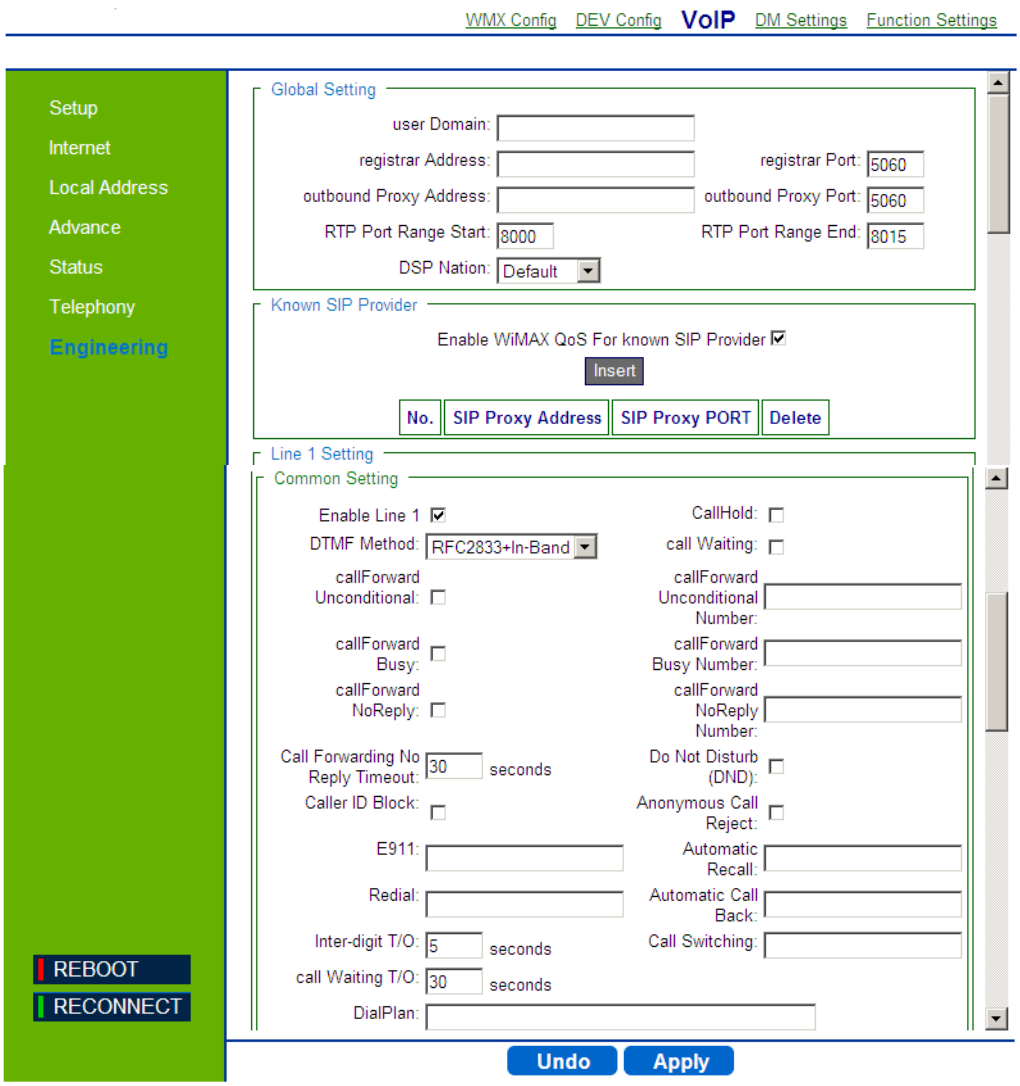


Figure 9-3: Engineering - VoIP

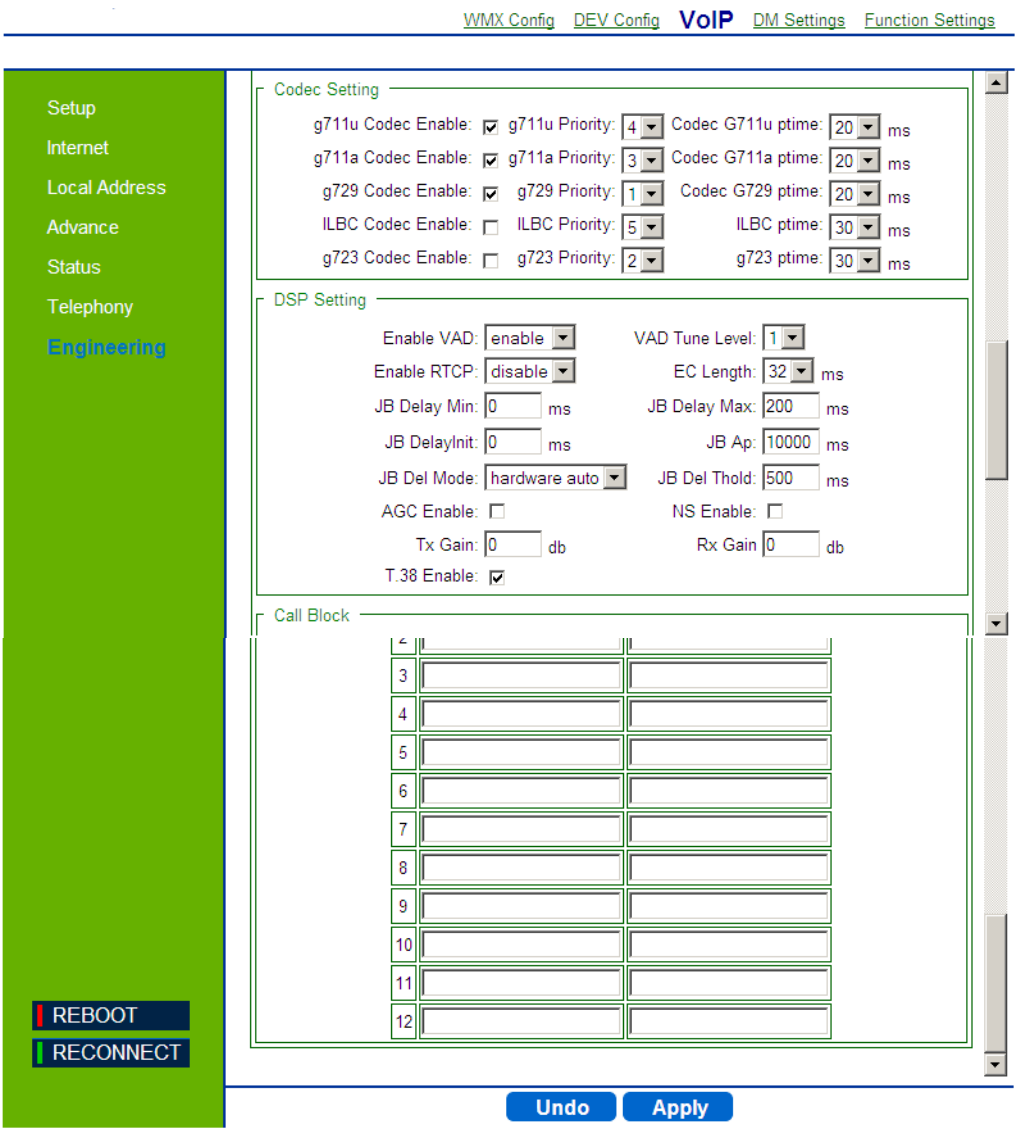


Figure 9-4: Engineering - VoIP (continued)

The following table describes the VoIP Settings parameters:

Table 9-2: VoIP Settings

Parameter	Description	Default	Possible Values
Global Settings			
user Domain	The host portion of the SIP Uniform Resource Identifiers (URIs) that are assigned to users in a network. The SIP domain name can sometimes be different from the internal network domain name.	N/A	Up to 256 characters
registrar Address	The IP address of the SIP registrar server. A registrar is a server that accepts SIP register requests and places the information it receives in those requests into the location service for the domain it handles.	N/A	Up to 256 characters
registrar Port	The TCP port number used by the VoIP service provider's register server.	5060	Range: 1030 to 65535
outbound Proxy Address	Address of the VoIP service provider SIP proxy server.		Up to 256 characters
outbound Proxy Port	The TCP port number used by the VoIP service provider's SIP proxy server.	5060	Range: 1030 to 65535
RTP Port Range Start	Enter the port Start and End to define the range that Real-time Transport Protocol will use	8000	Range: 1030 to 65535
RTP Port Range End		8015	
DSP Nation	National protocol definition	Default	
Caller ID	Select the standard by which the caller is identified: ■ Bellcore - (Bell Communications Research) - used in the USA, Canada, Australia, China, Hong Kong and Singapore ■ ETSI FSK - European Telecommunications Standards Institute Frequency Shift Keying - ■ V-23 FSK - developed by NTT in Japan ■ BT=>4 - British Telecom standard	Bellcore	

Table 9-2: VoIP Settings (Continued)

