BreezeNET® B

System Manual

Legal Rights

Trade Names

Statement of Conditions

Warranties and Disclaimers

Exclusive Warranty

Disclaimer

(a) 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.

(c) 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.

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 Radio Frequency Interference Statement

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

FCC Radiation Hazard Warning

To comply with FCC RF exposure requirement in section 1.1307, the antenna used for this transmitter must be fixed-mounted on outdoor permanent structures with a separation distance of at least 2 meter from al persons for antennas with a gain up to 28 dBi and 2.6 meter for a 31.2 dBi dish antenna, and must not be co-located or operating in conjunction with any other antenna or transmitter.

R&TTE Compliance Statement

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

Safety Considerations

For the following safety considerations, "Instrument" means the BreezeNET B system's components and their cables.

Caution

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

Line Voltage

Before connecting this instrument to the power line, make sure that the voltage of the power source matches the requirements of the instrument.

Radio

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

Outdoor Unit and Antenna Installation and Grounding

Ensure that outdoor units, antennas and supporting structures are properly installed to eliminate any physical hazard to either people or property. Make sure that the installation of the outdoor unit, antenna and cables is performed in accordance with all relevant national and local building and safety codes. Even where grounding is not mandatory according to applicable regulation and national codes, it is highly recommended to ensure that the outdoor unit and the antenna mast (when using external antenna) are grounded and suitable lightning protection devices are used so as to provide protection against voltage surges and static charges. In any event, Alvarion is not liable for any injury, damage or regulation violations associated with or caused by installation, grounding or lightning protection.

Important Notice

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

■ This manual contains proprietary information belonging to Alvarion. 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.

■ 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 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 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 Guide

This manual describes the BreezeNET B Point-to-Point Wireless Bridge Release 3.0 and how to install, operate and manage the system components.

This guide is intended for technicians responsible for installing, setting up and operating the BreezeNET B system, and for system administrators responsible for managing the system.

This guide contains the following chapters and appendices:

■ **Chapter 1** – **System description:** Describes the BreezeNET B system and its components.

■ **Chapter 2** – **Installation:** Describes how to install the system components.

■ **Chapter 3** – **Commissioning:** Describes how to configure basic parameters, align the antenna and validate unit operation.

■ **Chapter 4** – **Operation and Administration:** Describes how to use the BreezeNET B Configuration Utility application for configuring parameters, checking system status and monitoring performance.

■ **Appendix A** – **Software Version Loading Using TFTP:** Describes how to load a new software version using TFTP.

■ **Appendix B** – **File Download and Upload Using TFTP:** Describes how to download and upload configuration files using TFTP. This procedure is also applicable for uploading country code and feature license files.

■ **Appendix C – Using the Restore Link Parameters Utility:** Describes how to use the special Restore Link Parameters utility to enable management access to units where wrong or unknown configuration disables regular access to the unit for management purposes.

■ **Appendix D** – **Preparing the indoor to outdoor cable:** Provides details on preparation of the indoor to outdoor Ethernet cable.

■ **Appendix E** – **Parameters Summary:** Provides an at a glance summary of the configuration parameters, value ranges and default values.

■ **Appendix F – Using the Feature License Web application:** Describes how to use the Feature License web application for getting License Keys.

Contents

Figures

Tables

1

Chapter 1 - System Description

In this Chapter

Introducing BreezeNET B

BreezeNET B is a high performance wireless bridge system that provides high-capacity, high-speed point-to-point links. The BreezeNET B system utilizes advanced technologies to support optimal performance in spectrally polluted environments. BreezeNET B products operate in Time Division Duplex (TDD) mode, using Orthogonal Frequency Division Multiplexing (OFDM) modulation with Forward Error Correction (FEC) coding. Using the enhanced multi-path resistance capabilities of OFDM modem technology, BreezeNET B enables operation in near and non-line-of-sight (NLOS) environments. These qualities enable service providers to reach a previously inaccessible and broader segment of the subscriber population. The system also features adaptive modulation for automatic selection of modulation schemes, including BPSK, QPSK, 16 and 64 QAM to maximize data rate and improve spectral efficiency.

Where allowed by applicable radio regulations, BreezeNET B supports the use of 40MHz frequency channels. When using 40MHz (instead of 20MHz) the BreezeNET B is operating in the "Turbo Mode". The use of this "Turbo Mode" increases the net throughput of the BreezeNET B link, especially for links that suffer from low net throughput due to challenging link budget conditions that result from very long link distances, RF absorbing terrain or non line of sight. Alternatively, the Turbo Mode can extend the range of the BreezeNET B while the capacity is maintained constant.

BreezeNET B supports sensitive applications through optional use of authentication and/or data encryption utilizing WEP or AES algorithm with 128-bit keys. The system supports Virtual LANs based on IEEE 802.1Q, enabling secure operation and Virtual Private Network (VPN) services and enabling tele-workers or remote offices to conveniently access their enterprise network.

BreezeNET B products are currently available in the following frequency bands:

Table 1-1: Frequency Bands	
Band	**Frequencies (GHz)**
5.2	5.150 – 5.350
5.4	5.470 – 5.725
5.8	5.725 – 5.850

The available frequencies, as well as other parameters, depend on applicable local regulations. The actual operating frequencies used by the system can be configured according to applicable radio regulations and specific deployment considerations.

BreezeNET B system components can be managed using standard management tools through SNMP agents that implement standard and proprietary MIBs for remote setting of operational modes and parameters. The BreezeCONFIG utility is an SNMP-based application designed to manage BreezeNET B system components and upgrade unit software versions. The system administrator can use the BreezeCONFIG utility to control any number of units from a single location. In addition, BreezeCONFIG enables loading an updated configuration file to multiple units simultaneously, thus radically reducing the time spent on unit configuration maintenance.

System Components

The BreezeNET B system includes a Base Unit (BU), typically installed at the main site, and a Remote Bridge (RB).

Each unit is comprised of a desktop or wall-mountable Universal Indoor Unit (IDU) and an outdoor unit (ODU). The IDU provides the interface to the user's equipment and is powered from the 110/220 VAC mains. The customer's data equipment is connected via a standard IEEE 802.3 Ethernet 10/100BaseT (RJ 45) interface. The indoor unit is connected to the outdoor unit via a Category 5 Ethernet cable. This cable carries Ethernet traffic between the indoor and the outdoor units, and also transfers power (54 VDC) and control from the indoor unit to the outdoor unit.

The BreezeNET B14 system is comprised of a BU-B14 Base Unit and an RB-B14 Remote Bridge, delivering a total link throughput up to 14 Mbps.

The BreezeNET B28 system is comprised of a BU-B28 Base Unit and an RB-B28 Remote Bridge, delivering a total link throughput up to 22 Mbps.

The ODU contains the processing and radio modules and are available either with an integral flat antenna or with a connection to a detached antenna (D models).

Currently available detached antennas include the following:

Table 1-2: 5 GHz Band Detached Antennas			
Antenna	**Band (GHz)**	**Horizontal Beam Width**	**Gain**
UNI-23-9	5.150-5.875	9°	23 dBi
UNI-28-4	5.150-5.875	4.5°	28 dBi

Specifications

Radio specifications

Table 1-3: Radio Specifications	
Item	**Description**
Frequency[1]	5.2 GHz Family: 5.150 – 5.350 GHz
	5.3 GHz Family: 5.250 – 5.350 GHz
	5.4 GHz Family: 5.470 – 5.725 GHz
	5.8 GHz Family: 5.725 – 5.850 GHz
Operation Mode	Time Division Duplex (TDD)
Channel Bandwidth[1]	20, 40 (Turbo Mode) MHz
Central Frequency Resolution	10 MHz
ODU Integral Antenna	21dBi in the 5.150-5.875 GHz band. 10.5^o horizontal x 10.5^o vertical, vertical polarization, compliant with EN 302 085 V1.1.1 Range 1, Class TS 1, 2, 3, 4, 5
Detached 5 GHz Antennas[2]	■ UNI-23-9: 23dBi, 5.150-5.875 GHz, 9° horizontal x 9° vertical, vertical polarization, compliant with EN 302 085 V1.1.2 (2001-2002) ■ UNI-28-4: 28dBi, 5.150-5.875 GHz, 4.5^o horizontal x 4.5^o vertical, vertical polarization, compliant with EN 302 085 V1.1.2 (2001-2002).
Antenna Port (D-model ODU)	N-Type, 50 ohm
Max. Input Power (at antenna port)	-30dBm typical
Maximum Output Power[3]	21 dBm.

Table 1-3: Radio Specifications			
Item	**Description**		
Sensitivity, typical (dBm at antenna port, PER<10%, 20 MHz bandwidth[4])	Modulation Level[5]	Sensitivity	Min. SNR
	1	-89 dBm	6 dB
	2	-88 dBm	7 dB
	3	-86 dBm	9 dB
	4	-84 dBm	11 dB
	5	-81 dBm	14 dB
	6	-77 dBm	18 dB
	7	-73 dBm	22 dB
	8	-71 dBm	23 dB
Modulation	OFDM modulation, 64 FFT points; BPSK, QPSK, QAM16, QAM64		

[1] The actually available frequency channels and bandwidth are defined by the selected Sub-Band, which reflects the applicably regulatory constraints. For more details refer to Show Country Dependent Parameters on page 4-8).

[2] In 5.4 GHz units with a detached antenna, if the gain of the antenna (as inserted into Antenna gain field) is higher than 30dBm, then the Maximum EIRP can vary by more than +/-3dB. Since regulations in most countries limit the EIRP of units operating in the 5.4 GHz band, it is recommended to use detached antennas up to and including 28dBi.

[3] The actually available maximum output power for each modulation level is defined by the selected Sub-Band, which reflects the applicably regulatory constraints. For some countries the power may also be limited by limitations on the maximum EIRP (also included in the Sub-Band parameters) and the Antenna Gain parameter. For more details refer to Show Country Dependent Parameters on page 4-8 and to Transmit Power on page 4-54. For information on specific HW and Country Code limitations, see the Country Codes document.

[4] The sensitivity values are for a bandwidth of 20 MHz. When using a 40 MHz bandwidth ("Turbo mode"), the Sensitivity for each modulation level is higher by 3 dB.

[5] Modulation Level indicates the radio transmission rate and the modulation scheme. Modulation Level 1 is for the lowest radio rate and modulation scheme.

Data Communication

<table>
<tr><td colspan="2" align="center">Table 1-4: Data Communication</td></tr>
<tr><td>Item</td><td>Description</td></tr>
<tr><td>Standard compliance</td><td>IEEE 802.3 CSMA/CD</td></tr>
<tr><td>VLAN Support</td><td>Based on IEEE 802.1Q</td></tr>
<tr><td>Layer-2 Traffic Prioritization</td><td>Based on IEEE 802.1p</td></tr>
<tr><td>Layer-3 Traffic Prioritization</td><td>IP ToS according to RFC791</td></tr>
</table>

Configuration and Management

<table>
<tr><td colspan="2" align="center">Table 1-5: Configuration and Management</td></tr>
<tr><td>Type</td><td>Standard</td></tr>
<tr><td>Management</td><td>Via Telnet
SNMP based Configuration Utility
Configuration upload/download</td></tr>
<tr><td>Management Access</td><td>From Wired LAN, Wireless Link</td></tr>
<tr><td>Management access protection</td><td>Multilevel password
Configuration of remote access direction (from Ethernet only, from wireless link only or from both)
Configuration of IP addresses of authorized stations</td></tr>
<tr><td>Security</td><td>Authentication messages encryption option
Data encryption option
WEP or AES 128-bit encryption standards
ESSID</td></tr>
<tr><td>SNMP Agents</td><td>SNMP ver 1 client, MIB II, Bridge MIB, Private MIB</td></tr>
<tr><td>Allocation of IP parameters</td><td>Configurable or automatic (DHCP client)</td></tr>
<tr><td>Software upgrade</td><td>FTP
TFTP</td></tr>
<tr><td>Configuration upload/download</td><td>FTP
TFTP</td></tr>
</table>

Mechanical

NOTE

The equipment may be shipped with either a PS1036 or a PS1073 IDU. The differences are primarily in the mechanical structure. The basic functionality is the same.

Table 1-6: Mechanical Specifications			
Unit	Structure	Dimensions (cm)	Weight (kg)
General	An IDU indoor unit and an ODU outdoor unit		
IDU PS1036	Plastic box (white), desktop or wall mountable	16 x 9 x 6	0.55
IDU PS1073	Plastic box (black), desktop or wall mountable	14 x 6.6 x 3.5	0.3
ODU with Integral Antenna	Metal box plus an integral antenna in a cut diamond shape in a plastic enclosure, poll or wall mountable	43.2 x 30.2 x 5.9	2.9
ODU with a Connection to a Detached Antenna	Metal box, pole or wall mountable	30.6 x 12.0 x 4.7	1.85
UNI-23-9	A pole mountable antenna include a mounting bracket supporting +/- 22.5° tilt and a 1.5m LMR 400 cable.	30.5 x 30.5 x 2.5	1.5
UNI-28-4	A pole mountable antenna include a mounting bracket supporting +/- 22.5° tilt and a 1.5m LMR 400 cable.	60 x 60 x 5.5	5

Connectors

<table>
<tr><td colspan="3">**Table 1-7: Connectors**</td></tr>
<tr><td>**Unit**</td><td>**Connector**</td><td>**Description**</td></tr>
<tr><td>IDU</td><td>ETHERNET</td><td>10/100BaseT Ethernet (RJ-45) with 2 embedded LEDs.

Cable connection to a PC: crossed

Cable connection to a hub: Straight</td></tr>
<tr><td></td><td>RADIO</td><td>10/100BaseT Ethernet (RJ-45): Ethernet + power for outdoor connection over a CAT-5 shielded cable</td></tr>
<tr><td></td><td>AC IN</td><td>3 pin AC power plug</td></tr>
<tr><td>ODU</td><td>INDOOR</td><td>10/100BaseT Ethernet (RJ-45), protected by a waterproof sealing assembly</td></tr>
<tr><td></td><td>ANT (D models)</td><td>N-Type jack, 50 ohm, lightning protected</td></tr>
</table>

Electrical

<table>
<tr><td colspan="2">**Table 1-8: Electrical Specifications**</td></tr>
<tr><td>**Unit**</td><td>**Details**</td></tr>
<tr><td>General</td><td>Power consumption: 25W</td></tr>
<tr><td>IDU</td><td>AC power input: 100-240 VAC, 50-60 Hz</td></tr>
<tr><td>ODU</td><td>54VDC from the IDU over the indoor-outdoor Cat-5 shielded Ethernet cable</td></tr>
</table>

Environmental

Table 1-9: Environmental Specifications		
Type	**Unit**	**Details**
Operating temperature	Outdoor units	-40 $^{\circ}$C to 55 $^{\circ}$C
	Indoor equipment	0 $^{\circ}$C to 40 $^{\circ}$C
Operating humidity	Outdoor units	5%-95% non condensing, Weather protected
	Indoor equipment	5%-95% non condensing

Standards Compliance, General

Table 1-10: Standards Compliance, General		
Type	**Standard**	
EMC	■ FCC Part 15 class B ■ ETSI EN 300 489-1	
Safety	■ UL 1950 ■ EN 60950	
Environmental	Operation	■ ETS 300 019 part 2-3 class 3.2E for indoor units ■ ETS 300 019 part 2-4 class 4.1E for outdoor units
	Storage	ETS 300 019-2-1 class 1.2E
	Transportation	ETS 300 019-2-2 class 2.3
Lightning protection	EN 61000-4-5, Class 3 (2kV)	
Radio	■ FCC Part 15 ■ ETSI EN 301 753 ■ ETSI EN 301 021 ■ ETSI EN 301 893 (2003-04)	

2

Chapter 2 - Installation

In this Chapter

Installation Requirements

This section describes all the supplies required to install the BreezeNET B system components and the items included in each installation package.

Packing List

■ IDU indoor unit with a wall mounting kit

■ Mains power cord

■ ODU outdoor unit with an integrated antenna (regular model)
Or
ODU outdoor unit with a connection to a detached antenna (not included)

■ Pole mounting kit for the ODU

■ Cat.5 indoor-to-outdoor Ethernet cable with shielded RJ-45 connectors

Additional Installation Requirements

The following items are also required to install the BreezeNET B system:

■ Detached Antenna* (for D model units), including a pole mounting kit and an RF cable.

■ Ethernet cable (straight for connecting to a hub/switch etc., crossed for connecting directly to a PC's NIC)

■ If the Inddor-to-Outdoor cable supplied with the equipment is not long enough - Category 5 Ethernet cable with shielded RJ-45 connectors * (available in different lengths. For more details refer to [Indoor-to-Outdoor Cables](#) on page 2-3).

■ Crimping tool for RJ-45 connectors.

■ Ground cables with an appropriate termination.

■ Mains plug adapter or termination plug (if the power plug on the supplied AC power cord does not fit local power outlets).

■ Portable PC with Ethernet card and BreezeCONFIG* application and a crossed Ethernet cable.

■ Installation tools and materials, including appropriate means (e.g. a pole) for installing the outdoor equipment.

NOTE

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

Indoor-to-Outdoor Cables

NOTE

The length of the Ethernet cable connecting the indoor unit to the user's equipment, together with the length of the Indoor-to-Outdoor cable, should not exceed 100 meters.

Use only Category 5E cables from approved manufacturers, listed in Table 2-1. Consult with Alvarion specialists on the suitability of other cables.

Table 2-1: Approved Category 5E Cables	
Manufacturer	**Part Number**
Superior Cables Ltd. www.cvalim.co.il	612098
HES Cabling Systems www.hescs.com	H5E-00481
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
Teldor www.teldor.com	8393204101

Equipment Location Guidelines

This section provides key guidelines for selecting the optimal installation locations for the various BreezeNET B system components.

> **NOTE**
>
> ONLY experienced installation professionals who are familiar with local building and safety codes and, wherever applicable, are licensed by the appropriate government regulatory authorities should install outdoor units and antennas.
>
> Failure to do so may void the BreezeNET B product warranty and may expose the end user or Service Provider to legal and financial liabilities. Alvarion and its resellers or distributors are not liable for injury, damage or regulation violations associated with the installation of Outdoor Units or antennas.

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

■ The outdoor unit can be either pole or wall mounted. Its location should enable easy access to the unit for installation and testing.

■ The higher the placement of the antenna, the better the achievable link quality.

■ ODU units with a detached antenna (D model) should be installed as close as possible to the antenna.

■ The ODU outdoor unit with its integrated antenna (or the detached antenna) should be installed to provide a direct, or near line of sight with the antenna of the other side.

■ The indoor equipment should be installed as close as possible to the location where the indoor-to-outdoor cable enters the building. The location of the indoor equipment should take into account its connection to a power outlet and the CPE.

Installing the Outdoor Unit

The following sections describe how to install the outdoor units, including pole mounting the ODU, and connecting the indoor-to-outdoor, grounding and RF cables.

NOTE
Ensure that outdoor units, antennas and supporting structures are properly installed to eliminate any physical hazard to either people or property. Make sure that the installation of the outdoor unit, antenna and cables is performed in accordance with all relevant national and local building and safety codes. Even where grounding is not mandatory according to applicable regulation and national codes, it is highly recommended to ensure that the outdoor unit and the antenna mast (when using external antenna) are grounded and suitable lightning protection devices are used so as to provide protection against voltage surges and static charges. In any event, Alvarion is not liable for any injury, damage or regulation violations associated with or caused by installation, grounding or lightning protection.

Pole Mounting the Outdoor Unit

The Outdoor Unit can be mounted on a pole using one of the following options:

■ Special brackets and open-ended bolts are supplied with each unit. There are two pairs of threaded holes on the back of the unit, enabling the special brackets to be mounted on diverse pole widths.

■ Special grooves on the sides of the unit enable the use of metal bands to secure the unit to a pole. The bands must be 9/16 inches wide and at least 12 inches long. The metal bands are not included with the installation package.

Figure 2-1 shows the locations of the holes and band grooves on the back, top and bottom of the Outdoor Unit.