Parameter	Description	Default	Possible Values
Known SIP Provider			
Enable WiMAX QoS For known SIP Provider	(Not available for this CPE) This check-box enables the CPE to select the quality of service level from a known SIP. This feature is used for MS initial service -flow.	N/A	Enable/disable
List of SIP providers	Click **Insert** to add a known SIP provider to the list and specify the SIP Proxy address and Proxy port. To remove from the list, click **Del**.	N/A	
Line 1 Settings - Common Settings			
Enable Line 1	To enable voice feature		Enable/disable
DTMF Method	Enable the sending of dual-tone multi-frequency (touch tone) phone signals over the VoIP connection: ■ InBand - The DTMF signals are sent over the RTP voice stream. ■ RFC2833 - Relay the DTMF signals over the RTP voice stream without any distortion ■ RFC2833+InBand - Uses the best method depending on the called party. ■ SIPInfo - Uses the data from SIP	RFC2833+ InBand	InBand, RFC2833, RFC2833+InBand, SIPInfo
callForward Unconditional	Forwards an incoming call to another number for all calls.	Disable	Enable/disable
callForward Unconditional Number	Enter the number to which to forward all incoming calls.	N/A	Up to 256 characters
callForward Busy	Forwards an incoming call to another number when the current line is busy.	Disable	Enable/disable
callForward Busy Number	Enter the number to which to forward incoming calls when the current line is busy.	N/A	
callForward NoReply	Incoming calls are forwarded to another phone number only if there is no answer after a pre-configured timeout.	Disable	Enable/disable
Call Forwarding No Reply Timeout	The time (in seconds) a call waits for an answer before being forwarded to the number specified in callForward NoReply	30 seconds	N/A

Table 9-2: VoIP Settings (Continued)

Parameter	Description	Default	Possible Values
callForward NoReply Number	Enter the number to which to forward incoming calls when there is no reply from current line.	N/A	
Caller ID Block	Select this check-box to hide your name and number when calling another number.	Disabled	Enable/disable
E911	Emergency call: Enter a number that will be referref as the emergency call. When dialing “911” this call will be routed to the emergency service.	N/A	
Redial	Enter a shortcut (e.g. *53) to define redialing to the last number		
Inter-digit T/O	timeout in seconds		
call Waiting T/O	timeout in seconds		
DialPlan	Establish the expected number and pattern of digits for a telephone number		
CallHold	Enables holding the line while speaking with one participant in a conversation .		Enable/disable
call Waiting	Enables suspending the current telephone call and switch to a new incoming call.		Enable/disable
Do Not Disturb(DND)	Select this checkbox to reject any incoming calls. The call will result in Busy tone.	Disable	Enable/disable
Anonymous Call Reject	Select this checkbox to block calls from an unidentified number.	Disable	Enable/disable
Automatic Recall	Return call: Enables calling back the number whose call you missed by pressing some buttons.		Enable/disable
Automatic Call Back	Repeat dial if busy: automatically redial the number time and again, until the recipient's line is free. Then your phone will ring back when you are being connected.		Enable/disable
Call Switching	Set a shortcut (e.g. *66) to enable switching from one phone to another without hanging up. Switching is done by pressing the flash button and dialing the shortcut number.		
Codec Setting			

Table 9-2: VoIP Settings (Continued)

Parameter	Description	Default	Possible Values
g711u Codec Enable	The ITU-T G.711 with mu-law standard codec that uses Pulse Code Modulation (PCM) to produce a 64 Kbps high-quality voice data stream. This standard is used in North America and Japan.	Enable	Enable/disable
g711u Priority	The priority of codec by which the unit will attempt to use for best voice quality	Fourth priority	
g711u ptime	Set the time (in miliseconds) for the unit to attempt to use the codec highest priority in the list before trying the next lower one.	30 ms	
g711a Codec Enable	(G711.aLaw): The ITU-T G.711 with A-law standard codec that uses Pulse Code Modulation (PCM) to produce a 64 Kbps high-quality voice data stream. This standard is used in Europe and most other countries around the world.	Enable	Enable/disable
g711a Priority	The priority of codec by which the unit will attempt to use for best voice quality	Third priority	
g711a ptime	Set the time (in miliseconds) for the unit to attempt to use the codec highest priority in the list before trying the next lower one.	30 ms	
g729 Codec Enable	The ITU-T G.729ab standard codec that uses Conjugate Structure Algebraic-Code Excited Linear Prediction (CS-ACELP) with silence suppression to produce a low-bandwidth data stream of 8 Kbps. Note that DTMF and fax tones do not transport reliably with this codec, it is better to use G.711 for these signals.	Enable	Enable/disable
g729 Priority	The priority of codec by which the unit will attempt to use for best voice quality	First priority	
g729 ptime	Set the time (in miliseconds) for the unit to attempt to use the codec highest priority in the list before trying the next lower one.	30 ms	
ILBC Codec Enable	Internet Low Bitrate Codec	Enable	Enable/disable
ILBC Priority:	The priority of codec by which the unit will attempt to use for best voice quality	Last priority	
ILBC ptime	Set the time (in miliseconds) for the unit to attempt to use the codec highest priority in the list before trying the next lower one.	30 ms	

Table 9-2: VoIP Settings (Continued)

Parameter	Description	Default	Possible Values
DSP Setting (Digital Signal Processing)			
Enable VAD	Voice Activity Detection - detects the periods of silence in the audio stream so that it is not transmitted over the network.	Enable	Enable/Disable
VAD Tune Level	VAD threshold can be tuned according to the guideline below: 1 Best bandwidth saving; but lowest quality for high noise level. 2 Bandwidth saving is reduced and quality is improved from Option 1. Noise level above 'very loud noise' (about 5 dB SNR) is detected as voice. 3 Bandwidth saving is reduced and quality is improved from Option 2. Noise level above 'loud noise' (about 10dB SNR) is detected as voice. 4 Bandwidth saving is reduced and quality is improved from Option 3. Noise level above 'less loud noise' (about 20dB SNR) is detected as voice. 5 Least bandwidth saving; but highest quality. Noise level above 'audible noise' (about 30dB SNR) is detected as voice.	1	1 - 5
Enable RTCP	Select this check-box to enable Real-time Transport Control Protocol	Enable	Enable/Disable
EC Length	Echo Cancellation - Sets the delay time (in miliseconds) for voice echo cancellation. A voice echo can be created on some two-wire phone loops, which becomes increasingly louder and annoying when there is a long delay. If voice echo is a problem during a call, you can adjust this parameter to try and reduce or remove it.	32	16, 32, 48
JB Delay Min	Jitter Buffer control: JB delays the arriving packets so that the end user experiences a clear connection with very little sound distortion. Set the minimum and maximum jitter buffer delay time (in miliseconds)		
JB Delay Max			

Table 9-2: VoIP Settings (Continued)