NOTE
Be sure to install the unit with the bottom panel, which includes the LED indicators, facing downward.
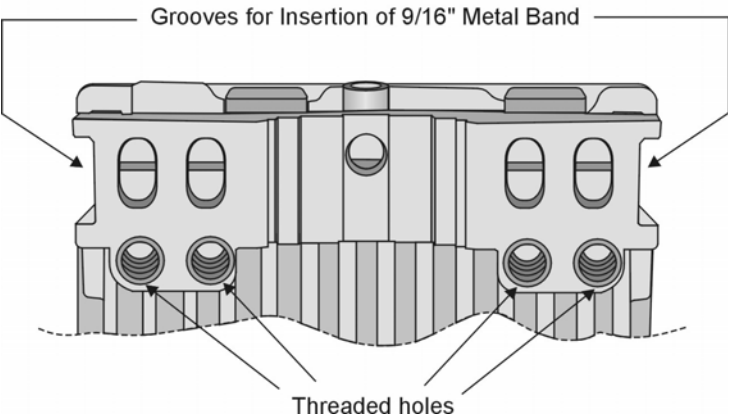
Figure 2-1: Threaded Holes/Grooves

Figure 2-2 illustrates the method of installing an outdoor unit on a pole, using the brackets and open-ended bolts.
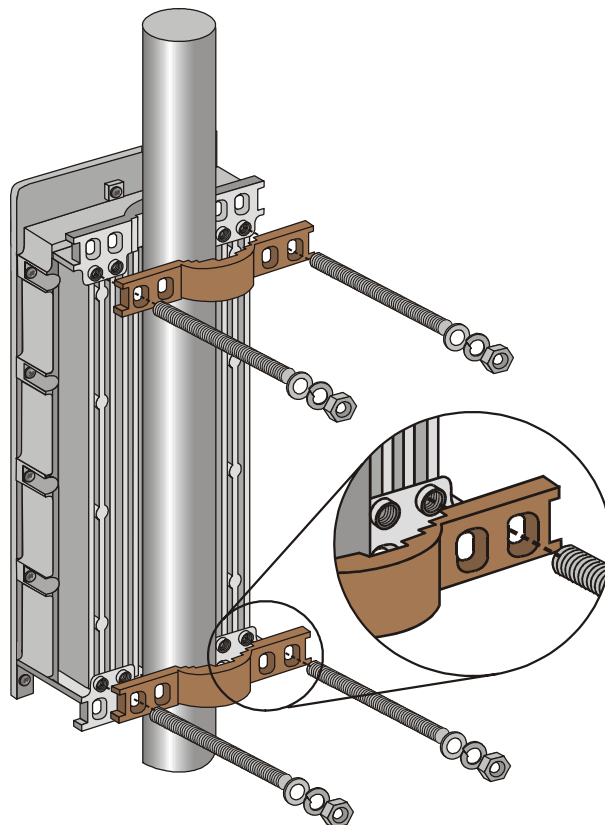
Figure 2-2: 3" Pole Installation Using Special Brackets

NOTE

Be sure to insert the open ended bolts with the grooves pointing outward, since these grooves enable you to use a screwdriver to fasten the bolts to the unit.

Connecting the Ground and Antenna Cables

The Ground terminal (marked ⏚) is located on the bottom panel of the outdoor unit. The Antenna RF connector (marked Ⓨ) is located on the top panel of the D-model ODU.

To prepare the ground cable:

1. Connect one end of a grounding cable to the ground terminal and tighten the ground screw firmly.

2. Connect the other end of the ground cable to a ground connection.

To connect the RF cable (D model):

1. Connect one end of the coaxial RF cable to the RF connector on the top panel of the unit

2. Connect the other end of the RF cable to the antenna.

3. The RF connectors should be sealed properly to protect against rain and moisture
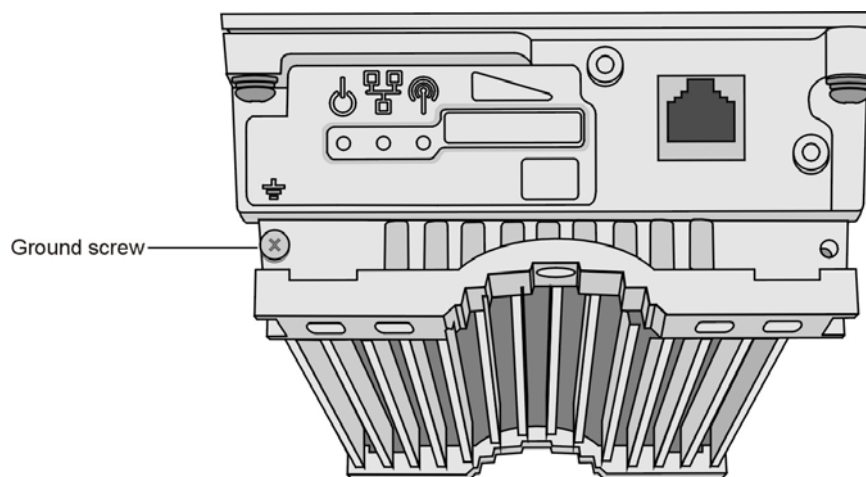
Figure 2-3: Bottom Panel of the Outdoor Unit (without the seal assembly)

> **NOTE**
>
> The MAC Address of the unit is marked on both the ODU and the IDU (on the bottom side of the unit). If due to any reason the ODU is not used with the IDU with whom it was shipped, the MAC Address of the system is in accordance with the marking on the ODU.

Connecting the Indoor-to-Outdoor Cable

Units with an installed waterproof seal

> **To connect the indoor-to-outdoor cable:**

1. Remove the two screws holding the waterproof seal to the outdoor unit and remove the waterproof seal.

2. Unscrew the top nut from the waterproof seal.
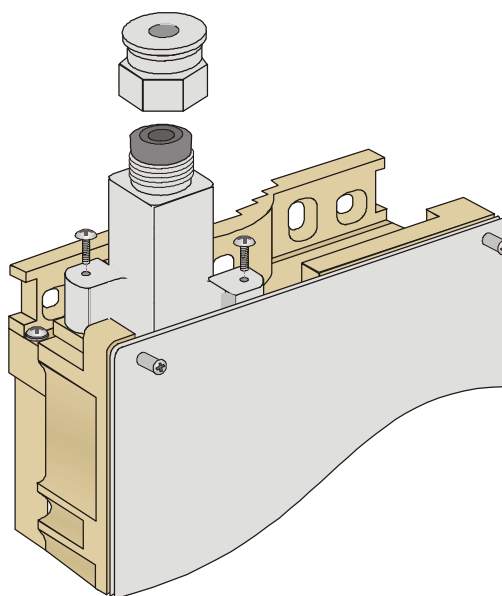
Figure 2-4: The Waterproof Seal

3. Route a straight Cat. 5 Ethernet cable (8-wire, 24 AWG) through both the top nut and the waterproof seal.

NOTE

Use only Category 5E 4x2x24# FTP outdoor cables from an approved manufacturer. See list of approved cables and length limitations in Indoor-to-Outdoor Cables on page 2-3.

4. Insert and crimp the RJ-45 connector. Refer to Appendix C for instructions on preparing the cable.

5. Connect the Ethernet cable to the outdoor unit RJ-45 connector.

---

6. Replace the waterproof seal and then the top nut. Make sure that the external jack of the cable is well inside the waterproof seal to guarantee a good seal.

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

8. Assemble an RJ-45 connector with a protective cover on the indoor end of the indoor-to-outdoor cable.

Units with a waterproof seal supplied with the Ethernet cable

To connect the indoor-to-outdoor cable:

1. Verify that the o-ring supplied with the cable kit is in place.

2. Connect the RJ-45 connector of the Ethernet cable to the outdoor unit.

3. Attach the waterproof seal to the unit. Tighten the top nut.

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

5. Assemble an RJ-45 connector with a protective cover on the indoor end of the indoor-to-outdoor cable.
    See Appendix C - Preparing the Indoor to Outdoor Cable for instructions on preparing the cable.

Installing the Universal IDU Indoor Unit

The unit can be placed on a desktop or a shelf. Alternatively, it may be wall-mounted. The drilling template included with the unit can be used to simplify the wall installation process.

The equipment is shipped with either a PS1036 (white box) or a PS1073 (black box) IDU. The type is marked on the bottom of the unit. The functionality is very similar, although there are some mechanical differences between the two types, as shown in the following figures:
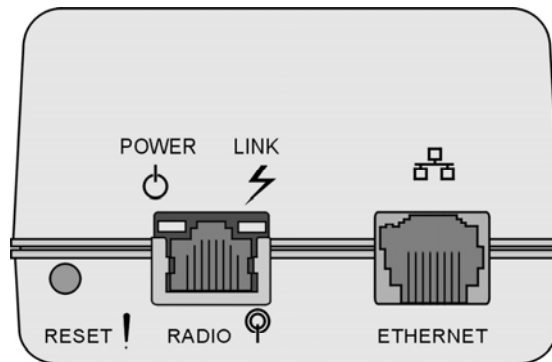
Figure 2-5: IDU PS 1036 Front Panel
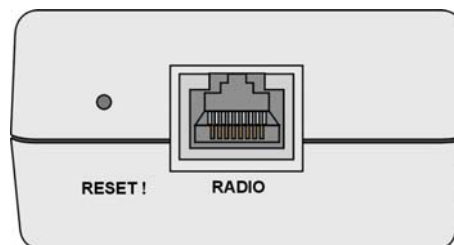
Figure 2-6: IDU PS 1073 Front Panel

In the PS1036 IDU, all connectors, indicators and RESET button are located on the front panel. In the smaller PS1073 (black colored) IDU, the RADIO connector and RESET button are located on the front panel, the ETHERNET connector is located on the side panel and LEDs are located on the top panel. There are also some differences in the names and functionality of the LEDs.

CAUTION
Do not connect the data equipment to the RADIO port. The RADIO port supplies DC power to the ODU, and this may harm other equipment connected to it.

To install the IDU:

1. Connect the Indoor-to-Outdoor cable to the RADIO connector, located on the front panel of the indoor unit.

2. Connect the power cord to the unit's AC socket, located on the rear panel. Connect the other end of the power cord to the AC mains. The unit can operate with AC mains of 100-240 VAC, 50-60 Hz.

> **NOTE**
>
> The color codes of the power cable are as follows:
>
> | | | |
> |---|---|---|
> | Brown | Phase | ~ |
> | Blue | Neutral | 0 |
> | Yellow/Green | Ground | ⏚ |

3. Verify that the POWER LED (located on the front panel of the PS1036 and on the top panel of the PS1073) is lit, indicating that power is supplied to the unit.

4. Configure the basic parameters as described in Configuring Basic Parameters on page 3-2.

5. Connect the 10/100 BaseT ETHERNET connector (located on the front panel of the PS1036 and or the side panel of the PS1073) to the network. The cable connection should be a straight Ethernet if connecting the indoor unit to a Hub/Switch and a crossed cable if connecting it directly to a PC Network Interface Card (NIC).

> **NOTE**
>
> The length of the Ethernet cable connecting the indoor unit to the user's equipment, together with the length of the Indoor-to-Outdoor cable, should not exceed 100 meters.

RESET button Functionality

Using a sharp object, press the recessed RESET push button for a short time to reset the unit and reboot from the Main version.

In units with ODU HW revision C and an IDU PS 1073, the RESET button can be used for setting the unit to its factory defaults. Press the button for at least 5 seconds (until the ETH LED of the IDU stops blinking): the unit will reboot with the factory default configuration.

> **NOTE**
>
> Reset the unit using the RESET push button on the IDU after connecting or reconnecting the indoor and outdoor units with the indoor-to-outdoor cable.

This page left intentionally blank.

3

Chapter 3 - Commissioning

About this Chapter

Configuring Basic Parameters

After completing the installation process, as described in the preceding chapter, the basic parameters must be configured to ensure that the unit operates correctly. Once the basic parameters have been configured, additional parameters can be remotely configured via the Ethernet port or the wireless link using the BreezeCONFIG utility, or by loading a configuration file.

Refer to Working with the Monitor Program on page 4-2 for information on how to access the Monitor program using Telnet. Refer to the BreezeCONFIG for BreezeNET B User's Guide for instructions on using the configuration utility.

The Basic Configuration menu in the Monitor program includes all the parameters necessary for the initial installation and operation of BreezeNET B units. In many installations, most of these parameters should not be changed from their default values. The basic parameters and their default values are listed in Table 3-1.

Refer to Menus and Parameters on page 4-5 for detailed information on the applicable parameters.

> **NOTE**
>
> For compliance with ETSI regulations, the bandwidth used in the default Sub Band for units in the 5.4 GHz band is 20 MHz. The use of a Sub Band with a 40 MHz bandwidth (Turbo Mode) in the 5.4 GHz band is allowed only if approved by the applicable local regulatory administration.

Table 3-1: Basic Parameters		
Parameter	**Default Value**	**Comment**
Ethernet Port Negotiation Mode (in Unit Control Parameters)	Auto Negotiation	
IP Address	10.0.0.1	
Subnet Mask	255.0.0.0	
Default Gateway Address	0.0.0.0	
DHCP Options	Disable	
Access to DHCP	BU: From Ethernet Only RB: From Wireless Only	

Table 3-1: Basic Parameters		
Parameter	**Default Value**	**Comment**
ESSID	ESSID1	
Sub Band Select	1	Applicable only if more than one Sub Band is available
Frequency (BU)	The lowest frequency in the selected Sub Band	
Frequency Subset Definition (RB)	A (All)	The list of frequencies is in accordance with the Sub Band.
Tx Power for Modulation Levels 1 to 5	Depend on unit type and Sub Band	Tx Power cannot be higher than the applicable Maximum Tx Power parameter
Tx Power for Modulation Level 6		
Tx Power for Modulation Level 7		
Tx Power for Modulation Level 8		
Maximum Tx Power for Modulation Levels 1 to 5 (RB)	Depend on Sub Band	Max Tx Power cannot be higher than the upper limit according to the Sub Band in use.
Maximum Tx Power for Modulation Level 6 (RB)		
Maximum Tx Power for Modulation Level 7 (RB)		
Maximum Tx Power for Modulation Level 8 (RB)		
Tx Control (BU)	On	
Antenna Gain	Depends on unit type and Sub Band	If set to "Not Set Yet", must be configured according to actual value, taking into account cable's attenuation.
ATPC Option	Enable	
Best BU Support (RB)	Disable	

Table 3-1: Basic Parameters		
Parameter	Default Value	Comment
Preferred BU MAC Address (RB)	00-00-00-00-00-00 (none)	Applicable only when Best BU Support is enabled
Link Distance Mode (BU)	Automatic	
Maximum Link Distance (BU)	0 (No Compensation)	
Maximum Modulation Level	8 (or the highest value supported according to the country code).	Refer to Configuring the Maximum Modulation Level on page 3-7
VLAN ID-Management	65535	
Authentication Algorithm	Open System	Availability of security parameters depends on support according to the Country Code.
Data Encryption Option	Disable	
Security Mode	WEP	
Promiscuous Authentication (BU)	Disable	
Default Key (RB)	Key 1	
Key 1 to Key 4	00……0 (32 zeros, meaning no key)	

NOTE

Some parameters are changed to their new values only after reset (refer to Appendix E - Parameters Summary for more details). Once the basic parameters are configured, the unit should be reset in order to activate the new configuration.

Aligning the RB's Antennas

An SNR bar display is located on the bottom panel of the RB-ODU. The ten LEDs are used for indicating the quality of the received signal. The higher the number of green LEDs indicating On, the higher the quality of the received signal. This section describes how to align the antennas using the SNR bar display.

> **NOTE**
>
> Antenna alignment using the SNR bar display is possible only after the RB is associated with a BU. Both units must be operational and configured with the correct basic parameters. If not, the unit will not be able to synchronize with the BU. As the SNR measurement is performed on received frames, its results are meaningless unless the RB is associated with a BU.

To align the antenna:

1. Align the antenna (integrated into the front side of the ODU unit, or detached) by pointing it in the general direction of the BU.

2. Verify that the power indication of the units is **On**.

3. Verify that the WLNK orange LED of the RB-ODU is **On**, indicating that the unit is associated with the BU. If the WLNK LED is **Off**, check that the **ESSID** and **Frequency** parameters are correctly configured. If the RB is still not associated with the BU, increase the transmit power level to its maximum value. If the unit is still not associated with the BU, improve the quality of the link by changing the direction of the antennas or by placing the antenna at a higher or alternate location.

4. Rotate the antenna of the RB-ODU until the maximum SNR reading is achieved, where at least 1 green LED is on: If you encounter prolonged difficulty in illuminating the minimum required number of green LEDs, try to improve the reception quality by placing the antenna at a higher point or in an alternate location.

5. Ensure that the front of the antenna is always facing the location of the BU. However, in certain conditions, such as when the line of site to the BU is hampered, better reception may be achieved using a reflected signal. In this case, the antenna is not always directed toward the BU.

6. Secure the unit firmly to the pole.

> **NOTE**
>
> In some cases, the antenna may need to be tilted to ensure that the level at which the RB receives transmissions from the BU (and vice versa) is not too high. As a rule of thumb, if the RB is located at a distance of less than 300 meters from the BU, it is recommended to up-tilt the antennas by approximately 10° to 15°. To guarantee a safety margin from the saturation level (received signal of -40dBm at the antenna port), the SNR should not be higher than 50dB. The orange LED of the SNR bar indicates that the SNR is higher than 50dB.

Configuring the Maximum Modulation Level

This section describes how to configure the maximum modulation level for BreezeNET B units.

> **NOTE**
>
> If the RB is associated with the BU, then the final configuration of the Maximum Modulation Level parameter may be performed remotely, for example, from the site of the BU or from another site.

To configure the Maximum Modulation Level:

1. If the SNR of the RB at the BU is too low, and vice versa, it is recommended that you configure the *Maximum Modulation Level parameter* to a value that is lower than the maximum supported by the unit. This can decrease the number of retransmissions due to attempts to transmit at modulation levels that are too high for the actual quality of the link.

2. Check the SNR of the RB at the BU. You can use Telnet to view the SNR values in *the MAC Address Database* of the BU, which can be accessed from the *Site Survey* menu. If the ATPC algorithm is not enabled in both units, the test should be done with the *Tx Power Level* parameters configured to their maximum values (subject to local regulatory limitations). If the SNR is lower than the values required for the maximum modulation level according to Table 3-2, it is recommended that you decrease the value of the Maximum Modulation Level.

> **NOTE**
>
> The SNR measurement at the BU is accurate only when receiving transmissions from the RB. If necessary, ping the BU to verify data transmission from the RB.

3. Configure the *Maximum Modulation Level* according to Table 3-2, using the typical SNR values. It is recommended that a 2 dB margin be added to compensate for possible measurement inaccuracy or variance in the quality of the link.

4. Repeat steps 2 - 3 for the BU, checking the SNR at which it is received at the RB using the *Continuous Link Quality Display* option in the *Site Survey* menu. There is no need to ping the RB, since the SNR measurement at the RB is based on beacons which are continuously transmitted by the BU.

Table 3-2: Recommended Maximum Modulation Level	
SNR	**Maximum Modulation Level**
SNR> 23 dB	8
21 dB < SNR < 23 dB	7
16 dB< SNR < 21 dB	6
13 dB < SNR < 16 dB	5
10 dB < SNR < 13 dB	4
8 dB < SNR < 10 dB	3
7 dB < SNR < 8 dB	2
6 dB<SNR < 7 dB	1

Operation Verification

The following sections describe how to verify the correct functioning of the Outdoor Unit, Indoor Unit, Ethernet connection and data connectivity.

Outdoor Unit Verification

To verify the correct operation of the Outdoor Unit, examine the LED indicators located on the bottom panel of the outdoor unit.

The following tables list the provided LEDs and their associated indications.

NOTE

Verifying the correct operation of the Outdoor Unit using the LEDs, as described below, is only possible after the configuration and alignment processes are completed.

Table 3-3: BU-ODU LEDs			
Name		**Description**	**Functionality**
W-LINK	⏻	Wireless Link Indictor	■ Green – Unit is associated with an RB ■ Blinking red – Unit is not associated ■ Off – Wireless link disabled
Status	⏽	Self-test and power indication	■ Green – Power is available and self-test passed. ■ Blinking Amber – Testing (not ready for operation) ■ Red – Self-test failed – fatal error
ETH	⊟	Ethernet activity/ connectivity indication	■ Green –Ethernet link detected. ■ Amber – No Ethernet connectivity between the indoor and outdoor units.

Table 3-4: RB-ODU LEDs		
Name	**Description**	**Functionality**
W-LINK ⏻	Wireless Link Indictor	■ Green – Unit is associated with a BU, no wireless link activity ■ Blinking Green – Data received or transmitted on the wireless link. Blinking rate is proportional to wireless traffic rate ■ Off – Wireless link disabled
Status ⏻	Self-test and power indication	■ Green – Power is available and self-test passed. ■ Blinking Amber – Testing (not ready for operation) ■ Red – Self-test failed – fatal error
ETH 🖧	Ethernet activity/ connectivity indication	■ Green – Ethernet link between the indoor and outdoor units is detected, no activity ■ Blinking Green –Ethernet connectivity is OK, with traffic on the port. Blinking rate proportional to traffic rate. ■ Red – No Ethernet connectivity between the indoor and outdoor units.
SNR BAR	Received signal strength Indication	■ Red LED: Signal is too low (SNR<4dB) ■ 8 green LEDs: Quality of the received signal ■ Orange LED: Signal is too high (SNR>50dB)

Table 3-5: RB-ODU SNR Bar LED Functionality	
SNR Bar LEDs	**SNR (typical)**
LED 1 (red) is On	Signal is too low (SNR < 4dB)
LED 2 (green) is On	SNR > 4 dB
LEDs 2 to 3 (green) are On	SNR > 8 dB
LEDs 2 to 4 (green) are On	SNR > 13 dB
LEDs 2 to 5 (green) are On	SNR > 19 dB
LEDs 2 to 6 (green) are On	SNR > 26 dB
LEDs 2 to 7 (green) are On	SNR > 31 dB
LEDs 2 to 8 (green) are On	SNR > 38 dB
LEDs 2 to 9 (green) are On	SNR > 44 dB
LEDs 2 to 9 (green) and 10 (orange) are On	Signal is too high (SNR > 50 dB)

Indoor Unit Verification

To verify the correct operation of the indoor equipment, examine the LED indicators located on the top panel of the IDU units.

The following tables list the LEDs of the PS1036 and the PS1073 IDUs and their associated indications.

Table 3-6: PS1036 IDU LEDs		
Name	**Description**	**Functionality**
POWER	Power Indication	■ Orange - 48VDC is present on the RADIO port. ■ Off - No power is supplied to the RADIO port.
LINK	Self test and end-to-end Ethernet connectivity	■ Off – No Ethernet connectivity has been detected between the outdoor unit and the device connected to the indoor unit. ■ Green– Self-test passed and Ethernet connection confirmed by the outdoor unit (Ethernet integrity check passed).

Table 3-7: PS1073 IDU LEDs		
Name	**Description**	**Functionality**
POWER	Power Indication	■ Green – IDU power is OK ■ Off - No power or power failure
ETH	Self test and end-to-end Ethernet connectivity	■ Off – No Ethernet connectivity has been detected between the outdoor unit and the device connected to the indoor unit. ■ Green– Self-test passed and Ethernet connection confirmed by the outdoor unit (Ethernet integrity check passed).

Verifying Data Connectivity

To verify data connectivity, from the end-user's PC or from a portable PC connected to the unit, ping the other unit or a station behind it.

4

Chapter 4 - Operation and Administration

In this Chapter

- [Working with the Monitor Program](), page 4-2
- [Menus and Parameters](), page 4-5

Working with the Monitor Program

Accessing the Monitor Program Using Telnet

1. Connect a PC to the Ethernet port, using a crossed cable.

2. Configure the PC's IP parameters to enable connectivity with the unit. The default IP address is 10.0.0.1.

3. Run the Telnet program. The *Select Access Level* menu is displayed.

4. Select the required access level, depending on your specific access rights. A password entry request is displayed. Table 4-1 lists the default passwords for each of the access levels.

Table 4-1: Default Passwords	
Access Rights	**Password**
Read-Only	public
Installer	user
Administrator	private

> **NOTE**
>
> Following three unsuccessful login attempts (using incorrect passwords), the monitor program is blocked for several minutes. To enable access to the monitor program during that time, the unit must be reset via SNMP or by disconnecting/reconnecting power.

5. Enter your password and press **Enter**. The *Main Menu* is displayed as shown in Figure 4-1: . The unit type, SW version number and SW release date displayed in the **Main Menu** vary according to the selected unit and SW version.

```
BreezeNET B/BU

Official Release Version – 1.1.3

Release Date: Mon Jul 01 2003, 17:10:21

Main Menu

==========

1 – Info Screens

2 – Unit Control

3 – Basic Configuration

4 – Site Survey

5 – Advanced Configuration

x – Exit

>>>
```

Figure 4-1: Main Menu (Administrator Level)

NOTE

If the Telnet session is not terminated properly; for example, if you simply close the window, the monitor program is blocked for several minutes. To enable access to the monitor program during that time, the unit must be reset via SNMP or by disconnecting/reconnecting power.

The appearance of the *Main Menu* varies depending on the user's access level, as follows.

■ For users with read only access rights, only the *Info Screens* option is displayed. Users with this access level are not able to access the *Unit Control, Basic Configuration, Site Survey* and *Advanced Configuration* menus.

■ For users with Installer access rights, the first four menu items, *Info Screens, Unit Control, Basic Configuration* and *Site Survey*, are displayed. Users with this access level are not able to access the *Advanced Configuration* menu.

■ For users with Administrator access rights, the full *Main Menu* is displayed. These users can access all the menu items.

Common Operations

The following describes the standard operations that are used when working with the Monitor program.

- Type an option number to open or activate the option. In certain cases you may need to click **Enter**.

- Click Esc to exit a menu or option.

In some cases, to activate any configuration changes, you must reset the unit. Certain settings are automatically activated without the need to reset the unit. Refer to Appendix E - Parameters Summary for information on which parameters are run time configurable, which means that the unit need not be reset for the parameter to take effect, and which parameters do require that the unit be reset.

Menus and Parameters

The following sections describe the menus and parameters provided by the Monitor program.

Main Menu

The *Main Menu* enables you to access the following menus, depending on your access level, as described in <u>Working with the Monitor Program</u>, on page 4-2.

■ **Info Screens:** Provides a read only display of status information and current parameter values. Available at all access levels.

■ **Unit Control:** Enables you to access general operations, such as resetting the unit, reverting to factory default parameters, changing passwords and switching between software versions. Available at the Installer and Administrator access levels.

■ **Basic Configuration:** Enables you to access the set of parameters that are configured during the installation process. These parameters are also available in the *Advanced Configuration* menu. Available at the Installer and Administrator access levels.

■ **Site Survey:** Enables you to activate certain tests and view various system counters. Available at the Installer and Administrator access levels.

■ **Advanced Configuration:** Enables you to access all system parameters, including the parameters that are also available in the *Basic Configuration* menu. Available only at the Administrator access level.

Info Screens Menu

The Info Screens menu enables you to view the current values of various parameter sets. The parameter sets are identical to the main parameter groups in the configuration menus. You can view a specific parameter set or choose to view all parameters at once. While this menu is available at all access levels, some security related parameters including the encryption Keys, ESSID and Operator ESSID are only displayed to users with Administrator access rights.

The Info Screens menu includes the following options:

■ Show Unit Status

■ Show Basic Configuration

■ Show Advanced Configuration

■ Show Country Dependent Parameters

■ Show All Parameters

Show Unit Status

The Show Unit Status menu is a read only menu that displays the current values of the following parameters:

■ **Unit Name:** As defined in Unit Control menu.

■ **Unit Type:** Identifies the unit's function: BU-28, BU-14, RB-28 or RB-14.

■ **Unit MAC Address:** The unit's unique IEEE MAC address.

■ **Unit Status** (RB only)**:** The current status of the RB. There are two status options:

  ➢ **SCANNING:** The RB is searching for a BU with which to associate. If the DFS Option is enabled and the RB is currently looking for its previous BU, the BU's MAC Address will be displayed.

  ➢ **ASSOCIATED:** The RB is associated with a BU.

■ **BU MAC Address** (RB only)**:** The MAC address of the BU with which the unit is currently associated. If the unit is not associated with any BU, the address defaults to the IEEE broadcast address, which is FF-FF-FF-FF-FF-FF.

■ **Number of Associations Since Last Reset:** Displays the total number of associations since the last reset, including duplicate associations.

■ **Unit Hardware Version:** The version of the outdoor unit hardware.

■ **Unit BOOT Version:** The version of the BOOT SW

■ **Time Since Last Reset**

- **Flash Versions**:

    - ➢ **Running from:** Shows whether the unit is running from the Main or from the Shadow Version.

    - ➢ **Main Version File Name:** The name of the compressed file (with a ".bz" extension) of the version currently defined as the main version.

    - ➢ **Main Version Number:** The software version currently defined as the main version.

    - ➢ **Shadow Version File Name:** The name of the compressed file (with a ".bz" extension) of the version currently defined as the shadow (backup) version.

    - ➢ **Shadow Version Number:** The software version currently defined as the shadow (backup) version.

- **Radio Band:** The radio band of the unit

- **Log Out Timer:** The value of the Log Out Timer as defined in Unit Control menu.

- **Ethernet Port Negotiation Mode**: The Ethernet port negotiation mode as defined in Unit Control menu.

- **Ethernet Port State:** The actual state of the Ethernet port.

- **FTP Parameters:** General FTP parameters (common to SW Version Download, Configuration File Upload/Download and Event File Upload using FTP):

    - ➢ FTP Client IP Address

    - ➢ FTP Client IP Mask

    - ➢ FTP Server IP Address

    - ➢ FTP Gateway IP Address

    - ➢ FTP User Name

    - ➢ FTP Password

- **FTP Software Download Parameters:** The parameters for SW download using FTP, as defined in Unit Control menu.

    - ➢ FTP Source Directory

    - ➢ FTP SW Version File Name

■ **Configuration File Download/Upload Parameters:** The parameters for Configuration file upload/download using FTP, as defined in Unit Control menu.

> Configuration File Name

> Configuration File Source Directory

> Operator Defaults File Name

■ **FTP Log File Upload Parameters:** The parameters for Event Log file upload using FTP, as defined in Unit Control menu.

> FTP Log File Name

> FTP Log File Destination Directory

■ **Event Log Policy**

Show Basic Configuration

The Show Basic Configuration menu is a read only menu that displays the current values of the parameters included in the Basic Configuration menu.

Show Advanced Configuration

The Show Advanced Configuration menu enables you to access the read only sub menus that display the current values of the parameters included in the applicable sub menus of the Advanced Configuration menu.

Show Country Dependent Parameters

Each country has its radio regulation regarding transmissions in the applicable bands that affect parameters such as available frequencies, bandwidth, transmit power, etc. Some other parameters and options may also vary among countries. For each country, one or more sets of parameters are pre-configured in the factory. If more than one set is available, the set to be used can be selected. The Show Country Dependent Parameters displays the available set(s) of these parameters, and includes the following:

- **Country Code:** The up to 3 digits country code according to ISO 3166 and the country name. Some regulatory requirements apply to more than one country. In these cases the Country Code includes a 4 digits proprietary group code and the Country Group name (for example FCC).

- **Data Encryption Support**: Indicates whether data encryption is supported for the applicable country.

- **AES Encryption Support**: Indicates whether encryption using AES is supported for the applicable country.

- **Authentication Encryption Support**: Indicates whether authentication encryption is supported for the applicable country.

For each of the available sets (Sub Bands), the following information is provided:

- **Sub Band ID and Frequencies**

- **Allowed Bandwidth:** If more than one bandwidth is allowed, than each bandwidth is associated with a different sub-band, since the bandwidth may affect the available frequencies. Currently, a bandwidth of 20 MHz is supported by all Sub Bands. Where allowed, a bandwidth of 40 MHz (Turbo Mode) is also supported.

- **Regulation Max Tx Power at Antenna Port:** The maximum transmit power allowed at the antenna port of the unit.

- **Regulation Max EIRP:** The maximum allowed EIRP (Effective Isotropic Radiated Power) in dBm, or No Limit.

- **Min Modulation Level:** The lowest allowed modulation level

- **Max Modulation Level:** The highest allowed modulation level

- **Burst Mode**: Indicates whether Burst Mode operation is allowed.

- **Maximum Burst Duration**: If Burst Mode is supported, this parameter displays the upper limit for the Maximum Burst Duration parameters.

- **DFS Option**: Indicates whether the DFS (Dynamic Frequency Selection) mechanism for identification and avoidance of channels with radar activity is supported.

- **Minimum HW Revision Support**: The minimum HW revision required to support the Sub Band.

New Country Code files can be uploaded remotely using TFTP (see Appendix B - File Download and Upload Using TFTP).

Show All Parameters

The Show All Parameters menu is a read only menu that displays the current values of all status and configuration parameters.

NOTE

The values of some security related parameters, including the encryption Keys, ESSID and Operator ESSID, are available only with Administrator access rights.

Unit Control Menu

The Unit Control menu enables configuring control parameters for the unit.

The Unit Control menu includes the following options:

■ Reset Unit

■ Default Settings

■ Change Unit Name

■ Change Password

■ Flash Memory Control

■ SW Version Download

■ Configuration File Upload/Download

■ Log Out Timer

■ Ethernet Port Negotiation Mode

■ Change System Location

■ Event Log Menu

■ Feature Upgrade

Reset Unit

The Reset Unit option enables resetting the unit. After reset, any modifications made to the system parameters are applied.

Default Settings

The Set defaults submenu enables resetting the system parameters to a predefined set of default or saving the current configuration as the set of Operator Defaults.

The Default Setting options are available only to users with Administrator access rights.

The available options are:

■ Set Defaults

■ Save Current Configuration As Operator Defaults

Set Defaults:

The Set Defaults submenu enables reverting the system parameters to a predefined set of defaults. There are two sets of default configurations:

A. Factory Defaults: This is the standard default configuration.

B. Operator Defaults: Operator Defaults configuration can be defined by the Administrator using the Save Current Configuration As Operator Defaults option in this menu. It may also be defined at the factory according to specific operator's definition. The default Operator Defaults configuration is the Factory Defaults configuration.

The current configuration file and the Operator Defaults configuration file can be uploaded/downloaded by the unit using FTP. For more information, see Configuration File Upload/Download option on page 4-19. These files can also be uploaded/downloaded remotely using TFTP (see Appendix B - File Download and Upload Using TFTP).

The available options in the Set Defaults submenu are:

■ Set Complete Factory Defaults

■ Set Partial Factory defaults

■ Set Complete Operator Defaults

■ Set Partial Operator defaults

■ Cancel Current Pending Request

Set Complete Factory Defaults

Select this option to reset the unit to the standard Factory Defaults configuration, excluding several parameters that are listed in Table 4-2.

Table 4-2: Parameters not reset after Set Complete Factory/Operator Defaults	
Parameters Group	**Parameter**
Unit Control Parameters	All Passwords
	FTP Server IP address* (see note below)
	FTP Gateway IP address* (see note below)
	FTP Client IP address* (see note below)
	FTP Client IP Mask* (see note below)
	FTP User Name* (see note below)
	FTP Password* (see note below)
	Ethernet Port Negotiation Mode
Air Interface Parameters	Selected Sub Band
	Frequency (BU)
	DFS Option (BU)
	Frequency Subset (BU)
	Antenna Gain (BU)

NOTE

The FTP parameters are not set to their default values after Set Complete Operator Defaults. However, they are set to their default value after Set Complete Factory Defaults. Note that in this case they are set to the default values immediately upon selecting the Set Complete Factory Default option (even before the next reset).

Set Partial Factory defaults

Select this option to reset the unit to the standard Factory Default configuration, excluding the parameters that are required to maintain connectivity and management access. The parameters that do not change after Set Partial Factory Defaults are listed in Table 4-3.

Table 4-3: Parameters that are not reset after Set Partial Factory/Operator Defaults	
Parameters Group	**Parameter**
Unit Control parameters	Passwords
	Ethernet Port Negotiation Mode
	FTP Server IP address
	FTP Gateway IP address
	FTP Client IP address
	FTP Client IP Mask
	FTP User Name
	FTP Password
IP Parameters	IP Address
	Subnet Mask
	Default Gateway Address
	DHCP Option
	Access to DHCP
Security Parameters	Authentication Algorithm
	Default Key (RB)
	Data Encryption Mode
	Default Multicast Key (BU)
	Security Mode
	Key # 1 to Key # 4
Air Interface Parameters	ESSID
	Operator ESSID Option (BU)
	Operator ESSID (BU)
	Link Distance Mode (BU)
	Maximum Link Distance (BU)
	Selected Sub Band

Table 4-3: Parameters that are not reset after Set Partial Factory/Operator Defaults	
Parameters Group	**Parameter**
	Frequency (BU)
	DFS Option (BU)
	Frequency Subset
	RB Waiting Option (BU)
	Channel Reuse Option (BU)
	Radar Activity Assessment Period (BU)
	Maximum Number of Detections in Assessment Period (BU)
	ATPC Option (BU)
	Transmit Power
	Tx Control (BU)
	Best BU Support (BU)
	Preferred BU MAC Address (RBU)
Performance Parameters	Adaptive Modulation Decision Thresholds
Bridge Parameters	VLAN ID – Management

Set Complete Operators Defaults

Select this option to reset the unit to the Operator Defaults configuration, excluding several parameters that are listed in Table 4-2.

Set Partial Operator defaults

Select this option to reset the unit to the Operator Defaults configuration, excluding the parameters that are required to maintain connectivity and management access. The parameters that do not change after Set Partial Operator Defaults are listed in Table 4-3.

Cancel Current Pending Request

Once you selected one of the Set defaults options, it will be executed after the next reset. This option enables you to regret and cancel the pending request before execution (provided the unit has not been reset yet).

Save Current Configuration As Operator Defaults

The Save Current Configuration As Operator Defaults option is available only under Administrator access rights. It enables defining the current configuration of the unit as the Operator Defaults configuration.

Change Unit Name

The Change Unit Name option enables changing the name of the unit, which is also the system's name in the MIB2. The name of the unit is also used as the prompt at the bottom of each Monitor window.

Valid values: A string of up to 32 printable ASCII characters.

The default unit name is an empty string.

Change Password

The Change Password submenu enables changing the access password(s). A user with Installer access rights can view and change the passwords for Read Only and Installer levels. A user with Administrator access rights can view and change the passwords for all levels.

Valid values: A string of up to 8 printable ASCII characters.

Refer to <u>Working with the Monitor Program</u>, on page 4-2 for a list of the default passwords for each of the access levels.

Flash Memory Control

The Flash Memory Control submenu enables selecting the active software version for the unit.

The flash memory can store two software versions. One version is called Main and the other is called Shadow. New software versions are loaded as the shadow version. You can select the shadow version as the new active version by selecting **Reset and Boot from Shadow Version**. However, after the next reset, the main version is re-activated. To continue using the currently active version after the next reset, select **Use Running Version After Reset**: The previous shadow version will be the new main version, and vice versa.

The parameters configured in the unit are not changed as a result of loading new software versions unless the new version includes additional parameters or additional changes in the list of parameters. New parameters are loaded with their default values.

Select from the following options:

■ **Reset and Boot from Shadow Version:** Activates the shadow (backup) software version. The unit is reset automatically. Following the next reset the unit will switch to the main version.

■ **Use Running Version After Reset:** Defines the current running version as the new main version. This version will also be used following the next reset.

SW Version Download

The SW Version Download submenu enables the optional downloading of a SW Version file from a remote FTP server. The SW Version Download submenu includes the following options:

■ **Execute FTP GET SW Version:** The Execute FTP GET SW Version option executes the SW Version FTP download according to the parameters defined below.

■ **FTP SW Source Dir:** The FTP SW Source Dir option enables defining the source directory of the SW version file.