Parameter	Description	Default	Possible Values
JB DelayInit	The initial delay of the jitter buffer in miliseconds. The system holds the 1st received packet for the time defined in DelayInit before sending it out.		
JB AP	Jitter Buffer Adaptation Period: controls the speed (in milliseconds) at which the jitter buffer can adapt downwards when current network conditions allow. The larger the value, the slower the jitter buffer adapts down, when jitter decreases.	max. 10000ms (10 seconds) min.1000ms (1 second)	Max value of AP is 65.535
JB Del Mode	Determines how frames are deleted when jitter buffer adapts down: ■ Hardware auto - places more emphasis on maximum delay, which may negatively affect audio quality. ■ Software auto - places more emphasis on audio quality, while maximum delay may be exceeded		hardware auto, software auto
JB Del Thold	JB Deletion Threshold (in miliseconds). Frames exceeding the deletion threshold are deleted immediately. Audio quality may be negatively affected.		From the DelayMax value up to 500 ms
AGC Enable	Select this check-box to enable Automatic Gain Control. Voice signal will be enlarged by DSP so that the voice is louder and clearer.	Disabled	Enable/disable
NS Enable	Select this check-box to enable Noise Suppression (eliminating noise).	Disable	Enable/disable
Tx Gain	Enter a value (in db) to control the voice transmission quality	0	-5 to +5
Rx Gain	Enter a value (in db) to control the voice receiving quality	0	-5 to +5
T.38 Enable	Select this checkbox to send fax messages over the VoIP network from a fax machine connected to one of the RJ-11 Phone ports on the unit.	Enable	Enable/disable
Call Block			
Incoming	Blocks incoming calls from the listed numbers.	N/A	up to 256 digits
Outgoing	Blocks outgoing calls from the listed numbers.	N/A	

9.5 DM (Device Management) Settings (TR-069)

NOTE

OMA DM option is currently not supported.

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

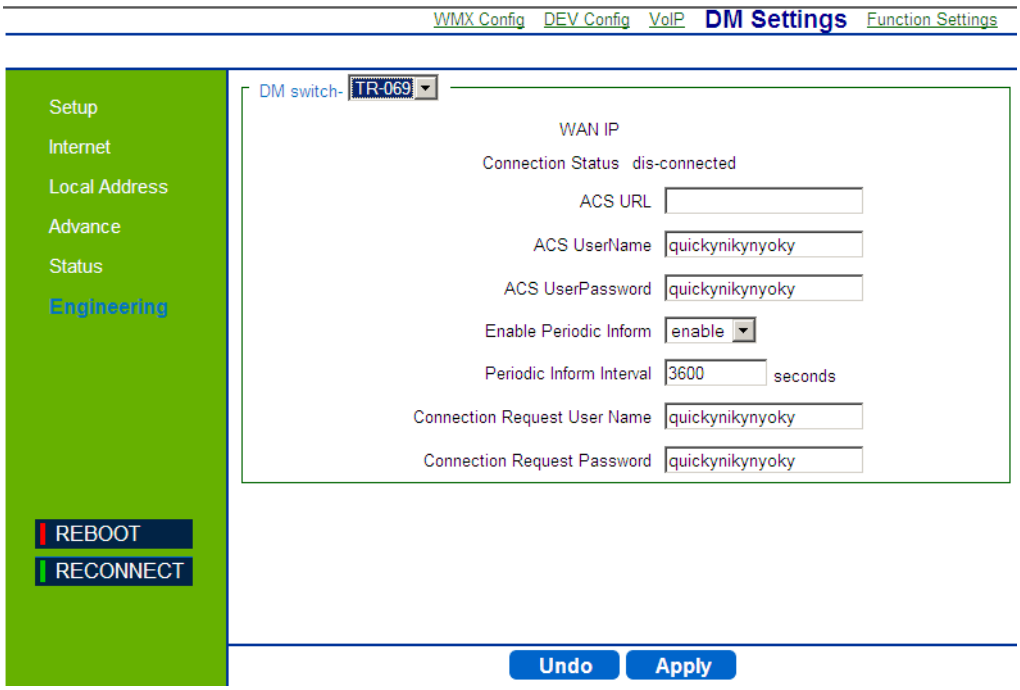


Figure 9-5: Engineering - DM Settings (TR-069)

The following table describes the configurable TR-069 parameters:

Table 9-3: DM Settings - TR-069

Parameter	Description	Default	Possible Values
Connection Status	Displays the CPE connection state	N/A	Connected/disconnected
ACS URL	Enter the URL of the ACS server	N/A	N/A
ACS UserName	Enter the username for the ACS application	quickynikynoky	Up to 256 characters
ACS UserPassword	Enter the password for the ACS application	quickynikynoky	Up to 256 characters
Enable Periodic Inform	Select this check-box to enable the CPE to send periodical information messages to the ACS	Enable	Enable/disable
Periodic Inform Interval	Set the interval (in seconds) for sending messages from CPE to ACS	3600 seconds	Less than defined in StarACS
Connection Request User Name	Enter the CPE username for connecting with ACS.	quickynikynoky	Up to 256 characters
Connection Request Password	Enter the CPE password for connecting with ACS.	quickynikynoky	Up to 256 characters

9.6 Function Settings

In this page you reserve DSCP (Differentiated Services Code Point) markings for classification settings.