Valid values: A string of up to 80 printable ASCII characters. To clear the field press "."

The default is an empty string.

■ **FTP SW Version File Name:** The FTP SW Version File Name option enables defining the name of the SW version file in the FTP server.

Valid values: A string of up to 20 printable ASCII characters. An empty string is not allowed.

The default is VxWorks.bz.

■ **FTP Client IP Address:** The FTP Client IP Address option enables defining the IP address of the FTP client in the unit. This secondary IP address is required only to support the optional FTP process.

The default is: 1.1.1.3

■ **FTP Client IP Mask**: The FTP Client IP Mask option enables defining the IP Mask for the FTP client mask in the unit.

The default is: 255.255.255.0

■ **FTP Server IP Address:** The FTP Server IP Address option enables defining the IP address of the FTP server that is hosting the SW Version file.

The default is: 1.1.1.4

■ **FTP Gateway IP Address**: The FTP Gateway IP Address option enables defining the FTP default gateway address.

The default is: 0.0.0.0.

■ **FTP User Name:** The FTP User Name option enables defining the user name to be used for accessing the FTP server that is hosting the SW Version file.

Valid values: A string of up to 18 printable ASCII characters.

The default is: vx

■ **FTP Password:** The FTP Password option enables defining the password to be used for accessing the FTP server that is hosting the SW Version file.

Valid values: A string of up to 18 printable ASCII characters.

The default is: vx

■ **Show SW Version Download Parameters and Status:** Displays the current values of the SW Version Download parameters, the current SW version and the SW versions stored in the Flash memory.

NOTE

There is one set of general FTP parameters (FTP Server IP Address, FTP Gateway IP Address, FTP Client IP Address, FTP Client IP Mask, FTP User Name and FTP Password). This set (or relevant parts of the set) serves the SW Download Procedure, the Configuration File Upload/Download procedure and the Event Log File Upload procedure. Changing any of these parameters in the menu for either procedure will automatically change its value in the menu for the other procedures.

Configuration File Upload/Download

The Configuration File Upload/Download submenu enables the optional uploading or downloading of a configuration or an Operator Defaults file from a remote FTP server. The Configuration File Upload/Download submenu includes the following options:

■ **Execute FTP GET/PUT Configuration File:** The Execute FTP GET/PUT Configuration File executes the upload/download of a Configuration file or an Operator Defaults file according to the parameters defined below. The following options are available:

➢ Execute FTP Get Configuration File (cfg)

➢ Execute FTP Put Configuration File (cfg)

➢ Execute FTP Get Operator Defaults File (cmr)

➢ Execute FTP Put Operator Defaults File (cmr)

■ **FTP Configuration File Source Dir:** The FTP Configuration File Source Dir option enables defining the source directory of the configuration/Operator Defaults file.

Valid values: A string of up to 80 printable ASCII characters. To clear the field press ".".

The default is an empty string.

■ **Configuration File FTP File Name:** The Configuration File FTP File Name option enables defining the name of the configuration file to be uploaded/downloaded.

Valid values: A string of up to 20 printable ASCII characters. An empty string is not allowed.

The default is config.cfg.

■ **Operator Defaults FTP File Name:** The Operator Defaults File Name option enables defining the name of the Operator Defaults file to be uploaded/downloaded.

Valid values: A string of up to 20 printable ASCII characters. An empty string is not allowed.

The default is operator.cmr.

■ **FTP Client IP Address:** The FTP Client IP Address option enables defining the IP address of the FTP client in the unit. This secondary IP address is required only to support the optional FTP process.

The default is: 1.1.1.3

■ **FTP Client IP Mask**: The FTP Client IP Mask option enables defining the IP Mask for the FTP client mask in the unit.

The default is: 255.255.255.0

■ **FTP Server IP Address:** The FTP Host IP Address option enables defining the IP address of the FTP server that is hosting the file.

The default is: 1.1.1.4

■ **FTP Gateway IP Address**: The FTP Gateway IP Address option enables defining the FTP default gateway address.

The default is: 0.0.0.0.

■ **FTP User Name:** The FTP User Name option enables defining the user name to be used for accessing the FTP server that is hosting the file.

Valid values: A string of up to 18 printable ASCII characters.

The default is: vx

■ **FTP Password:** The FTP Password option enables defining the password to be used for accessing the FTP server that is hosting the file.

Valid values: A string of up to 18 printable ASCII characters.

The default is: vx

■ **Show Configuration File Upload/Download Parameters:** Displays the current values of the Configuration File Upload/Download parameters.

NOTE

There is one set of general FTP parameters (FTP Server IP Address, FTP Gateway IP Address, FTP Client IP Address, FTP Client IP Mask, FTP User Name and FTP Password). This set (or relevant parts of the set) serves the SW Download Procedure, the Configuration File Upload/Download procedure and the Event Log File Upload procedure. Changing any of these parameters in the menu for either procedure will automatically change its value in the menu for the other procedures.

Log Out Timer

The Log Out Timer parameter determines the amount of inactive time following which the unit automatically exits the Monitor program.

The time out duration can range from 1 to 999 minutes.

The default value is 5 minutes.

Ethernet Port Negotiation Mode

The Ethernet Port Negotiation Mode submenu displays the current Ethernet port state and enables defining the negotiation mode of the Ethernet port. The available options are:

■ Force 10 Mbps and Half-Duplex

■ Force 10 Mbps and Full-Duplex

■ Force 100 Mbps and Half-Duplex

■ Force 100 Mbps and Full-Duplex

■ Auto Negotiation (10/100 Mbps and Half/Full Duplex)

The default is Auto Negotiation (10/100 Mbps and Half/Full Duplex)

Change System Location

The Change System Location option enables changing the system location of the unit, which is also the sys location in MIB2. The System Location is also displayed as a part of the Monitor menu's header.

Valid values: A string of up to 35 printable ASCII characters.

The default system location is an empty string.

Event Log Menu

The Event Log Menu enables controlling the event log feature. The event log is an important debugging tool and a flash memory sector is dedicated for storing it. Events are classified according to their severity level: Message (lowest severity), Warning, Error or Fatal (highest severity).

The severity at which events are saved in the Event Log is configurable. Events from the configured severity and higher are saved and may be displayed upon request. Log history can be displayed up to the full number of current active events. In the log, an event is defined as active as long as it has not been erased (a maximum of 1000 events may be stored). The Event Log may be read using TFTP, with remote file name <SNMP Read Community>.log (the default SNMP Read Community is "public"). The Event Log may also be uploaded to a remote FTP server.

The Event Log Menu includes the following options:

- Event Log Policy

- Display Event Log

- Erase Event Log

- Event Load Upload

Event Log Policy

The Event Log Policy determines the minimal severity level. All events whose severity is equal to or higher than the defined severity are logged.

Valid values are: Message (MSG) Level, Warning (WRN) Level, Error (ERR) Level, Fatal (FTL) Level, Log None.

The default selection is Warning Level severity.

Display Event Log

The Display Event Log option enables viewing how many events are logged and selecting the number of events to be displayed (up to 1000). The display of each event includes the event time (elapsed time since last reset), the severity level and a message string. The events are displayed in descending order, with the most recent event displayed first.

Erase Event Log

The Erase Event Log option enables clearing the event log.

Event Log Upload

The Event Log Upload submenu enables the optional uploading of the event log file to a remote FTP server. The Event Log Upload submenu includes the following options:

- **FTP Event Log Upload Execute:** The FTP event Log Upload Execute executes the upload of the Event Log file according to the parameters defined below.

- **Event Log Destination Directory:** The Event Log Destination Directory enables defining the destination directory for the Event Log File.

    Valid values: A string of up to 80 printable ASCII characters. To clear the field press "."

    The default is an empty string.

■ **Event Log File Name:** The Event Log File Name option enables defining the name of the event log file to be uploaded.

Valid values: A string of up to 20 printable ASCII characters.

The default is logfile.log.

■ **FTP Server IP Address:** The FTP Host IP Address option enables defining the IP address of the FTP server that is hosting the file.

The default is: 1.1.1.4

■ **FTP Gateway IP Address**: The FTP Gateway IP Address option enables defining the FTP default gateway address.

The default is: 0.0.0.0.

■ **FTP User Name:** The FTP User Name option enables defining the user name to be used for accessing the FTP server that is hosting the file.

Valid values: A string of up to 18 printable ASCII characters.

The default is: vx

■ **FTP Password:** The FTP Password option enables defining the password to be used for accessing the FTP server that is hosting the file.

Valid values: A string of up to 18 printable ASCII characters.

The default is: vx

■ **Show FTP Event Log File Upload Parameters:** Displays the current values of the Event Log Upload parameters.

> NOTE
>
> There is one set of general FTP parameters (FTP Server IP Address, FTP Gateway IP Address, FTP Client IP Address, FTP Client IP Mask, FTP User Name and FTP Password). This set (or relevant parts of the set) serves the SW Download Procedure, the Configuration File Upload/Download procedure and the Event Log File Upload procedure. Changing any of these parameters in the menu for either procedure will automatically change its value in the menu for the other procedures.

Feature Upgrade

The Feature Upgrade option enables to enter a license string for upgrading the unit to support new features and/or options. Upon selecting the Manual Feature Upgrade option the user will be requested to enter the license string. Each license string is associated with a unique MAC Address and one feature/option. If the encrypted MAC Address in the license string does not match the unit's MAC Address, the string will be rejected. If there is a match, a message notifying of the new feature/option will be displayed. The unit must be reset for the change to take effect.

The license string should comprise 32 to 64 hexadecimal digits.

New Feature License files can be uploaded remotely using TFTP (see Appendix B - File Download and Upload Using TFTP).

Basic Configuration Menu

The Basic Configuration menu includes all parameters required for the initial installation and operation of the unit. Once the unit is properly installed and operational, additional parameters can be configured either locally or remotely using Telnet or SNMP management.

> **NOTE**
>
> All parameters in the Basic Configuration menu are also available in the relevant sub menus of the Advanced Configuration menu.

The Basic Configuration menu enables to access the following parameter sets:

IP Parameters

- IP Address

- Subnet Mask

- Default Gateway Address

- DHCP Client

  ➢ DHCP Option

  ➢ Access to DHCP

Refer to for a description of these parameters.

Air Interface Parameters

- ESSID

- Operator ESSID Parameters (BU)

  ➢ Operator ESSID Option

  ➢ Operator ESSID

- Frequency Definition

  ➢ Select Sub Band (if more than one Sub Band is available)

  ➢ Frequency (BU)

  ➢ Sub Band Definition

- Best BU Parameters (RB)

  ➢ Best BU Support

> ➢ Preferred BU MAC Address

■ ATPC

> ➢ ATPC Option

■ Transmit Power parameters

■ Maximum Transmit Power parameters (RB)

■ Tx Control (BU)

■ Antenna Gain

■ Link Distance Parameters

> ➢ Link Distance Option (BU)

> ➢ Maximum Link Distance (BU)

Refer to Air Interface Parameters, on page 4-43, for a description of these parameters.

Performance Parameters

■ Maximum Modulation Level

Refer to Performance Parameters on page 4-76, for a description of these parameters.

Bridge Parameters

■ VLAN ID – Management

Refer to VLAN Support, on page 4-65, for a description of these parameters.

Security Parameters

■ Authentication Algorithm

■ Data Encryption Option

■ Security Mode

■ Default Key (RB)

■ Default Multicast Key (BU)

■ Key 1 to Key 4

■ Promiscuous Authentication (BU)

Some or all of the security parameters may not be available in units that do not support the applicable features. Refer to Security Parameters, on page 4-86, for a description of these parameters.

Site Survey Menu

The Site Survey menu displays the results of various tests and counters for verifying the quality of the wireless link. These tests can be used to help determine where to position the units for optimal coverage, antenna alignment and troubleshooting. The counters can serve for evaluating performance and identify potential problems. In the BU, there is also an extensive database for the RB served by it.

■ The Site Survey menu includes the following options:

■ Traffic Statistics

■ Ping Test

■ Continuous Link Quality display (RB only)

■ MAC Address Database

■ Per Modulation Level Counters

■ Link Capability

Traffic Statistics

The traffic statistics are used to monitor, interpret and analyze the performance of the wired and wireless links. The counters display statistics relating to wireless link and Ethernet frames. The Traffic Statistics menu includes the following options:

■ **Display Counters:** Select this option to display the current value of the Ethernet and wireless link (WLAN) counters.

■ **Reset Counters:** Select this option to reset the counters.

Ethernet Counters

The unit receives Ethernet frames from its Ethernet port and forwards the frames to its internal bridge, which determines whether each frame should be transmitted to the wireless media. Frames discarded by the unit's hardware filter are not counted by the Ethernet counters. The maximum length of a regular IEEE 802.1 Ethernet frame that can be accepted from the Ethernet port is 1518 bytes. For tagged 802.1Q frames the maximum size is 1522 bytes.

The unit transmits valid data frames received from the wireless media to the Ethernet port, as well as internally generated frames, such as responses to management queries and pings received via the Ethernet port. The Ethernet Counters include the following statistics:

■ **Total received frames via Ethernet:** The total number of frames received from the Ethernet port. This counter includes both invalid frames (with errors) and valid frames (without errors).

■ **Transmitted wireless to Ethernet:** The number of frames transmitted by the unit to the Ethernet port. These are generally frames received from the wireless side, but also include frames generated by the unit itself.

WLAN Counters

The unit submits data frames received from the Ethernet port to the internal bridge, as well as self generated control and wireless management frames. After a data frame is transmitted, the unit waits for an acknowledgement (ACK) message from the receiving unit. Some control and wireless management frames are not acknowledged. If an ACK is not received after a predefined time, the unit retransmits the frame until an ACK is received. If an ACK is not received before the number of retransmissions has reached a maximum predefined number, which is determined by the **Number of HW Retries** and **Number of SW Retries** parameters, the frame is dropped.

The Wireless Link Counters include the following statistics:

■ **Total transmitted frames to wireless:** The number of frames transmitted to the wireless media. The total includes one count for each successfully transmitted frame (excluding retransmissions), and the number of transmitted control and wireless management frames. In the BU, there are also separate counters for the following:

> ➢ Beacons

> ➢ Management and Other Data frames, including successfully transmitted unicast frames and multicast/broadcast data frames (excluding retransmissions, excluding Beacons in BU)

■ **Total submitted frames (bridge):** The total number of data frames submitted to the internal bridge for transmission to the wireless media. The count does not include control and wireless management frames, or retransmissions. There are also separate counts for each priority queue to which the frames were routed, which are High, Mid and Low (currently the High queue is not used for data frames).

■ **Frames dropped (too many retries):** The number of dropped frames, which are the frames unsuccessfully retransmitted until the maximum permitted number of retransmissions without being acknowledged. This count includes dropped data frames as well as dropped control and wireless management frames.

■ **Total retransmitted frames:** The total number of retransmissions, including all unsuccessful transmissions and retransmissions.

■ **Total transmitted concatenated frames:** The total number of concatenated frames transmitted successfully to the wireless media, excluding retransmissions. There are also separate counts for Single and Double concatenated frames (for more details refer to Concatenation Parameters on page 4-81).

■ **Total Tx events:** The total number of transmit events. Typically, transmission events include cases where transmission of a frame was delayed or was aborted before completion. The following additional counters are displayed to indicate the reason for and the nature of the event:

➢ Dropped: The number of dropped frames, which are the frames unsuccessfully retransmitted until the maximum permitted number of retransmissions without being acknowledged.

➢ Underrun: The number of times that transmission of a frame was aborted because the rate of submitting frames for transmission exceeds the available transmission capability.

➢ Others: The number of frames whose transmission was not completed or delayed due to a problem other than those represented by the other counters.

■ **Total received frames from wireless:** The total number of frames received from the wireless media. The count includes data frames as well as control and wireless management frames. The count does not include bad frames and duplicate frames. For a description of these frames, refer to Bad frames received and Duplicate frames discarded below.

■ **Total received data frames:** The total number of data data frames received from the wireless media, including duplicate frames. Refer to Duplicate frames discarded below.

■ **Total Rx events:** The total number of frames that were not received properly. The following additional counters are displayed to indicate the reason for the failure:

> ➢ Phy: Applicable only when DFS is enabled. The number of unidentified signals.

> ➢ CRC: The number of frames received from the wireless media containing CRC errors.

> ➢ Overrun: The number of frames that were discarded because the receive rate exceeded the processing capability or the capacity of the Ethernet port.

> ➢ Decrypt: The number of frames that were not received properly due to a problem in the data decryption mechanism.

- **Total received concatenated frames:** The total number of concatenated frames received from the wireless media, including duplicate frames. There are also separate counts for Single and Double concatenated frames (for more details refer to Concatenation Parameters on page 4-81).

- **Bad fragments received:** The number of fragments received from the wireless media containing CRC errors.

- **Duplicate frames discarded:** The number of data frames discarded because multiple copies were received. If an acknowledgement message is not received by the originating unit, the same data frame can be received more than once. Although duplicate frames are included in all counters that include data frames, only the first copy is forwarded to the Ethernet port.

- **Internally discarded MIR:** The number of data frames received from the Ethernet port that were discarded by the MIR mechanism to avoid exceeding the maximum permitted information rate.

Ping Test

The *Ping Test* submenu is used to control pinging from the unit and includes the following options:

- **Destination IP Address:** The destination IP address of the device being pinged. The default IP address is 192.0.0.1.

- **Number of Pings to Send:** The number of ping attempts per session. The available range is from 0 to 9999. The default value is **1**. Select 0 for continuous pinging.

- **Ping Frame Length:** The ping packet size. The available range is from 60 to 1472 bytes. The default value is 64 bytes.

■ **Ping Frame Timeout:** The ping frame timeout, which is the amount of time (in ms) between ping attempts. The available range is from 100 to 60,000 ms. The default value is 200 ms.

■ **Start Sending:** Starts the transmission of ping frames.

■ **Stop Sending:** Stops the transmission of ping frames. The test is automatically ended once the number of pings has reached the value specified in the **No. of Pings** parameter, described above. The **Stop Sending** option can be used to end the test before completing the specified number of pings, or if continuous pinging is selected.

■ **Show Ping Test Values:** Displays the current values of the ping test parameters, the transmission status, which means whether it is currently sending or not sending pings, the number of pings sent, and the number of pings received, which means the number of acknowledged frames.

Link Quality (RB only)

The Link Quality submenu enables viewing continuously updated information on the quality of the wireless link. The Link quality submenu includes the following options:

Continuous Average SNR Display

The Continuous Average SNR Display option displays continuously updated information regarding the average quality of the received signal, using Signal to Noise Ratio (SNR) measurements.

Click the **Esc** key to abort the test.

Continuous UpLink Quality Indicator Display

The Continuous UpLink Quality Indicator Display option displays continuously updated information regarding the average quality of the wireless link to the BU, using the dynamically updated average modulation level measurements. The Link Quality Indicator (LQI) calculation is performed using the formula:

LQI = (0.9 x "Previous LQI") + (0.1 x "Last Successful Modulation Level").

Each successful transmit will be included in this average, by using the modulation level in which the frame was successfully transmitted as the "Last Successful Modulation Level".

In order to get quick and reliable LQI measurements, there should be sufficient traffic between the RB and the BU. It is recommended to have traffic of at least 100 packets per second. The traffic can be generated either by an external utility (FTP session, ping generator, etc.) or by the Ping Test option in the Site Survey menu with the appropriate settings (see <u>Ping Test</u> on page 4-31).

NOTE

If Limited Test is indicated next to the LQI results, it means that the results may not indicate the true quality since not all modulation levels from 1 to 8 are available. The limitation may be due to the applicable parameters in the country code, or the configurable Maximum Modulation Level parameter.

Click the **Esc** key to abort the test.

MAC Address Database

The MAC Address Database submenu includes the following options:

■ MAC Address Database in BU

■ MAC Address Database in RB

MAC Address Database in BU

The **MAC Address Database** option in the BU displays information regarding the RB associated with it, as well as bridging (forwarding) information. The following options are available:

■ **Display Bridging and Association Info:** The Display Bridging and Association Info option displays a list that includes the associated RB and stations in the BU's Forwarding Database. For stations behind an RB, the RB's MAC address is also displayed (RB Address).