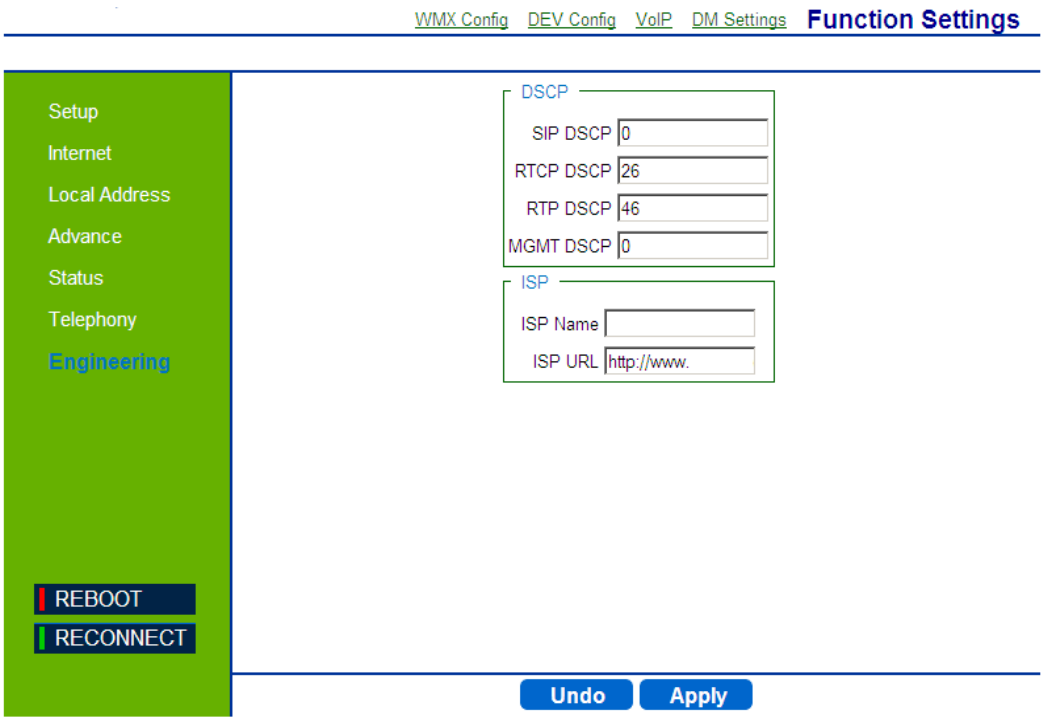


Figure 9-6: Engineering - Function Settings

Table 9-4: Function Settings

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

Chapter 10

Troubleshooting

In This Chapter:

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

Check the following before contacting local Customer Support.

1 If you cannot access the Internet from the PC, check the following:

- If you cannot access the Internet, be sure your Windows system is correctly configured for TCP/IP. The IP settings should be set to “obtain an IP address automatically”.
- You may be out of the service area of the WiMAX base station. Check with the WiMAX service provider for service coverage information.
- If you cannot resolve the problem, check the System Status page of the web interface and contact your WiMAX service provider.

2 If the management interface cannot be accessed using a web browser:

- Be sure the management station is correctly configured for TCP/IP. The IP settings should be set to “obtain an IP address automatically.”
- Try a Ping command from the management station to the unit’s IP address to verify that the entire network path between the two devices is functioning correctly.
- Check that the management station has a valid network connection and that the Ethernet port that you are using has not been disabled.
- Check the network cabling between the management station and the unit. If the problem is not resolved, try using a different port or a different cable.

3 Forgot or Lost the Password

- Set the unit to its default configuration by pressing the reset button on the rear panel for 5 seconds or more. Then use the default password “Alvarion” to access the management interface.

NOTE

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

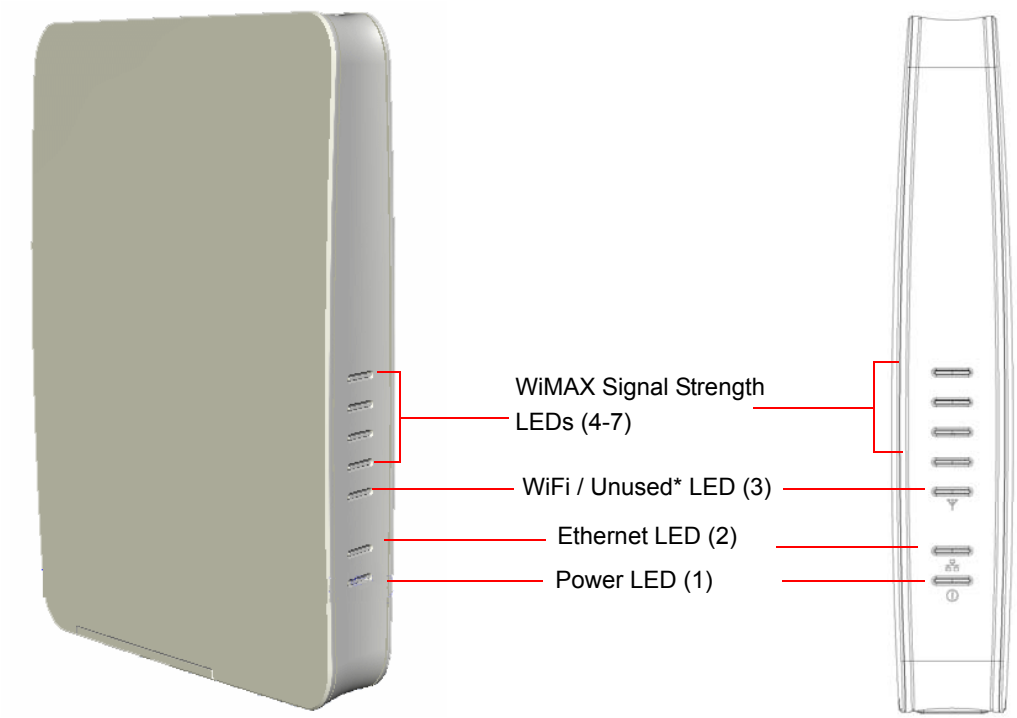
4 If all other recovery measures fail and the unit is still not functioning properly, take either of these steps:

- Reset the unit using the web interface, or through a power reset.
- Reset the unit to its factory default configuration by pressing the reset button on the rear panel for 5 seconds or more. Then use the default user

name and password to access the management interface (see “Accessing the Web Management Interface” on page 28).

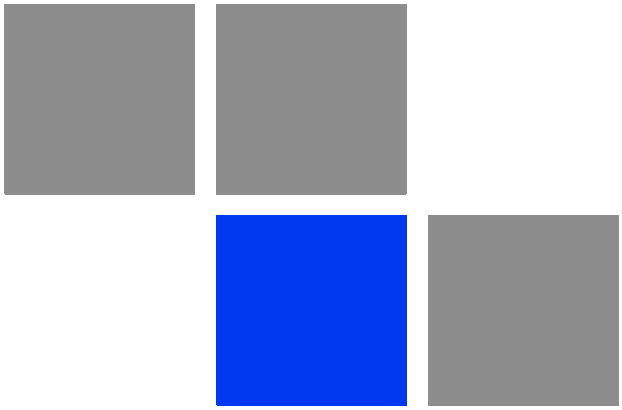
Table 10-1: Troubleshooting Chart

Ports	Description
■ Power LED is Off	■ AC power adapter may be disconnected. Check connections between the unit, the AC power adapter, and the wall outlet.
■ WiMAX LED is Off	■ Check with the WiMAX service provider for service coverage information.
■ WiMAX Signal Strength LEDs are Off	■ Change the location of the unit, to a nearby window or an upper floor if possible. Keep away from metal objects. ■ Check with the WiMAX service provider for service coverage information.
■ LAN link LED is Off	■ Verify that the unit and attached device are powered on. ■ Be sure the cable is plugged into both the unit and corresponding device. ■ Verify that the proper cable type is used and its length does not exceed specified limits. ■ Check the cable connections for possible defects. Replace the defective cable if necessary.



* WiFi LED (3) in 3.5 GHz models, unused LED in 2.5 GHz models

Figure 10-1: BreezeMAX Si 4000Front Panel



Glossary

100BASE-TX	IEEE 802.3u specification for 100 Mbps Fast Ethernet over two pairs of Category 5 or better UTP cable.
10BASE-T	IEEE 802.3 specification for 10 Mbps Ethernet over two pairs of Category 3 or better UTP cable
Advanced Encryption Standard (AES)	An strong encryption algorithm that implements symmetric key cryptography.
Access List (ACL)	A list of MAC addresses which are allowed to access the device
Automatic Gain Control (AGC)	Automatic electronic regulation by recording devices of video and audio signals at a predetermined rate (by electronic control).
Authentication	The process to verify the identity of a client requesting network access. IEEE 802.11 specifies two forms of authentication: open system and shared key.
Auto-negotiation	Signalling method allowing each node to select its optimum operational mode (speed and duplex mode) based on the capabilities of the node to which it is connected.
Best Effort (BE)	One of the five QoS service types defined in the IEEE 802.16 WiMAX.
Base Station	A WIMAX service provider's equipment that is installed at a fixed location to provide network connectivity for subscriber stations within a defined service area.
Broadcast Key	Broadcast keys are sent to stations using 802.1X dynamic keying. Dynamic broadcast key rotation is often used to allow the access point to generate a random group key and periodically update all key-management capable wireless clients.
Channel Allocation Priority Level (CAPL)	CAPL scan list is defined by the customer provisioned list. There are some parameters with CAPL scan: NAPID, priority and RefID. NAPID is used to filter some BS if the NAPID is not matched. Priority is the customer defined priority scan order. Higher priority will be scanned first. RefID is a result of mapping from IDs into a scan list from the channel plan.