Each MAC address entry is followed by a description, which may include the following:

➢ **Et (Ethernet):** An address learned from the Ethernet port.

➢ **Vp (Virtual port):** An address of a node behind an associated RB. For these addresses, learned from the wireless port, the address of the RB is also displayed (in parenthesis).

➢ **St (Static):** An associated RB. For this entry, the SW version of the RB is also displayed.

➢ **Sp (Special):** 7 addresses that are always present, which include:

■ The MAC address of the BU, which appears twice as it is learned from both the Ethernet and wireless ports.

■ The MAC address of the internal Operating System stack, which also appears twice.

■ Alvarion's Multicast address (01-20-D6-00-00-01, which also appears twice. The system treats this address as a Broadcast address.

■ The Ethernet Broadcast address (FF-FF-FF-FF-FF-FF).

In addition, a summary table displays information about the Forwarding Database (Bridging Info) and the Associated RB Database (Association Info). Each database includes the following information:

➢ The current number of entries. For Bridging Info this includes the **Et** (Ethernet) and the **Vp** (Virtual ports) entries. For Association Info this is the number of currently associated RBs (0 or 1).

NOTE

There is no aging algorithm for associated RBs. An RB is only removed from the list of associated RBs under the following conditions:

a. A SNAP frame is received from another BU indicating that the RB is now associated with the other BU.

b. The RB failed to respond to a certain number of consecutive frames transmitted by the BU and is considered to have "aged out".

➢ The aging time specified for entries in these tables. The aging time for Bridging Info is as specified by the **Bridge Aging Time** parameter. The default is **300** seconds. There is no aging time for Association Info entries.

➢ The maximum number of entries permitted for these tables, which are **1017** (1024 minus the number of special Sp addresses as defined above) for Bridging Info and 1 for Association Info.

■ **Display Association Info:** Displays information regarding the RB associated with the BU. The entry includes the following information:

➢ The MAC Address of the associated RB

➢ Age in seconds, indicating the elapsed time since receiving the last packet from the RB.

➢ The value configured for the Maximum Modulation Level parameter of the RB

➢ The Status of the RB. There are three options:

A. **Associated**

B. **Authenticated**

C. **Not Authenticated** (a temporary status)

The various status states are described in Table 4-4 (this is a simplified description of the association process without the effects of the Best BU algorithm).

Table 4-4: Authentication and Association Process		
Message	**Direction**	**Status in BU**
RB Status: Scanning		
A Beacon with correct ESSID	BU $\rightarrow$ RB	-
RB Status: Synchronized		
Authentication Request	RB $\rightarrow$ BU	Not authenticated
Authentication Successful	BU $\rightarrow$ RB	Authenticated
RB Status: Authenticated		
Association Request	RB $\rightarrow$ BU	Authenticated
Association Successful	BU $\rightarrow$ RB	Associated
RB Status: Associated		
ACK	RB $\rightarrow$ BU	Associated
Data Traffic	RB $\leftrightarrow$ BU	Associated

➢ The SNR measured at the RB

➢ The SW version of the RB.

➢ Distance.

➢ Unit Type.

In addition, a summary table displays information about the Forwarding Database (Bridging Info). The database includes the following information:

➢ The current number of entries. This is the number of currently associated RBs (0 or 1).

> **NOTE**
>
> There is no aging algorithm for associated RBs. An RB is only removed from the list of associated RBs under the following conditions:
>
> A. A SNAP frame is received from another BU indicating that the RB is now associated with the other BU.
>
> B. The RB failed to respond to a certain number of consecutive frames transmitted by the BU and is considered to have "aged out".

> ➢ The aging time specified for entries in these table. There is no aging time for Association Info entries.

> ➢ The maximum number of entries permitted for this table, which is 1.

MAC Address Database in RB

The **MAC Address Database** option in the RB displays information regarding the RB's bridging (forwarding) information. The following option is available:

■ **Display Bridging Info:** The Display Bridging Info option displays a list of all the stations in the RB's Forwarding Database.

Each MAC address entry is followed by a description, which may include the following:

> ➢ **Et (Ethernet):** An address learned from the Ethernet port.

> ➢ **Wl (Wireless):** An address of a node behind the associated BU, learned via the wireless port.

> ➢ **Sp (Special):** 8 addresses that are always present, which include:

> > ■ The MAC address of the RB, which appears twice as it is learned from both the Ethernet and wireless ports.

> > ■ The MAC address if the internal Operating System stack, which also appears twice.

> > ■ Alvarion's Multicast address (01-20-D6-00-00-01), which also appears twice. The system treats this address as a Broadcast address.

> > ■ Alvarion's special Multicast address (01-20-D6-00-00-05), reserved for future use.

> > ■ The Ethernet Broadcast address (FF-FF-FF-FF-FF-FF).

In addition, a summary table displays information about the Forwarding Database (Bridging Info). The summary table includes the current number of entries, the aging time specified by the Bridge Aging Time parameter and the maximum number of entries permitted for this table, which is 1016.

Per Modulation Level Counters

The Per Modulation Level Counters display statistics relating to wireless link performance at different radio modulation levels. The Per Modulation Level Counters menu includes the following options:

■ **Display Counters:** Select this option to display the current values of the Per Modulation Level Counters.

■ **Reset Counters:** Select this option to reset the Per Modulation Level Counters.

The statistics show the number of frames accumulated in different categories since the last reset.

The Per Modulation Level Counters display the following information for each modulation level supported by the unit:

■ **SUCCESS:** The total number of successfully transmitted frames at the applicable modulation level.

■ **FAILED:** The total number of failures to successfully transmit a frame during a HW Retry cycle at the applicable rate.

In the RB, the **Average Modulation Level (AML)** is also displayed. This is the average modulation level (rounded to the nearest integer) since the last time the Per Modulation Level counters were reset. The average is calculated using the **SUCCESS** count at each modulation level as weights.

Link Capability

The Link Capability option provides information on HW and SW capabilities of relevant units. In a BU, the information provided in the Link Capability reports is for the associated RB. In an RB, the Link Capability reports include information on all BUs in the neighboring BUs table (all BUs with whom the RB can communicate).

The Link Capability feature enables to adapt the configuration of the unit according to the capabilities of other relevant unit(s) to ensure optimal operation.

The Link Capability submenu differs between BUs and RBs:

Link Capability options in RB

Show Link Capability-General

Select this option to view information on general parameters of relevant BUs. For each relevant BU, identified by its MAC address, the following details are displayed:

■ **HwVer**: the hardware version of the unit.

■ **Country**: The 3 or 4 digits country code supported by the unit.

■ **SwVer**: The SW version used by the unit.

Show Link Capability-Wireless Link Configuration

Select this option to view information on current wireless link parameters of relevant BUs. For each relevant BU, identified by its MAC address, the following details are displayed:

■ **ATPC Option**: Enable or Disable.

■ **Adaptive Modulation Option**: Enable or Disable.

■ **Burst Mode Option**: Enable or Disable.

■ **DFS Option**: Enable or Disable.

■ **Concatenation Option**: Enable or Disable.

Show Link Capability-Security Configuration

Select this option to view information on current security related parameters of relevant BUs. For each relevant BU, identified by its MAC address, the following details are displayed:

■ **Security Mode**: WEP or AES.

■ **Authentication Algorithm**: Shared Key or Open System.

■ **Data Encryption Option**: Enable or Disable.

Show Link Capability by BU (RB only)

Select this option to view all capabilities information (General, wireless Link Configuration, Security Configuration) of a selected BU (by its MAC address).

Link Capability Options in BU

In the BU, the Link Capability submenu includes a single option, Show Link Capability:

Show Link Capability

Select this option to view all capabilities information (General, Wireless Link Configuration, Security Configuration) of the associated RB. The displayed information includes:

<u>**General:**</u>

- ■ **HwVer**: the hardware version of the unit.

- ■ **CpldVer**: The version of the Complex Programmable Logic Device (CPLD) used in the RB.

- ■ **Country**: The 3 or 4 digits country code supported by the unit.

- ■ **BootVer**: The Boot Version of the unit.

<u>**Wireless Link Configuration:**</u>

- ■ **ATPC Option**: Enable or Disable.

- ■ **Adaptive Modulation Option**: Enable or Disable.

- ■ **Burst Mode Option**: Enable or Disable.

- ■ **DFS Option**: Enable or Disable. This parameter is available only in RBs, displaying the current option in the relevant BU.

- ■ **Concatenation Option**: Enable or Disable.

<u>**Security Configuration:**</u>

- ■ **Security Mode**: WEP or AES.

- ■ **Authentication Algorithm**: Shared Key or Open System.

- ■ **Data Encryption Option**: Enable or Disable.

Advanced Configuration Menu

The Advanced Configuration menu provides access to all parameters, including the parameters available through the Basic Configuration menu.

The Advanced Configuration menu enables accessing the following menus:

■ IP Parameters

■ Air Interface Parameters

■ Network Management Parameters

■ Bridge Parameters

■ Performance Parameters

■ Service Parameters (RB only)

■ Security Parameters

IP Parameters

The IP Parameters menu enables defining IP parameters for the selected unit and determining its method of IP parameter acquisition.

The IP Parameters menu includes the following options:

■ IP Address

■ Subnet Mask

■ Default Gateway Address

■ DHCP Client

IP Address

The IP Address parameter defines the IP address of the unit.

The default IP address is 10.0.0.1.

Subnet Mask

The Subnet Mask parameter defines the subnet mask for the IP address of the unit.

The default mask is 255.0.0.0.

Default Gateway Address

The Default Gateway Address parameter defines the IP address of the unit's default gateway.

The default value for the default gateway address is 0.0.0.0.

DHCP Client

The DHCP Client submenu includes parameters that define the method of IP parameters acquisition.

The DHCP Client submenu includes the following options:

■ DHCP Option

■ Access to DHCP

DHCP Option

The DHCP Option displays the current status of the DHCP support, and allows selecting a new operation mode. Select from the following options:

■ Select **Disable** to configure the IP parameters manually. If this option is selected, configure the static IP parameters as described above.

■ Select **DHCP Only** to cause the unit to search for and acquire its IP parameters, including the IP address, subnet mask and default gateway, from a DHCP (Dynamic Host Configuration Protocol) server only. If this option is selected, you must select the port(s) through which the unit searches for and communicates with the DHCP server, as described in the following parameter, Access to DHCP. You do not have to configure static IP parameters for the unit. DHCP messages are handled by the units as management frames.

■ Select **Automatic** to cause the unit to search for a DHCP server and acquire its IP parameters from the server. If a DCHP server is not located within approximately 40 seconds, the currently configured parameters are used. If this option is selected, you must configure the static IP parameters as described above. In addition, you must select the port(s) through which the unit searches for and communicates with the DHCP server, as described in the following parameter, Access to DHCP.

The default is Disable.

Access to DHCP

The Access to DHCP option enables defining the port through which the unit searches for and communicates with a DHCP server. Select from the following options:

■ From Wireless Link Only

■ From Ethernet Only

■ From Both Ethernet and Wireless Link

The default for BU is From Ethernet Only. The default for RB is From Wireless Link Only.

Show IP Parameters

The Show IP Parameters option displays the current values of the IP parameters, including the **Run Time IP Address, Run Time Subnet Mask** and **Run Time Default Gateway Address**.

Air Interface Parameters

The Air Interface Parameters menu enables viewing the current Air Interface parameters defined for the unit and configuring new values for each of the relevant parameters.

Country Code and Sub Bands

Each country has its own regulations regarding operation modes and parameters such as allowable frequencies and bandwidth, the need to employ an automatic mechanism for detection and avoidance of frequencies used by radar systems, maximum transmit power at each of the supported modulation levels and the ability to use burst transmissions. To efficiently manage these country dependent parameters, each unit has a 'Country Code' parameter and a set of accompanying parameters, which depend on this country code. Where more than one set of parameters can be used, the available sets are defined as Sub Bands, selectable through the Frequency configuration menu.

ESSID Parameters

The ESSID (Extended Service Set ID) is a string used to identify a wireless network and to prevent the unintentional merging of two wireless networks or two sectors in the same network. Typically, a different ESSID is defined for each BU. To facilitate easy addition of an RB to an existing network without a prior knowledge of which specific BU will serve it, and to support the Best BU feature, a secondary "global" ESSID, namely "Operator ESSID", can be configured in the BU. If the Operator ESSID Option is enabled at the BU, the Beacon frames transmitted by it will include both the ESSID and Operator ESSID. The RB shall regard such frames if either the ESSID or the Operator ESSID matches it own ESSID. The ESSID of the BU with which the RB is eventually associated is defined as the Run-Time ESSID of the RB. Typically, the initial ESSID of the RB is configured to the value of the Operator ESSID. Once the RB has become associated with a specific BU, its ESSID can be reconfigured to the value of the ESSID of the BU.

ESSID

The ESSID parameter defines the ESSID of the unit.

Valid values: A string of up to 31 printable ASCII characters.

The default value is ESSID1.

> **NOTE**
>
> The ESSID string is case sensitive.

Operator ESSID Parameters (BU only)

The Operator ESSID Parameters submenu includes the following parameters:

Operator ESSID Option

The Operator ESSID Option enables or disables the use of Operator ESSID for establishing association with RBs.

The default is Enable.

Operator ESSID

The Operator ESSID parameter defines the Operator ESSID.

Valid values: A string of up to 31 printable ASCII characters.

The default value is ESSID1.

> **NOTE**
>
> The Operator ESSID string is case sensitive.

Frequency Definition Parameters

Sub-Bands and Frequency Selection

The parameters that determine the frequency to be used are set in the BU. The RB should be configured with a minimal set of parameters to ensure that it will be able to automatically detect and use the frequency used by the BU, including possible changes in this frequency.

To simplify the installation process the RB scans a definable frequencies subset after power-up. If the Best BU feature is enabled, the RB will scan the defined subset and the operating frequency will be determined by the Best BU mechanism (including the optional use of the Preferred BU feature). Otherwise the RB will try to associate with the first BU it finds. If no BU is found, the RB will start another scanning cycle.

Each unit is delivered with one or more pre-configured Sub-Bands, according to the country code. These sets of parameters include also the frequencies that can be used and the bandwidth. If more than one Sub-Band is available, the sub-band to be used can be selected in both the BU and the RB. If only one Sub-Band is supported, then the sub-band selection option is not available.

Avoiding Frequencies with Radar Activity

In some regions, it is important to ensure that wireless equipment does not interfere with certain radar systems in the 5 GHz band. In case radar is being detected, the wireless equipment should move automatically to a frequency that does not interfere with the radar system.

The country dependent set of parameters includes also an indication whether DFS (Dynamic Frequency Selection) should be used. The DFS algorithm is designed to detect and avoid operation in channels with radar activity. If the current sub-band does not support DFS, then the DFS parameters configuration submenu is not available.

When the DFS Option is enabled, the BU monitors the spectrum continuously, searching for signals with a specific pattern indication radar activity. Upon detecting radar activity, the BU immediately stops transmitting on this frequency and starts looking for another radar-free frequency. The subset of viable frequencies is configurable.

The BU maintains a continuously updated database of all applicable frequencies, where each frequency is marked as Radar Free, Radar Detected or Adjacent to Radar. The BU attempts to check a new frequency only if it is marked as Radar Free. If a radar activity was detected on a certain frequency, it will be marked in the database as a Radar Detected frequency. The BU will not attempt to check for radar activity in frequencies marked as Radar Detected. A certain time after detecting radar activity on a frequency, it will be removed from the list of Radar Detected frequencies and will be marked as Radar Free. If radar activity was detected on a certain frequency, adjacent channels should not be used as well, according to the bandwidth. For instance, if the bandwidth is 20 MHz, then if radar activity was detected in 5800 MHz, frequencies 5790 MHz and 5810 MHz should not be used as well. These frequencies are marked in the database as Adjacent to Radar, and will be treated the same as Radar Detected frequencies.

Before ceasing transmission on the frequency where radar signals had been detected, the BU sends a special disassociation message to its associated RB. This message includes an indication whether the RB should wait for this BU. If the RB should wait, the message includes also the waiting time. During this time each RB searches for the BU in the defined frequencies subset. If the BU was not found within the waiting time, or if a waiting request was not included in the message, the RB starts searching for any BU, using the Best BU mechanism if applicable.

Typically, operators prefer to preserve the original frequency planning and to avoid moving to a new channel unless we are sure that there is a continuous radar activity in the original channel. It should be noted that detection of radar activity does not necessarily indicate a continuous radar activity in the channel. A channel reuse algorithm enables returning to the original channel under certain conditions that indicates low radar activity on the channel.

Frequency Definition Submenu in BU

The Frequency Definition submenu in BU includes the following parameters:

Sub Band Select

This parameter is available only if the country code supports two or more Sub Bands. For information on how to view the Sub Bands supported by the unit and the supported parameters' values and options, refer to **Show Country Dependent Parameters** on page 4-8.

The range depends on the number of Sub Bands supported by the country code.

The default selection is Sub Band 1.

> **NOTE**
>
> For compliance with ETSI regulations, the bandwidth used in the default Sub Band for units in the 5.4 GHz band is 20 MHz. The use of a Sub Band with a 40 MHz bandwidth (Turbo Mode) in the 5.4 GHz band is allowed only if approved by the applicable local regulatory administration.

Frequency

The Frequency parameter defines the transmit/receive frequency when the DFS Option is not enabled. If the DFS Option is enabled, it sets the initial operational frequency upon starting the DFS mechanism the first time.

The range depends on the selected Sub Band.

The default is the lowest frequency in the Sub Band.

NOTE

In units operating in the 5.3 GHz band, the following rules must be met for full compliance with FCC regulations:

1. In units that use a 20 MHz bandwidth:

   a. Frequency channel 5260 MHz should not be used.

   b. When operating at 5270 MHz, the Transmit Power parameter in the BU, and the Maximum Tx Power parameter in the RB connected to this BU, should not be set to a value above "17-Antenna Gain" (The maximum allowed EIRP for 5270 MHz is 17 dBm).

2. In units that use a 40 MHz bandwidth (Turbo Mode): Frequency channels 5270 and 5280 MHz should not be used.

DFS Parameters

The DFS Parameters submenu is available only if DFS is supported by the current Sub Band. The DFS Parameters submenu includes the following parameters:

DFS Option

The DFS Option enables or disables the radar detection and dynamic frequency selection mechanism.

The default is Enable.

Frequency Subset Definition

The Frequency Subset Definition parameter defines the frequencies that will be used in the DFS mechanism. The available frequencies according to the Sub Band are displayed, and each of the frequencies in the list is associated with an index. The frequencies subset can be defined by entering the indexes of the required frequencies, or "A" to select all available frequencies.

The default is the complete list of frequencies available in the Sub Band.

Channel Check Time

The Channel Check Time defines the time allocated for checking whether there is a radar activity on a new frequency after power up or after trying to move to a new frequency upon detecting radar activity on the previously used frequency. During this time the BU does not transmit.

The range is 1 to 3600 seconds.

The default is 60 seconds.

Channel Avoidance Period

The Channel Avoidance Period defines the time that the frequency will remain marked in the database as Radar Detected or Adjacent to Radar after detecting radar activity. These frequencies will not be used when searching for a new frequency. Once this time has elapsed, the unit frequency's marking will change to Radar Free.

The range is 1 to 60 minutes.

The default is 30 minutes.

RB Waiting Option

The RB Waiting Option defines whether the disassociation message sent by the BU, after detecting radar activity on the current frequency, will include a message instructing the RB to search only for the BU before attempting to search for another BU. The message includes also the time period during which the RB should not search for any other BU. The waiting tine is the Channel Check Time plus 5 seconds.

The default is Enable.

Minimum Pulses to Detect

The Minimum Pulses to Detect parameter defines the minimum number of radar pulses that should be detected before reaching a decision that radar is active on the channel.

The range is from 1 to 100 pulses.

The default is 6 pulses.