CINR	Carrier to Interference-plus-Noise Ratio (CINR), expressed in decibels (dBs), is a measurement of signal effectiveness. The carrier is the desired signal, and the interference can either be noise or co-channel interference or both. In order for the signal receiver to be able to decode the signal, the signal must fall into an acceptable CINR range, which differs with the technology used (i.e., CDMA, GSM, etc.).
Clear to Send (CTS)	Signal that gives a modem permission to send data.
Customer Premise Equipment (CPE)	Customer Premise Equipment: Communications equipment that resides on the customer's premises.
Dynamic Host Configuration Protocol (DHCP)	A protocol used to assign IP addresses to computers on a Microsoft NT local area network
Domain Name System (DNS)	A mechanism used for translating host names for network nodes into IP addresses.
Dynamic Domain Name System (DDNS)	A method, protocol, or network service that provides the capability for a networked device to notify a domain name server to change the active DNS configuration of its configured hostnames, addresses or other information stored in DNS, in real-time.
Dynamic Host Control Protocol (DHCP)	Dynamic Host Configuration Protocol: Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.
(“Demilitarized Zone”) DMZ	A server that acts as "neutral zone" and separates an internal network from a public one (in order to prevent outside access to a company's private data.
Data/Digital Signal Processor (DSP)	A system that controls voice quality
Differentiated Services Code Point (DSCP)	A field in the header of IP packets for packet classification purposes.
Dual Tone Multi Frequency (DTMF)	Allocation of a unique tone to each button on an appliance (made up of two frequencies - high and low) that allows a computer to recognize the tone.
Extended Real-time POLLING SERVICE (ertPS)	One of the five QoS service types defined in the IEEE 802.16 WiMAX.

Ethernet	A popular local area data communications network, which accepts transmission from computers and terminals.
Ethernet Conversion Sublayer (ETH CS)	A mode in which transmitted packets contain an 802.3 header
Encryption	Data passing between the SU-A-EZ and clients can use encryption to protect from interception and evesdropping.
Extended Service Set (ESS)	Extended Service Set: More than one wireless cell can be configured with the same Service Set Identifier to allow mobile users can roam between different cells with the Extended Service Set.
Extensible Authentication Protocol (EAP)	An authentication protocol used to authenticate network clients. EAP is combined with IEEE 802.1X port authentication and a RADIUS authentication server to provide “mutual authentication” between a client, the access point, and the a RADIUS server
EAP-Tunneled Transport Layer Security (EAP-TTLS)	An EAP protocol that extends TLS. (see “Transport Layer Security (TLS)” on page 134)
File Transfer Protocol (FTP)	File Transfer Protocol: A TCP/IP protocol used for file transfer.
Hypertext Transfer Protocol (HTTP)	Hypertext Transfer Protocol: HTTP is a standard used to transmit and receive all data over the World Wide Web.
IDENT	An Internet protocol that helps identify the user of a particular TCP connection.
IEEE 802.16e	A standard that provides mobile broadband wireless access using Scalable Orthogonal Frequency Division Multiple Access (SOFDMA).
Internet Low Bitrate Codec (iLBC)	A free speech codec suitable for robust voice communication over IP. The codec is designed for narrow band speech and results in a payload bit rate of 13.33 kbit/s with an encoding frame length of 30 ms and 15.20 kbps with an encoding length of 20 ms. The iLBC codec enables graceful speech quality degradation in the case of lost frames, which occurs in connection with lost or delayed IP packets.
IP Conversion Sublayer (IP-CS)	A mode in which transmitted packets contain an 802.3 header
Itsy Package Management System (IPKG, ipkg)	Itsy Package Management System - a lightweight package management system designed for embedded devices.

Internet Protocol Security (IPsec)	A protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream.
Jitter Buffer (JB)	A shared data area where voice packets can be collected, stored, and sent to the voice processor in evenly spaced intervals. Variations in packet arrival time, called jitter, can occur because of network congestion, timing drift, or route changes. The jitter buffer, which is located at the receiving end of the voice connection, intentionally delays the arriving packets so that the end user experiences a clear connection with very little sound distortion.
Local Area Network (LAN)	Local Area Network: A group of interconnected computer and support devices.
Layer 2 Tunneling Protocol (L2TP)	A tunneling protocol used to support virtual private networks (VPNs).
Media Access Control (MAC)	Media Access Control: The lower of the two sub-layers of the data link layer defined by the IEEE. The MAC sub-layer handles access to shared media, such as whether token passing or contention will be used.
MAC Address	Standardized data link layer address that is required for every port or device that connects to a LAN. Other devices in the network use these addresses to locate specific ports in the network and to create and update routing tables and data structures. MAC addresses are 6bytes long and are controlled by the IEEE.
Maximum Transmission Unit (MTU)	Largest size of a data packet or frame that can be sent in one complete unit over a packet-based computer network
Multiple Input Multiple Output (MIMO)	Using multiple antennas in a Wi-Fi device to improve performance and throughput.
MSCHAPV2 (MS-CHAP. v2)	Microsoft version of the Challenge-handshake authentication protocol, version 2. MS-CHAPv2 provides mutual authentication between peers by adding a peer challenge upon the Response packet and an authenticator response on the Success packet.

Network Access Point (NAP)	Network exchange point equipped with large-scale switching facilities and serving as a connection point between individual Internet Service Providers
Network Address Translation (NAT)	A system for reusing IP addresses - The process of modifying network address information in datagram packet headers, while in transit, across a router, in order to remap a given address space into another.
Network Time Protocol (NTP)	NTP is a protocol designed to synchronize the clocks of computers over a network. The time servers operate in a hierarchical-master-slave configuration in order to synchronize local clocks within the subnet and to national time standards via wire or radio.
Open Mobile Alliance (OMA)	OMA DM (device Management) is a protocol specified by Open Mobile Alliance (OMA) for Device Management purposes, by the Device Management Working Group and the Data Synchronization (DS) Working Group.
Orthogonal Frequency Division Multiplexing (OFDM)	Orthogonal Frequency Division Multiplexing: OFDM allows multiple users to transmit in an allocated band by dividing the bandwidth into many narrow bandwidth carriers.
Physical Layer Device (PHY)	The term used for a transceiver in Fast Ethernet and Gigabit Ethernet systems.
Plain Old Telephone Service (POTS)	Standard analog telephone service, regular telephone line without extra enhancements
Power Over Ethernet (PoE)	Power over Ethernet: A specification for providing both power and data to low-power network devices using a single Category 5 Ethernet cable. PoE provides greater flexibility in the locating of Wi²s and network devices, and significantly decreased installation costs.
Point to Point Tunneling Protocol (PPTP)	This protocol enables the transfer of data packets of TCP / IP through a foreign network that is not based on these protocols (by marking the packet with an address suited to the foreign network)
Quadrature Phase Shift Keying (QPSK)	A digital modulation scheme that conveys data by changing, or modulating, the phase of a reference signal (the carrier wave).

Received signal strength indication (RSSI)	A measurement of the power present in a received radio signal. RSSI is generic radio receiver technology metric, which is usually invisible to the user of device containing the receiver, but is directly known to users of wireless networking of IEEE 802.11 protocol family.
Real-time Transport Protocol (RTP)	The Real-time Transport Protocol (RTP) defines a standardized packet format for delivering audio and video over the Internet.
Real-time Transport Control Protocol (RTCP)	Real-time Transport Control Protocol (RTCP) is a sister protocol of the Real-time Transport Protocol (RTP). RTCP provides out-of-band control information for an RTP flow. It partners RTP in the delivery and packaging of multimedia data, but does not transport any data itself. It is used periodically to transmit control packets to participants in a streaming multimedia session. The primary function of RTCP is to provide feedback on the quality of service being provided by RTP.
RTS Threshold	Transmitters contending for the medium may not be aware of each other. RTS/CTS mechanism can solve this “Hidden Node Problem”. If the packet size is smaller than the preset RTS Threshold size, the RTS/CTS mechanism will NOT be enabled.
Service Set Identifier (SSID)	An identifier that is attached to packets sent over the wireless LAN and functions as a password for joining a particular radio cell; i.e., Basic Service Set (BSS).
Session Key	Session keys are unique to each client, and are used to authenticate a client connection, and correlate traffic passing between a specific client and the AU-EZ.
Shared Key	A shared key can be used to authenticate each client attached to a wireless network. Shared Key authentication must be used along with the 802.11 Wireless Equivalent Privacy algorithm.
Session Initiation Protocol (SIP)	An application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. It can be used to create two-party, multiparty, or multicast sessions that include Internet telephone calls, multimedia distribution, and multimedia conferences.
Simple Network Management Protocol (SNMP)	Simple Network Management Protocol: The application protocol in the Internet suite of protocols which offers network management services.

Simple Network Time Protocol (SNTP)	SNTP allows a device to set its internal clock based on periodic updates from a Network Time Protocol (NTP) server. Updates can be requested from a specific NTP server, or can be received via broadcasts sent by NTP servers.
Single Input Single Output (SISO)	A form of antenna technology for wireless communications in which a single antenna at both the transmitter and at the destination (receiver) are used.
Subscriber Station	A general term for a customer's WIMAX terminal equipment that provides connectivity with a base station.
TR-069 (Technical Report 069)	A DSL Forum technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices. It provides the communication between CPE and Auto Configuration Servers (ACS).
Trivial File Transfer Protocol (TFTP)	Trivial File Transfer Protocol: A TCP/IP protocol commonly used for software downloads.
Transport Layer Security (TLS)	A cryptographic protocol that provides security for communications over networks such as the Internet. TLS encrypts the segments of network connections at the Transport Layer end-to-end.
Point to Point Tunneling Protocol (PPTP)	protocol that enables the transfer of data packets of TCP / IP through a foreign network that is not based on these protocols (by marking the packet with an address suited to the foreign network)
Unsolicited Grant Service (UGS)	One of the five QoS service types defined in the IEEE 802.16 WiMAX. It is designed to support real-time service flows that generate fixed-size data packets on a periodic basis, such as T1/E1 and Voice over IP without silence suppression.
User Datagram Protocol (UDP))	Protocol with no connection required between sender and receiver that allows sending of data packets on the Internet (thought unreliable because it cannot ensure the packets will arrive undamaged or in the correct order)

Universal Plug and Play Internet Gateway Device (UPnP IGD)	A set of networking protocols promulgated by the UPnP Forum. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home and in corporate environments for simplified installation of computer components.
UTP	Unshielded twisted-pair cable.
VoicE Activity Detection (VAD	Enables the detection of periods of silence in the audio stream so that it is not transmitted over the network.
Virtual Private Network (VPN)	A private communications network that is based on the public network and uses information security and channeling protocol in order to maintain security of information transferred over the general network.
Wide Area Network (WAN)	Communications network intended to connect between remote local area networks
Wired Equivalent Privacy (WEP)	Wired Equivalent Privacy: WEP is based on the use of security keys and the popular RC4 encryption algorithm. Wireless devices without a valid WEP key will be excluded from network traffic.
Wireless Application Protocol (WAP)	Wireless Application Protocol (WAP) is an open international standard for application-layer network communications in a wireless-communication environment. Most use of WAP involves accessing the mobile web from any mobile device or phone.