Reset Radar Detected Channels After Reset

When the Reset Radar Detected Channels After Reset is enabled, than after the next reset all viable frequencies will be marked in the database as Radar Free, including frequencies previously marked as either Radar Detected or Adjacent to Radar. In addition, the BU will start operation using its default frequency.

The default is Disable.

Channel Reuse Parameters (DFS+)

The Channel Reuse algorithm enables returning to the original channel under certain conditions that indicate low radar activity on the original channel. The conditions are that radar was detected in this channel not more than N times (Maximum Number of Detections in Assessment Period) during the last T hours (Radar Activity Assessment Period). When the Channel Reuse Option is enabled, then by the end of the Channel Avoidance Period the unit will attempt returning to the original frequency, provide these conditions are met.

The Channel Reuse Parameters submenu includes the following options:

■ **Channel Reuse Option**: Enabling/disabling the Channel Reuse algorithm.

The default is Disable.

■ **Radar Activity Assessment Period**: The period in hours used for assessment of radar activity in the original channel.

The range is 1 to 12 hours.

The default is 5 hours.

■ **Maximum Number of Detections in Assessment Period**: The maximum number of radar detection in the original channel during the Radar Activity Assessment Period that is required for reaching a decision to try again the original channel.

The range is 1 to 10 radar detections.

The default is 5 radar detections.

Show DFS Settings And Data

Upon selecting the Show DFS Settings and Data, the values of all DFS parameters and the current operating frequency will be displayed. The current defined frequency subset as well as the defined subset (to be used after the next reset) are also displayed. In addition, all the applicable frequencies will be displayed together with their status in the database (Radar Free, Radar Detected or Adjacent to Radar).

Show Frequency definitions

Upon selecting Show Frequency Definitions, the selected Sub Band and Frequency are displayed. In addition, all the parameters displayed upon selecting Show DFS Settings and Data are also displayed.

Frequency Definition Submenu in RB

Sub Band Select

This parameter is available only if the country code supports two or more Sub Bands. For information on how to view the Sub Bands supported by the unit and the supported parameters' values and options, refer to [Show Country Dependent Parameters](#) on page 4-8.

The range depends on the number of Sub Bands supported by the country code.

The default selection is Sub Band 1.

Frequency Subset Definition

The Frequency Subset Definition parameter defines the frequencies that will be used in by the RB when scanning for an BU. The available frequencies according to the Sub Band are displayed, and each of the frequencies in the list is associated with an index. The frequencies subset can be defined by entering the indexes of the required frequencies, or "A" to select all available frequencies.

The default is the complete list of frequencies available in the Sub Band.

Show Frequency Definitions

Upon selecting the Show Frequency Definitions, the selected Sub Band parameters and the current operating frequency will be displayed. The current frequency subset, as well as the defined subset (to be used after the next reset), are also displayed.

Best BU Parameters (RB)

In certain applications multiple BUs may be used to provide redundancy for high availability. An RB that can communicate with more than one BU using the same ESSID may become associated with the first BU it "finds", not necessarily the best choice in terms of quality of communication or other factors.

The desire to create best throughput conditions for the RB created the need for the Best BU feature, to enable an RB to connect to the best BU in its neighborhood.

When the Best BU feature is used, each of the BUs is given a quality mark based on the level at which it is received by the RB. The RB scans for a configured number of cycles, gathering information from all the BUs it can communicate with. At the end of the scanning period, the RB reaches a Best BU decision according to the information gathered. The BU with the highest quality mark is selected as the Best BU, and the RB will immediately try to associate with it. The quality mark given to each BU depends on the level at which it is received by the RB.

The Best BU selection mechanism can be overridden by defining a specific BU as the preferred BU.

The Best BU Parameters menu includes the following options:

Best BU Support

The Best BU Support option enables or disables the Best BU selection feature.

The default is Disable.

NOTE

If the Best BU feature is not used, the RB associates with the first free BU it finds whose ESSID or Operator ESSID is identical to its own ESSID.

Number Of Scanning Attempts

When the Best BU option is enabled, the RB gathers information on neighboring free BUs for approximately 2 seconds on each of the scanned frequencies. The Number of Scanning Attempts parameter defines the number of times that the process will be repeated for all relevant frequencies. A higher number may result in a better decision at the cost of an increased scanning time during which the RB is not operational.

Valid values: 1 - 255.

Default value: 4.

Preferred BU MAC Address

The Preferred BU MAC Address parameter defines a specific BU with which the RB should associate. Gaining control of the RB association is a powerful tool in network management. The Preferred BU MAC Address parameter is intended for applications where there is a need to dictate the preferred BU with whom the RB should associate. To prevent the RB from associating with the first viable BU it finds, the Best BU Support mechanism should be enabled. Once the RB has identified the preferred BU based on its MAC address, it will associate with it and terminate the scanning process. If the preferred BU is not found, the RB will associate with a BU according to the decision reached using the best BU algorithm.

Valid values: A MAC address string.

The default value for the Preferred BU MAC Address is 00-00-00-00-00-00 (12 zeros), meaning that there is no preferred BU.

Show Best BU Parameters and Data

The Show Best BU Parameters and Data option displays the applicable information:

The **Neighboring BU Data table** displays for each BU that the unit can communicate with the following details:

- **MAC Address**

- **SNR** of the received signal

- **Mark** - The computed quality mark for the BU.

- **Full** - The association load status of the BU. It is defined as full if it is already associated with an RB. A BU whose associations load status is full cannot be selected as the Best BU, even if its' computed mark is the highest.

- **ESSID** - The ESSID of the BU.

In addition to the neighboring BU data table, the following information is displayed:

- **Best BU Support**

- **Preferred BU MAC Address**

- **Number of Scanning Attempts**

- **Associated BU MAC Address** (the MAC address of the selected BU)

Scanning Mode (RB only)

The Scanning Mode parameter defines whether the RB will use Passive or Active scanning when searching for a BU.

In passive scanning, the RB "listens" to the wireless media for approximately two seconds at each frequency, searching for beacons. The disassociation period, which is the time from the moment the link was lost until the RB decides that it should start searching for another BU, is approximately seven seconds.

In some situations when there is a high probability that RB might need to roam among different BUs, the use of active scanning enables to significantly reduce the link establishment time. This is achieved by using shorter dwell periods, transmitting a Probe Request at each frequency. This reduces the time spent at each frequency as well as the disassociation period.

When DFS Option is enabled, Scanning Mode is forced to Passive.

The default selection is Passive.

Power Control Parameters

The Automatic Transmit Power Control (ATPC) algorithm simplifies the installation process and ensures optimal performance while minimizing interference to other units. This is achieved by automatically adjusting the power level transmitted by the RB according to the actual level at which it is received by the BU. To support proper operation of the system with optimal performance and minimum interference between neighboring systems, the ATPC algorithm should be enabled in both BU and RB.

The algorithm is controlled by the BU that calculates for each received frame the average SNR at which it receives transmissions from the RB. The average calculation takes into account the previous calculated average, thus reducing the effect of short temporary changes in link conditions. The weight of history (the previous value) in the formula used for calculating the average SNR is determined by a configurable parameter. In addition, the higher the time that has passed since the last calculation, the lower the impact of history on the calculated average. If the average SNR is not in the configured target range, the BU transmits to the RB a power-up or a power-down message. The target is that the RB will be received at an optimal level, or as high (or low) as possible if the optimal range cannot be reached because of specific link conditions.

Each time that the RB tries to associate with the BU (following either a reset or loss of synchronization), it will initiate transmissions using its' **Transmit Power** parameters. If after a certain time the RB does not succeed to synchronize with the BU, it will start increasing the transmit power level.

In a BU the maximum supported transmit power is typically used to provide maximum coverage. However, there may be a need to decrease the transmitted power level in order to support relatively short links and to minimize the interference with the operation of neighboring systems, or for compliance with local regulatory requirements.

In some cases the maximum transmit power of the RB should be limited to ensure compliance with applicable regulations or due to other reasons.

Different power levels may be used for different modulation levels to optimize performance taking into account the different modulation schemes as well as possible regulatory restrictions.

Transmit Power

The Transmit Power parameters are defined separately for different modulation levels. Note that the supported modulation levels depend on the Min modulation Level and Max Modulation Level defined for the applicable Sub Band.

In the BU, the Transmit Power parameter defines the fixed transmit power level and is not a part of the ATPC algorithm.

In the RB, The Initial Transmit Power parameter defines the fixed transmit power level when the ATPC algorithm is disabled. If the ATPC Option is enabled the value configured for this parameter serves for setting the initial value to be used by the ATPC algorithm after either power up or loosing synchronization with the BU.

The minimum value for the Transmit Power Parameters is -10 dBm. (The ATPC may reduce the actual transmit power of the SU to lower values). The maximum value of the Transmit Power Parameter depends on several unit properties and parameters:

■ The modulation level

■ The Maximum Allowed Tx Power as defined for the applicable Sub Band.

- The Maximum EIRP as defined for the applicable Sub Band, together with the value of the Antenna Gain. In certain countries the Maximum EIRP of some equipment types cannot exceed a certain value. In these cases the Transmit Power cannot exceed the value of (Maximum EIRP – Antenna Gain).

- Maximum Tx Power parameter (in RB only)

For information on how to view the Sub Bands supported by the unit and the supported parameters' values and options, refer to Show Country Dependent Parameters on page 4-8.

The unit calculates the maximum allowed Transmit Power according to the unit properties and parameters listed above, and displays the allowed range when a Transmit Power parameter is selected.

The default Transmit Power is the highest allowed value.

Maximum Tx Power (RB only)

The Maximum Tx Power parameter limits the maximum transmit power that can be reached by the ATPC algorithm. It also sets the upper limits for the Transmit Power parameters.

The minimum value for the Maximum Tx Power is -10 dBm. The maximum value depends on several unit properties and parameters:

- The modulation level

- The Maximum Allowed Tx Power as defined for the applicable Sub Band.

- The Maximum EIRP as defined for the applicable Sub Band, together with the value of the Antenna Gain. In certain countries the Maximum EIRP of some equipment types cannot exceed a certain value. In these cases the Transmit Power cannot exceed the value of (Maximum EIRP – Antenna Gain).

For information on how to view the Sub Bands supported by the unit and the supported parameters' values and options, refer to Show Country Dependent Parameters on page 4-8.

The unit calculates the maximum allowed Maximum Tx Power according to the unit properties and parameters listed above, and displays the allowed range when the Maximum Tx Power parameter is selected.

The default Maximum Tx Power is the highest allowed value.

ATPC Parameters in BU

ATPC Option

The ATPC Option enables or disables the Automatic Transmit Power Control (ATPC) algorithm.

The default is Enable.

ATPC Minimum SNR Level

The Minimum SNR Level defines the lowest SNR at which you want the RB to be received at the BU (the lower limit of the optimal reception level range).

Available values: 4 to 60 (dB).

Default value: 28 (dB).

ATPC Delta from Minimum SNR Level

The Delta from Minimum SNR Level is used to define the highest SNR at which you want each RB to be received at the BU (the higher limit of the optimal reception level range):

Max. Level=Minimum SNR Level + Delta from Minimum SNR Level.

Available values: 4 to 20 (dB).

Default value: 5 (dB) for units operating in the 4.4 or 5.8 GHz bands. 11 (dB) for units operating in the 5.2 or 5.3 GHz bands.

Minimum Interval Between ATPC Messages

The Minimum Interval Between ATPC Messages parameter sets the minimal time between consecutive power-up/power-down messages to the RB. Setting a low value for this parameter may lead to a higher overhead and an excessive rate of power level changes at the RBs High values for this parameter increase the time it will take until the RB reach optimal transmit power level.

Available values: 1 to 3600 seconds.

Default value: 30 seconds.

ATPC Power Level Step

The ATPC Power Level Step parameter defines the step size to be used by the RB for incrementing/decrementing the **Current Transmit Power** after receiving a power-up/power-down message. If the distance between the value of the **Current Transmit Power** and the desired range is smaller than the step size, the power-up/power-down message will include the specific step value required for this condition.

Valid range: 1-20 (dB)

Default value: 5 (dB)

ATPC Parameters in RB

ATPC Option

The ATPC Option enables or disables the Automatic Transmit Power Control (ATPC) algorithm. The parameter takes effect immediately. However, when changed from Enable to Disable, the transmit power level shall remain at the last Current Transmit Power determined by the ATPC algorithm before it was disabled. It will change to the value configured for the Initial Transmit Power parameter only after the next reset or following loss of synchronization.

The default is Enable.

NOTE

The accuracy of the Tx Power level is typically +/- 1 dB. However, at levels that are 15 dB or more below the maximum supported by the hardware, the accuracy is +/- 3 dB (for information on hardware limitations refer to the Country Codes document). At these levels the use of ATPC may cause significant fluctuations in the power level of the transmitted signal. When operating at such low levels, it is recommended to disable the ATPC Option and to set the Transmit Power parameter to the average Tx Power level before the ATPC was disabled.

Tx Control (BU only)

The Tx Control option enables turning Off/On the BU's transmitter. This feature can be used during maintenance or testing to avoid transmissions using undesired parameters.

The parameter is available only when managing the unit from its Ethernet port.

The default is On.

NOTE

The unit is reset immediately upon configuring the Tx Control parameter to either On or Off (even if it is set to its current option).

Antenna Gain

The Antenna Gain parameter enables to define the net gain of a detached antenna. The configured gain should take into account the attenuation of the cable connecting the antenna to the unit. The Antenna Gain is important especially in countries where there is a limit on the EIRP allowed for the unit; the maximum allowed value for the Transmit Power parameters cannot exceed the value of (EIRP- Antenna Gain), where the EIRP is defined in the selected Sub Band.

In certain units with an integral antenna the Antenna Gain is not available as a configurable parameter. However, it is available as a read-only parameter in the applicable "Show" menus.

The range is 0 – 50 (dB). A value of "Don't Care" means that the actual value is not important. A value of "Not Set Yet" means that the unit will not transmit until the actual value (in the range 0 to 50) is configured. The unit can be configured to "Don't Care" or "Not Set Yet" only in factory (when upgraded to SW version 2.0 from a lower version it will be set automatically to one of these options). Once a value is configured, it is not possible to reconfigure the unit to either "Don't Care" or "Not Set Yet".

The default value is typically Don't Care for units delivered to countries where there are no regulatory limitations regarding EIRP. When applicable regulations limit the EIRP, then the default is 21 (not changeable) for units with an integral antenna and Not Set Yet for units with a detached antenna.

Link Distance Parameters (BU only)

The higher the distance between the RB and the BU that is serving it, the higher the time it takes for messages sent by one of them to reach the other. The time that a unit waits for a response message before retransmission (acknowledge time delay) should take into account the round trip propagation delay between the two units. (the one-way propagation delay at 5 GHz is 3.3 microsecond/km). The higher the distance between the BU and the RB, the higher should be the acknowledge time delay used by both units.

The distance between the BU and the RB can be determined either manually or automatically. In manual mode, this distance is configured manually. In automatic mode, the BU uses a special algorithm to estimate its distance from the RB.

The Link Distance Parameters menu includes the following parameters:

Link Distance Mode

The Link Distance Mode option defines whether the distance between the BU and the RB will be determined manually (using the Maximum Link Distance parameter) or automatically.

The Options are Automatic or Manual.

The default is Automatic.

Maximum Link Distance

The Maximum Link Distance parameter allows configuring the distance between the BU and the RB when the Link Distance Mode option is Manual.

The range is 0 to 54 (Km). The value of 0 has a special meaning for No Compensation: Acknowledge Time Out is set to a value representing the maximum distance of 54 km. The time slot size is set to its minimal value of 9 microseconds.

The default is 0 (No Compensation).

Show Link Distance Parameters

Select Show Link Distance Parameters to view the Link Distance parameters. In addition, the Measured Maximum Link Distance and the MAC address of the RB are displayed. A distance of 1 km means any distance below 2km.

Wireless Link Trap Threshold (BU only)

The Wireless Link Trap Threshold parameter defines the threshold for the wireless quality trap, indicating that the quality of the wireless link has dropped below (on trap) or has increased above (off trap) the specified threshold.

The Wireless Link Trap Threshold is in percentage of retransmissions, and the allowed range is from 1 to 100 (%). The default is 30 (%).

Spectrum Analysis

Gaining knowledge of the noise characteristics per channel enables construction of a relatively noise free working environment. In order to gain information regarding noise characteristics in the location of the unit, the unit will enter passive scanning mode for a definite period, during which information shall be gathered. The scanned channels will be the channels comprising the selected sub set.

Upon activating the spectrum analysis the unit will automatically reset. During the information-gathering period the unit will not receive nor transmit data. It also will not be able to synchronize/associate, meaning that it cannot be managed via the wireless link. During the spectrum analysis period the unit security mode is changed to promiscuous to enable gathering information regarding all legal frames received by the unit. At the end of the period the unit will reset automatically regaining normal operability upon start up.

The Spectrum Analysis submenu includes the following options:

Spectrum Analysis Channel Scan Period

The Spectrum Analysis Channel Scan Period is the period of staying on each channel during each cycle for information gathering when performing spectrum analysis.

Range: 2-30 seconds.

Default value: 5 seconds.

Spectrum Analysis Scan Cycles

The Spectrum Analysis Scan Cycle is the number of scanning cycles when performing Spectrum Analysis.

Range: 1-100 cycles.

Default value: 2 cycles.

Automatic Channel Selection (BU only)

The Automatic Channel selection option defines weather the BU will choose the best noise free channel upon startup after completion of the spectrum analysis process. The selection is per analysis: once the analysis is completed it will be disabled automatically.

The default is Disable.

Spectrum Analysis Activation

The Spectrum analysis Activation option enables activation of the spectrum analysis process. Upon activation, the unit will reset automatically and start-up in spectrum analysis mode.

Reset Spectrum Analysis Information

The Reset Spectrum Analysis Information option enables resetting the spectrum analysis counters.

Spectrum Analysis Information Display

The Spectrum Analysis Information Display option enables viewing the results of the last analysis process. The displayed information includes the following details for each channel:

■ **Frequency in MHz**

■ **Signal Count**: The number of signals (excluding OFDM frames with the correct bandwidth) in the channel.

■ **Signal SNR**: The approximate SNR of signals (excluding OFDM frames with the correct bandwidth) in the channel.

■ **Signal Width**: The average width in microseconds of signals (excluding OFDM frames with the correct bandwidth) in the channel.

■ **OFDM Frames**: The number of OFDM frames with the correct bandwidth detected in the channel.

Spectrum Analysis Information Display - Continuous

The Spectrum Analysis Information Display - Continuous option is available only when the analysis process is active. It enables viewing the continuously updated results of the current analysis process. The displayed information includes the same details available for a regular Spectrum Analysis Information Display option.

Network Management Parameters

The Network Management Parameters menu enables protecting the Unit from unauthorized access by defining a set of IP addresses from which the unit can be managed using protocols such as Telnet, FTP, TFTP, SNMP, DHCP and ICMP. This excludes management messages generated in the unit, such as Traps or Ping Test frames, which are not filtered. You can also determine the direction from which management access is permitted, which means from the wireless media or the wired Ethernet or both.

The Network Management Parameters menu includes the following options:

■ Access to Network Management

■ Network Management Filtering

■ Set Network Management IP address

■ Delete a Network Management IP Address

■ Delete All Network Management IP Addresses

■ SNMP Traps

Access to Network Management

The Access to Network Management option defines the port through which the unit can be managed. The following options are available:

■ From Wireless Link Only

■ From Ethernet Only

■ From Both Ethernet and Wireless Link

The default selection is From Both Ethernet and Wireless Link.

CAUTION

Be careful not to block your access to the unit. For example, if you manage an RB via the wireless link, setting the Access to Network Management parameter to From Ethernet Only completely blocks your management access to the unit. In this case, a technician may be required to change the settings at the user's site.

Network Management Filtering

The Network Management Filtering option enables or disables the IP address based management filtering. If management filtering is enabled, the unit can only be managed by stations with IP addresses matching one of the entries in the Set Network Management IP Addresses option, described below, and that are connected to the unit via the defined port(s). The following options are available:

■ **Disable:** No IP address based filtering is configured.

■ **Activate IP Filter on Ethernet Port:** Applicable only if the Access to Network Management parameter is configured to either From Ethernet Only or From Both Ethernet and Wireless Link. The unit can be managed from the Ethernet port only by stations with IP addresses matching one of the entries in the Set Network Management IP Addresses parameter. If the Access to Network Management parameter is configured to From Both Ethernet and Wireless Link then no IP address based filtering is configured for the wireless port.

■ **Activate IP Filter on Wireless Link Port:** Applicable only if the Access to Network Management parameter is configured to either From Wireless Link Only or From Both Ethernet and Wireless Link. The unit can be managed from the wireless port only by stations with IP addresses matching one of the entries in the Set Network Management IP Addresses parameter. If the Access to Network Management parameter is configured to From Both Ethernet and Wireless Link then no IP address based filtering is configured for the Ethernet port.

■ **Activate IP filter on Both Ethernet and Wireless Link Ports:** Applicable to all options of the Access to Network Management parameter. The unit can be managed from the port(s) defined by the Access to Network Management parameter only by stations with IP addresses matching one of the entries in the Set Network Management IP Addresses parameter.

The default selection is Disable.

Set Network Management IP Address

The **Set Network Management IP Address** option enables defining up to 10 IP addresses of devices that can manage the unit if the Network Management Filtering option is enabled.

The default Network Management IP Address is 0.0.0.0 (all 10 addresses)

Delete a Network Management IP Address

The Delete Network Management IP Address option enables deleting IP address entries from the Network Management IP Addresses list.

Delete All Network Management IP Addresses

The Delete All Network Management IP Addresses option enables deleting all entries from the Network Management IP Addresses list.

SNMP Traps

The SNMP submenu enables or disables the transmission of SNMP Traps. If this option is enabled, up to 10 IP addresses of stations to which SNMP traps are sent can be defined.

Send SNMP Traps

The Send SNMP Traps option enables or disables the sending of SNMP traps.

The default selection is Disable.

SNMP Traps Destination IP Addresses

The SNMP Traps Destination IP Addresses submenu enables defining up to 10 IP addresses of devices to which the SNMP Traps are to be sent.

The default of all 10 SNMP Traps IP destinations is 0.0.0.0.

SNMP Traps Community

The SNMP Traps Community option enables defining the Community name for each IP address to which SNMP Trap messages are to be sent.

Valid strings: Up to 8 ASCII characters.

The default for all 10 addresses is "public", which is the default Read community.

Delete One Trap Address

The Delete One Trap Address option enables deleting Trap address entries from the SNMP Traps Addresses list.

Delete All Trap Addresses

The Delete All Trap Addresses option enables deleting all entries from the SNMP Traps Addresses list.

Bridge Parameters

The Bridge Parameters menu provides a series of parameter sets that enables configuring parameters such as control and filtering options for broadcast transmissions, VLAN support, and Type of Service prioritization.

The Bridge Parameters menu includes the following options:

■ VLAN Support

■ ToS Parameters

■ Ethernet Broadcast Filtering

■ Bridge Aging Time

■ Roaming Option (RB only)

VLAN Support

The VLAN Support menu enables defining the parameters related to the IEEE 802.1Q compliant VLAN aware (Virtual LAN aware) feature of the BreezeNET B units. Each VLAN includes stations that can communicate with each other, but cannot communicate with stations belonging to different VLANs. The VLAN feature also provides the ability to set traffic priorities for transmission of certain frames. The information related to the VLAN is included in the VLAN Tag Header, which is inserted in each frame between the MAC header and the data. VLAN implementation in BreezeNET B units supports frame routing by port information, whereby each port is connected to only one VLAN.

The VLAN Support menu includes the following parameters:

■ VLAN Link Type

■ VLAN ID – Data (RB only)

■ VLAN ID – Management

■ VLAN Forwarding

■ VLAN Traffic Priority

VLAN ID-Data (RB only)

The VLAN ID-Data is applicable only when the VLAN Link Type parameter is set to Access Link. It enables defining the VLAN ID for data frames, which identifies the VLAN to which the unit belongs.

Valid values range from 1 to 4094.

Default value: 1.

The VLAN ID-Data affects frames received from the wireless link port, as follows:

■ Only tagged frames with a VLAN ID (VID) equal to the **VLAN ID-Data** defined in the unit are forwarded to the Ethernet port.

■ The tag headers are removed from the data frames received from the wireless link before they are transmitted on the Ethernet port.

The VLAN ID-Data affects frames received from the Ethernet port, as follows:

■ A VLAN Data Tag is inserted in all untagged frames received from the Ethernet port before transmission on the wireless link. The tag includes the values of the **VLAN ID-Data** and the **VLAN Priority-Data** parameters.

■ Tagged frames received on Ethernet port, which are meant to be forwarded to the wireless link port, are discarded. This includes frames with tagging for prioritization purpose only.

VLAN ID-Management

The VLAN ID-Management is applicable for all link types. It enables defining the VLAN ID for management frames, which identifies remote stations for management purposes. This applies to all management applications using protocols such as SNMP, TFTP, ICMP (ping), DHCP and Telnet. All servers/stations using these protocols must tag the management frames sent to the unit with the value of the VLAN ID-Management parameter.

Valid values: 1 to 4094 or 65535 (No VLAN).

The default value is 65535.

If the VLAN ID-Management is other than 65535:

■ Only tagged management frames with a matching VLAN ID received on either the Ethernet or wireless link ports are forwarded to the unit.

■ A VLAN Management Tag is inserted in all management frames generated by the unit before transmission on either the Ethernet or wireless link port. The tag includes the values of the **VLAN ID-Management** and the **VLAN Priority-Management** parameters.

If the VLAN ID-Management is 65535 (No VLAN):

■ Only untagged management frames received on either the Ethernet or wireless link ports are forwarded to the unit.

■ Management frames generated by the unit are not tagged.

The following table summarizes the functionality of the internal management port in accordance with the value of the VLAN ID-Management parameter. The table is valid for all link types. Refer to the VLAN Link Type - Access Link and Trunk Link options for some restrictions when configuring this parameter.

Table 4-5: VLAN Management Port Functionality	
Action	**Management Port - Internal**
Receive from Ethernet	Tagged frames, matching VID-M Untagged frames when VID-M=65535
Receive from Wireless	Tagged frames, matching VID-M Untagged frames when VID-M=65535
Transmit	Insert VID-M, PID-M

Table Legend:

■ **VID-M:** VLAN ID-Management

■ **PID-M:** VLAN Priority-Management

VLAN Link Type

The VLAN Link Type parameter enables defining the functionality of the VLAN aware capability of the unit.

The available options are Hybrid Link, Trunk Link and Access Link (Access Link option is available only in RBs).

The default selection is Hybrid Link.

Access Link (RB only)

Access Link transfers frames while tagging/untagging them since all devices connected to the unit are VLAN unaware. Thus, the unit cannot transfer tagged frames.

Table 4-6 summarizes the functionality of the data port for an Access link.

Table 4-6: VLAN Data Port Functionality - Access Link	
Action	**Data Port - RB**
Receive from Ethernet	Untagged frames
Accept from Wireless	Tagged frames, matching VID-D
Tag Insert	VID-D, PID-D (to wireless)
Tag Remove	Yes (to Ethernet)

Table Legend:

■ VID-D: VLAN ID-Data

■ PID-D: VLAN Priority-Data

Trunk Link

Trunk Link transfers only tagged frames, since all devices connected to the unit are VLAN aware: Only tagged data frames received on the Ethernet or wireless link ports are forwarded.

CAUTION

It is not recommended that you configure a unit as a Trunk Link with the VLAN ID-Management parameter set at 65535, as it does not forward any 'NO VLAN' management frames to its other port making it impossible to manage devices connected behind the unit that are also configured with 'NO VLAN'.

If the VLAN Forwarding option is enabled, a data frame received with a VLAN ID that is not a member of the unit's VLAN Forwarding List is discarded.

NOTE

If the **VLAN Forwarding** option is enabled, be sure to include the **VLAN ID-Management** value of all units that should be managed via the wireless port of the unit, in the Forwarding List.

Table 4-7 summarizes the functionality of the data port for a Trunk link.

Table 4-7: VLAN Data Port Functionality - Trunk Link	
Action	**Data Port – BU and RB**
Accept from Ethernet	Tagged frames. If Forwarding is enabled, only frames with VLAN ID values which are included in the Forwarding list
Accept from Wireless	Tagged frames If Forwarding is enabled, only frames with VLAN ID values which are included in the Forwarding list
Tag Insert	No
Tag Remove	No

Hybrid Link

Hybrid Link transfers both tagged and untagged frames, since the devices connected to the unit can be either VLAN aware or VLAN unaware. This is equivalent to defining no VLAN support, as the unit is transparent to VLAN.

Table 4-8 summarizes the functionality of the data port for a Hybrid link.

Table 4-8: VLAN Data Port Functionality - Hybrid Link	
Action	**Data Port – BU and RB**
Accept from Ethernet	All
Accept from Wireless	All
Tag Insert	No
Tag Remove	No

VLAN Forwarding (BU and RB)

The VLAN Forwarding feature is applicable for Trunk Links only. It enables defining the VLAN ID values to be included in the VLAN Forwarding List. If the Link Type is defined as a Trunk Link and the VLAN Forwarding option is enabled, a data frame received with a VLAN ID that is not a member of the unit's VLAN Forwarding List is discarded.

The VLAN Forwarding submenu provides the following options:

VLAN Forwarding Support

The VLAN Forwarding Support option enables or disables the VLAN Forwarding feature.

Available selections are **Disable** and **Enable**.

The default selection is Disable.

Add Forwarding VLAN ID

The Add Forwarding VLAN ID option enables adding a VLAN ID to the VLAN Forwarding List. One VLAN ID can be entered at a time. The maximum number of VLAN IDs in the VLAN Forwarding List is 20.

Valid values are 1 to 4094.

Remove Forwarding VLAN ID

The Remove Forwarding VLAN ID option enables removing a VLAN ID from the VLAN ID Forwarding List.

Valid values are VID values (from 1 to 4094) that are included in the VLAN Forwarding List.

Show VLAN ID Forwarding List

The Show VLAN Forwarding List option displays the values of the VLAN IDs included in the VLAN Forwarding List.

NOTE
If the VLAN ID Forwarding List is empty and the VLAN Forwarding Support is set to Enable, then all data frames are discarded.

VLAN Traffic Priority

Each packet to be transmitted to the wireless link is transferred to one of three queues: Low, Medium and High. Packets in the High queue have the highest priority for transmission, and those in the Low queue have the lowest priority. The packets in the High queue will be transmitted first. When this queue is emptied, the packets in the Medium queue will be sent. Finally, when both the High and Medium queues are empty, the packets in the Low queue will be sent.

BreezeNET B units support layer-2 traffic prioritization according to the IEEE 802.1p standard. The priority field in the 802.1Q header tag can have a value in the range 0 to 7. This value determines the relative priority of the packet.

Packets received from the Ethernet port that have a priority higher than the value of the VLAN Priority Threshold are routed to the High queue.

Since the system also supports layer 3 prioritization, based on ToS, packets with precedence in the ToS field higher than the value of the ToS Precedence Threshold parameter are also routed to the High queue. This is applicable to both tagged and untagged frames.

MAC broadcasts are routed to the Medium queue. All other packets received from the Ethernet port are routed to the Low queue.

Control and wireless management frames generated in the unit are routed to the High queue.

Any frame coming from the Ethernet port, which is meant to reach the other BreezeNET B unit via the wireless port (as opposed to messages intended for stations behind the BreezeNET B unit), is sent to the High queue, regardless of the priority configuration.

NOTE
The prioritization mechanism is disabled when the traffic rate reaches the maximum information rate supported by the system.

The VLAN Traffic Priority menu includes the following parameters:

■ VLAN Priority – Data (RB only)

■ VLAN Priority – Management

■ VLAN Priority Threshold

VLAN Priority - Data (RB only)

The VLAN Priority - Data is applicable for Access Links only. It enables configuring the value of the VLAN Priority field for data frames transmitted to the wireless link. All data frames are routed to the Low queue. This parameter only impacts the way that other VLAN aware devices handle the packet.

Valid values range from 0 to 7.

The default value is 0.

NOTE
Packets Received from the Ethernet port with a ToS Precedence value higher than the defined **ToS Precedence Threshold** are routed to the Mid queue.

VLAN Priority - Management

The VLAN Priority - Management enables defining the value of the VLAN Priority field for management frames in units with VLAN ID Management that is other than **65535**. All management frames are routed to the High queue. This parameter only impacts the way other VLAN aware devices handle the packet.

Valid values range from 0 to 7.

The default value is 4 for RBs and 0 for BUs.

VLAN Priority Threshold

The VLAN Priority Threshold is applicable for Trunk and Hybrid Links only. It enables defining the value of the VLAN Priority Threshold. This parameter impacts the way the unit handles tagged packets received from the Ethernet port.

Since the system supports both layer 2 and layer 3 prioritization, a frame is routed to the High queue if either of the following conditions are met:

■ The precedence in the ToS field is higher than the value of the ToS Precedence Threshold parameter. This is applicable to both tagged and untagged frames.

■ The VLAN Priority field in a tagged frame is higher than the value of the VLAN Priority Threshold parameter.

Valid values range from 0 to 7.

The default value is 3.

Show VLAN Parameters

The Show VLAN Parameters option displays the current values of the VLAN support parameters.

ToS Parameters

ToS Precedence Threshold

The ToS Precedence Threshold parameter enables defining ToS based prioritization in accordance with the precedence bits of the ToS field in the IP header. An IP packet received from the Ethernet port is routed to the High queue if any one of the following conditions is met:

■ The precedence in the ToS field is higher than the value of the ToS Precedence Threshold parameter. This is applicable to both tagged and untagged frames.

■ The VLAN Priority field in a tagged frame (Hybrid or Trunk Link) is higher than the value of the VLAN Priority Threshold parameter.

All other packets received from the Ethernet port are routed to the Low queue.

Valid values are 0 to 7.

The default value is 3.

> **NOTE**
>
> The prioritization mechanism is disabled when the traffic rate reaches the maximum information rate supported by the system.

Ethernet Broadcast Filtering (RB only)

The Ethernet Broadcast Filtering menu enables defining the layer 2 (Ethernet) broadcast and multicast filtering capabilities for the selected RB. Filtering the Ethernet broadcasts enhances the security of the system and saves bandwidth on the wireless media by blocking protocols that are typically used in the customer's LAN but are not relevant for other customers, such as NetBios, which is used by the Microsoft Network Neighborhood. Enabling this feature blocks Ethernet broadcasts and multicasts by setting the I/G bit at the destination address to 1. This feature should not be enabled when there is a router behind the RB.

The Ethernet Broadcast Filtering menu includes the following parameters:

■ Filter Options

■ DHCP Broadcast Override Filter

■ PPPoE Broadcast Override Filter

■ ARP Broadcast Override Filter

Filter Options

The Filter Options enables defining the Ethernet Broadcast filtering functionality of the unit. Select from the following options:

■ **Disable**, which means no Ethernet Broadcast Filtering.

■ **On Ethernet Port Only**, which filters broadcast messages received from the Ethernet port.

■ **On Wireless Port Only**, which filters broadcast messages received from the wireless link port.

■ **On Both Ethernet and Wireless Ports**, which filters broadcast messages received from both the Ethernet and wireless link ports.

The default selection is Disable.

DHCP Broadcast Override Filter

The DHCP Broadcast Override Filter option enables or disables the broadcasting of DHCP messages. Even if according to the selected option in the Filter Options parameter, broadcast messages should be filtered, DHCP broadcasts are transmitted if this parameter is set to Enable. Select from the following options:

■ **Disable**, which means that DHCP Broadcast messages are filtered or transmitted according to the general filtering criteria in the Filter Options parameter.

■ **Enable**, which means that DHCP Broadcast messages are transmitted regardless of the selected value of the Filter Options parameter.

The default selection is Disable.

PPPoE Broadcast Override Filter

The PPPoE Broadcast Override Filter option enables or disables the broadcasting of PPPoE (Point to Point Protocol over Ethernet) messages. Even if according to the selected option in the Filter Options parameter, broadcast messages should be filtered, PPPoE broadcasts are transmitted if this parameter is set to Enable. Select from the following options:

■ **Disable**, which means that PPPoE Broadcast messages are filtered or transmitted according to the general filtering criteria in the Filter Options parameter.

■ **Enable**, which means that PPPoE Broadcast messages are transmitted regardless of the selected value of the Filter Options parameter.

The default selection is Disable.

ARP Broadcast Override Filter

The ARP Broadcast Override Filter option enables or disables the broadcasting of ARP messages. Even if according to the selected option in the Filter Options parameter, broadcast messages should be filtered, ARP broadcasts are transmitted if this parameter is set to Enable. Select from the following options:

■ **Disable**, which means that ARP messages are filtered or transmitted according to the general filtering criteria in the Filter Options parameter.

■ **Enable**, which means that ARP messages are transmitted regardless of the selected value of the Filter Options parameter.

The default selection is Enable.

Bridge Aging Time

The Bridge Aging Time parameter enables selecting the bridge aging time for learned addresses of devices on both the wired and wireless sides, not including BreezeNET B units.

The available range is 20 to 2000 seconds.

The default value is 300 seconds.

Roaming Option (RB only)

The Roaming Option defines the roaming support of the unit. When roaming is not expected, it is preferable to set this parameter to Disable. This will cause the unit to start scanning for another BU after loosing connectivity with the current BU only after 7 seconds during which no beacons were received from the current BU. This will prevent scanning for another BU in cases where no beacons were received due to a short temporary problem.

When set to Enable, the RB will wait only one second before it starts scanning for another BU. In addition, when the Roaming Option is enabled, the RB will send Roaming SNAP messages upon associating with a new BU. This enables fast distribution of the new location for all clients that are behind the RB. In this case, the RB will send multicast SNAP messages via the wireless link each time it associates with a new BU, except for the first association after reset. The RB will send one SNAP message for each client learned on its Ethernet port, based on its bridging table. In the SNAP message the clients' MAC address is used as the source address. The BU that receives this SNAP message learns from it the new location of the clients. It forwards the SNAP to other BUs and Layer-2 networking equipment via its Ethernet port, to facilitate uninterrupted connectivity and correct routing of transmissions to these clients.
The default is Disable.

Show Bridge Parameters

The Show Bridge Parameters option displays the current values of the Bridge parameters.

Performance Parameters

The Performance Parameters menu enables defining a series of parameters that control the method by which traffic is transmitted through the BreezeNET B wireless link.

The Performance Parameters menu includes the following parameters:

■ Maximum Modulation Level

■ Multicast Modulation Level (BU only)

■ Average SNR Memory Factor

■ Number of HW Retries

■ Burst Mode

■ Adaptive Modulation Algorithm

Maximum Modulation Level

When the Adaptive Modulation Algorithm (see Adaptive Modulation Algorithm on page 4-80) is enabled, it changes the modulation level dynamically according to link conditions. The purpose is to increase the probability of using the maximum possible modulation level at any given moment. Although the algorithm will avoid using modulation levels that are too high for the prevailing link conditions, it might be desired under certain conditions to limit the use of higher modulation levels. If the link quality is not sufficient, it is recommended that the maximum modulation level be decreased, since higher modulation levels increase the error rate. In such conditions, a higher Maximum Modulation Level increases the number or retransmissions before the modulation level is being reduced by the Adaptive Modulation Algorithm. A high number of retransmissions reduces the overall throughput of the link.

The link quality can be estimated based on the SNR measurement of the RB at the BU, which can be viewed in the MAC Address Database option in the Site Survey menu, and on the SNR measurement of the BU at the RB, which can be viewed using the Continuous Link Quality Display option. If the measured SNR is less than a certain threshold, it is recommended that the maximum modulation level be decreased in accordance with Table 4-9, using the values of typical sensitivity. It is recommended to add a 2 dB safety margin to compensate for possible measurement inaccuracy or variance in the link quality.

NOTE

The SNR measurement at the BU is accurate only when receiving transmissions from the applicable RB. If necessary, use the Ping Test utility in the Site Survey menu to verify data transmission.

When the Adaptive Modulation Algorithm is disabled, this parameter will serve to determine Fixed Modulation Level used for transmissions.

The minimum value for the Maximum Modulation Level is defined by the Sub Band in use.

The maximum value for the Maximum Modulation Level is defined by the Sub Band in use.

For information on how to view the Sub Bands supported by the unit and the supported parameters' values and options, refer to Show Country Dependent Parameters on page 4-8.

The default is the highest supported Modulation Level.

Table 4-9: Recommended Maximum Modulation Level*	
SNR	**Maximum Modulation Level**
SNR> 23 dB	8
21 dB < SNR < 23 dB	7
16 dB< SNR < 21 dB	6
13 dB < SNR < 16 dB	5
10 dB < SNR < 13 dB	4
8 dB < SNR < 10 dB	3
7 dB < SNR < 8 dB	2
6 dB<SNR < 7 dB	1

* the maximum supported value depends on the Max Modulation Level according to the Sub Band.

Multicast Modulation Level (BU only)

The Multicast Modulation Level parameter defines the modulation level used for transmitting multicast and broadcast data frames. Multicast and broadcast transmissions are not acknowledged; therefore if a multicast or broadcast transmission is not properly received there is no possibility of retransmitting. It is recommended that you set a lower modulation level for broadcast and multicast frame transmissions to increase the probability that they are received without errors.

The Multicast Modulation Level parameter is applicable only to data frames intended to unknown recipients. Beacons and other wireless management and control frames are always transmitted at the lowest modulation level according to the Sub Band.

The minimum value for the Multicast Modulation Level is defined by the Sub Band in use.

The maximum value for the Multicast Modulation Level is defined by the Sub Band in use.

For information on how to view the Sub Bands supported by the unit and the supported parameters' values and options, refer to Show Country Dependent Parameters on page 4-8.

The default value is the lowest supported modulation level.

Average SNR Memory Factor

The Average SNR Memory Factor defines the weight of history (value of last calculated average SNR) in the formula used for calculating the current average SNR for received data frames. This average SNR is used by the ATPC algorithm in the BU and is also included in the Adaptive Modulation Algorithm information messages transmitted by the BU and the RB. The higher the value of this parameter, the higher is the weight of history in the formula.

Available values: -1 to 32. -1 is for no weight for history, meaning that average SNR equals the last measured SNR.

Default value: 5

Number of HW Retries

The Number of HW Retries parameter defines the maximum number of times that an unacknowledged packet is retransmitted. When the Adaptive Modulation Algorithm is disabled a frame will be dropped when the number of unsuccessful retransmissions reaches this value. For details on the effect of this parameter when the Adaptive Modulation Algorithm is enabled, refer to Adaptive Modulation Algorithm, on page 4-80.

The available values range is from 1 to 15.

The default value is 10.

Burst Mode

Burst mode provides an increased throughput by reducing the overhead associated with transmissions in the wireless media. In a burst transmission the inter-frame spacing is reduced and data frames are transmitted without any contention period.

The Burst Mode is available only if Burst Mode is supported by the Sub Band in use. For information on how to view the Sub Bands supported by the unit and the supported parameters' values and options, refer to Show Country Dependent Parameters on page 4-8.

In BUs with HW Revision B, Burst Mode cannot be activated when the DFS option is used. In BUs with HW Revision B, the Burst Mode option will be "blocked" upon trying to enable Burst Mode when the DFS Option is enabled. This limitation does not apply to BUs with HW Revision C.

In RBs and BUs with HW Revision B, Burst Mode cannot be activated when using WEP for data encryption. In units with HW Revision B, the Burst Mode option will be "blocked" upon trying to enable it when using WEP for data encryption. This limitation does not apply to units with HW Revision C.

Burst Mode Option

The Burst Mode Option enables or disables the Burst Mode operation.

The default is Enable.

Burst Mode Time Interval

The Burst Mode Time Interval defines the burst size, which is the time in which data frames are sent immediately without contending for the wireless medium.

The range is 1 to to the value of the Maximum Burst Duration defined for the Sub Band.

The default is 5 milliseconds or the value of Maximum Burst Duration defined for the Sub Band (the lower of the two values).

Adaptive Modulation Algorithm (Multi Rate)

The Adaptive Modulation Algorithm enables adapting the modulation level of transmitted data to the prevailing conditions of the applicable radio link.

Link quality fluctuates due to various environmental conditions. Dynamically switching between the possible modulation levels increases the probability of using the maximum modulation level suitable for the current radio link quality at any given moment.

The decisions made by the Adaptive Modulation Algorithm for the modulation level to be used are based on multiple parameters, including information on received signal quality (SNR) that is received periodically from the destination unit, the time that has passed since last transmission to the relevant unit, and the recent history of successful and unsuccessful transmissions/retransmissions.

The transmission/retransmission mechanism operates as follows:

A. Each new frame (first transmission attempt) will be transmitted at a modulation level selected by the Adaptive Modulation algorithm.

B. If first transmission trial has failed, the frame will be retransmitted at the same modulation level up to the maximum number of retransmission attempts defined by the Number of HW Retries parameter.

The Adaptive Modulation menu includes the following parameters:

Adaptive Modulation Option

The Adaptive Modulation Option enables or disables the Adaptive Modulation decision algorithm. When enabled, the algorithm supports decrease/increase of transmission's modulation levels between the lowest possible level to the value configured for the Maximum Modulation Level parameter. If the Maximum Modulation Level is set at the lowest possible level, the Adaptive Modulation algorithm has no effect.

The default selection is Enable.

Minimum Interval Between Adaptive Modulation Messages

The Minimum Interval Between Adaptive Modulation Messages sets the minimum interval between two consecutive adaptive modulation messages, carrying information on the SNR of received signals.

The available range is from 1 to 3600 seconds.

The default is 4 seconds.

Adaptive Modulation Decision Thresholds

Enables selection between Normal and High decision thresholds for the Adaptive Modulation algorithm. In links with a low SNR (below 13), the Adaptive Modulation algorithm may not stabilize on the correct modulation level when using the standard decision thresholds. In this case the algorithm may try to use a modulation level that is too high, resulting in a relatively large number of dropped frames. The "High" option solves this limitation and ensures good performance also in links with a low SNR.

The default is Normal.

Concatenation Parameters

The Concatenation mechanism enables bundling two data frames into a single frame for transmission to the wireless link. This feature improves throughput and reduces the overhead in the wireless media, by reducing the overhead associated with each transmission. When concatenation is enabled, data packets in the queue of the internal bridge can be accumulated before the concatenated frame is transmitted to the wireless media. Two data frames can be accumulated, up to a maximum of 2200 bytes.

A frame is a candidate for bundling into a concatenated frame if all the following conditions are met:

■ The frame is a data frame

■ The destination is an entity behind the destination BU/RB.

■ The destination AU/SU can support the feature (uses SW version 3.0 or higher).

Once a frame is identified as an eligible candidate for concatenation, it is marked accordingly and will be processed according to the following:

■ If there is no other candidate frame designated to the same destination unit in the queue:

> ➢ If the hardware queue is empty – the frame is transmitted immediately.

> ➢ Otherwise (the queue is not empty) – the frame is inserted to the queue.

■ If a candidate frame designated to the same destination unit exists in the queue, it is taken out from the queue:

> ➢ If the combined length of both frames is above the maximum allowed concatenated frame length – both frames are transmitted as two separate frames.

> ➢ Otherwise (the combined frames length is bellow the maximum length) - A concatenated frame is built as a bundle of the two frames and transmitted to the wireless media.

NOTE

Once a frame is marked as a candidate for concatenation, it will be transmitted as a concatenated frame. If it is bundled with another data frame, it will be a concatenated frame with a single data frame (Concatenated Frame Single). If it is bundled with another data frame, it will be a concatenated frame with double data frames (Concatenated Frame Single).

The Concatenation Parameters submenu includes a single option:

Concatenation Option

The Concatenation Option enables or disables the concatenation mechanism.

The default is Enable.

Service Parameters (RB only)

The Service Parameters menu enables defining user filtering and MIR parameters.

The Service Parameters menu is only available to RBs and includes the following parameters:

■ User Filtering Parameters

■ MIR Parameters

User Filtering Parameters

The User Filtering Parameters submenu enables defining the IP addresses of user devices authorized to access the wireless media for security and/or control purposes. In addition, it can be used to enable the transmission and reception of specific protocol frames. These filtering options do not affect management frames sent to or generated by the unit.

The User Filtering Parameters menu provides the following options:

User Filtering Option

The User Filtering Option disables or enables the User Filtering feature. The following options are available:

■ **Disable**, which means no filtering.

■ **IP Protocol Only**, which means only IP Protocol packets pass.

■ **User Defined Addresses Only**, which means only IP frames from/to IP addresses included in the User Filter Addresses list pass.

■ **PPPoE Protocol Only**, which means only PPPoE messages pass (Ethernet type 0x8863 and 0x8864).

The default selection is Disable.

Set User Filter Address

The Set User Filter Address option enables entering up to 8 IP addresses from/to which IP frames are to pass if the User Defined Addresses Only option is selected in the User Filtering Option parameter.

The default for all addresses is 0.0.0.0.

Set User Filter Mask

The Set User Filtering Mask option enables entering subnet masks for each of the User Filter IP Address entries.

The default for all subnet masks is 255.255.255.255.

Set User Filter Range

The Set User Filter Range option enables defining a range of addresses for each of the User Filter IP Address entries. The range includes the base address.

Available values range from 0 to 255.

The default value is 0 (not used).

> **NOTE**
>
> Use either a mask or range, but not both, to define a group of user filter addresses. If the range is other than 0, than the mask is ignored.
>
> If IP broadcast packets are supposed to reach a device behind an RB unit, the broadcast IP address must be included in the list of user filter addresses.

Delete a User Filtering Entry

The Delete a User Filtering Entry option enables deleting a selected entry from the User Filtering list. The entry is replaced by the default value.

Delete all User Filtering Entries

The Delete All User Filtering Entries option enables deleting all entries from the User Filtering list. The list entries are replaced by the default values.

DHCP Unicast Override Filter

When user filtering is activated, unicast DHCP messages are filtered out; therefore the unit cannot communicate with the DHCP server. The DHCP Unicast Override Filter option enables to overcome this problem. When enabled, unicast DHCP messages pass, overriding the user filtering mechanism.

The default is Disable DHCP Unicast.

Show User Filtering Parameters

The Show All User Filtering Parameters option displays the current value of the User Filtering Option and the list of User Filtering addresses, subnet masks and ranges.

MIR Parameters

The MIR (Maximum Information Rate) value specifies the maximum data rate available for burst transmissions, enabling to limit it to a value lower than the maximum supported by the unit. The MIR values indicate the achievable net throughput for FTP applications.

MIR: Downlink

Sets the Maximum Information Rate of the downlink from the BU to the RB.

Available values range from 128 to 6912 Kbps for RB-14 and from 128 to 22016 Kbps for RB-28.

The actual value will be the entered value rounded to the nearest multiple of 128 (N*128).

The default value is 6912 Kbps for RB-14 and 22016 Kbps for RB-28.

MIR: Uplink

Sets the Maximum Information Rate of the uplink from the RB to the BU.

Available values range from 128 to 6912 Kbps for RB-14 and from 128 to 22016 Kbps for RB-28.

The actual value will be the entered value rounded to the nearest multiple of 128 (N*128).

The default value is 6912 Kbps for RB-14 and 22016 Kbps for RB-28.

NOTE

An asymmetrical link can be achieved using an RB-28 and a BU-14. In such a link the maximum downlink (BU to RB) rate is determined by the BU (max. 7 Mbps), and the maximum uplink (RB to BU) rate is determined by the RB (max 22 Mbps).

Show MIR Parameters

Displays the current values of the MIR parameters.

Show Service Parameters

Displays the current values of the Service Parameters, including the user filtering parameters and MIR parameters.

Security Parameters

BreezeNET B can support encryption of authentication messages and/or data frames using one of two encryption standards:

■ **WEP** Wireless Equivalent Privacy algorithm. WEP is defined in the IEEE 802.11 Wireless LAN standard and is based on the RSA's RC4 encryption algorithm.

■ **AES** Advanced Encryption Standard. AES is defined by the National Institute of Standards and Technology (NIST) and is based on Rijndael block cipher.

The following parameters are available through the Security Parameters menu (in certain units some or all of the security options may not be available):

■ Authentication Algorithm

■ Data Encryption Option

■ Security Mode

■ Default Key (RB only)

■ Default Multicast Key (BU only)

■ Key # 1 to Key # 4

■ Promiscuous Authentication (BU only)

Authentication Algorithm

The Authentication Algorithm option determines the operation mode of the selected unit. The two following options are available:

■ **Open System**: An RB configured to Open System can only associate with a BU also configured to Open System. In this case, the authentication encryption algorithm is not used.

■ **Shared Key**: The authentication messages are encrypted. An RB configured to use a Shared Key can only be authenticated by a BU configured to use a Shared Key, provided the applicable Key (which means both the key number and its content) in the BU is identical to the key selected as the Default Key in the RB.

The default is Open System.

The Shared Key option cannot be selected before at least one Key is defined. In the RB, a Default Key that refers to a valid Key must be selected.

The BU and the RB it serves should be configured to the same Authentication Algorithm option.

Data Encryption Option

The Data Encryption Option allows enabling or disabling data encryption. When enabled, all data frames are encrypted.

The default is Disable.

NOTE

The BU and the RB it serves should be configured to the same Data Encryption Option.

Security Mode

The Security Mode option enables selecting the algorithm to be used for encrypting the authentication messages and/or data frames.

The available options are WEP and AES.

The default is WEP.

NOTE

The BU and the RB it serves should be configured to the same Security Mode option.

Default Key (RB only):

The Default Key defines the Key to be used for encrypting/decrypting the authentication messages (Shared Key mode) and/or data frames (Data Encryption enabled). The BU learns the Default Key from the RB.

Available values range from 1 to 4.

The default is KEY # 1.

Default Multicast Key (BU only):

The Multicast Default Key defines the Key to be used for encrypting/decrypting multicasts and broadcasts when Data Encryption is enabled.

Available values range from 1 to 4.

The default is KEY # 1.

Key # 1 to Key # 4

The Key # options enables defining the encryption key to be used for initializing the pseudo-random number generator that forms a part of the encryption/decryption process. The Keys must be set before the Shared Key authentication algorithm or Data Encryption can be used. To support proper operation, both the Key # and the content must be identical at both sides of a wireless link.

Each Key is a string of 32 hexadecimal numbers. For security reasons, it is a "write only" parameter, displayed as a string of asterisks ("*").

The default for all 4 Keys is 000...0 (a string of 32 zeros), which means no key.

Promiscuous Authentication (BU only)

The Promiscuous Authentication mode enables a new RB to become associated with a BU where Shared Key operation and/or Data Encryption is used, even if this RB does not have the correct security parameters. After the RB is associated it should be remotely configured with the proper parameters (or upgraded). Once the RB is configured properly, the Promiscuous Mode should be disabled.

The default is Disable.

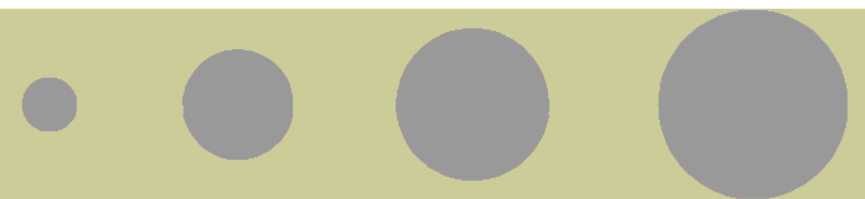| NOTE	
	Do not leave the BU in the mode of Promiscuous Authentication enabled for prolonged periods. Use it only when absolutely necessary, perform the required actions as quickly as possible and disable it. The unit will return automatically to Promiscuous Authentication disabled mode after reset.

This page left intentionally blank.

A

Appendix A - Software Version Loading Using TFTP

Firmware upgrades to the unit's FLASH memory can be performed by a simple loading procedure using a TFTP application. Before performing an upgrade procedure, be sure you have the correct files and most recent instructions.

Upgrade packages can be obtained from the Technical Support section of Alvarion's web site, http://www.alvarion.com/.

CAUTION

Shutting down power to the unit before completion of the loading procedure may cause the unit to be inoperable.

To load software versions:

1. Verify that IP connectivity to the required unit is established.

2. Ensure that the IP address of the PC from which the upgrade is to be performed belongs to the same subnet as the unit to be upgraded, unless the unit is behind a router. If the unit is behind a router, verify that the unit is configured with the correct **Default Gateway Address**.

3. To view the current IP parameters of the unit, use the Monitor program by connecting the PC to the unit either directly or via Telnet. To access the IP parameters via the Monitor program:

   A. From the *Main Menu* select **1 - Info Screens**.

   B. From the *Info Screen* menu select **2 - Show Basic Configuration**. The current basic configuration is displayed, including the run time values for the IP Address, Subnet Mask and Default Gateway Address parameters.

4. To modify any of the IP parameters:

   A. From the *Main Menu*, select **3 - Basic Configuration**.

   B. To configure the IP address, select: **1 - IP Address**.

   C. To configure the subnet mask, select **2 - Subnet Mask**.

   D. To configure the default gateway address, select **3 - Default Gateway Address**.

5. To verify the connection, PING the unit's IP address and verify that PING replies are being received.

6. Use the TFTP utility, with the following syntax, to perform the upgrade:

tftp -i hostaddress put sourcefile [destinationfile]

where *-i* is for binary mode and *hostaddress* is the IP address of the unit to be upgraded. *put* causes the PC client to send a file to the *hostaddress.*

7. The original *sourcefile* name of SW files supplied by Alvarion is in the structure uX_Y_Z.bz, where u is the unit type (a for BU, s for RB) and X.Y.Z is the version number.

8. destinationfile is the name of the file to be loaded. Use the SNMP write community <SnmpWriteCommunity>.bz to define the destination filename. The default SNMP write community is private. For example, to load the upgrade file a1_1_4.bz to a BU whose IP address is *206.25.63.65: tftp -i 206.25.63.65 put a1_1_4.bz private.bz*

9. When the loading is complete, the following message is displayed, indicating completion of the TFTP process:

    ```
    Download operation has been completed successfully
    ```

10. The unit decompresses the loaded file and checks the integrity of the new version. The new version replaces the previous shadow version only after verification. If verification tests fail, the loaded version will be rejected. Among other things that are tested, the unit will reject a file if either the file name or the version number matches either the current Main or Shadow versions. The unit will also reject a file designated for a different unit type, e.g. a BU upgrade file with the prefix a in the original file name will not be accepted by RBs.

11. The FLASH memory can store two software versions. One version is called Current and the second version is called *Shadow.* The new version is loaded into the Shadow (backup) FLASH memory. To check that the new firmware was properly downloaded and verified, view the firmware versions stored in the FLASH, as follows:

    A. From the Main Menu, select **2 - Unit Control**.

    B. From the Unit Control menu, select **5 - Flash Memory Control**.

    C. From the *Flash Memory Control* menu, select **S - Show Flash Versions**. The following information is displayed:

```
Flash Versions
============
Running from                :Main Version
Main Version File Name       :1_1_3.bz
Main Version Number          :1.1.3
Shadow Version File Name      :1_1_4.bz
File Name Number             :1.1.4
```

B

Appendix B - File Download and Upload Using TFTP

The BreezeNET B File Download/Upload feature simplifies the task of remotely configuring a large number of units using TFTP protocol. By downloading the configuration file to a PC it is possible to view all the parameters configured for the unit, as a plain ASCII text file. It is necessary to edit the file using a simple editor and remove certain parameters or change their values prior to uploading the configuration to another unit. The file loading procedure can also be used for uploading a feature license file or an updated country code file to multiple units.

When multiple configurations are being done simultaneously, which means that the file is being uploaded to several units, it is recommended that the file will include only the required parameters.

In the configuration file, the following three fields represent each parameter:

1. A symbolic string similar to the name of the parameter in the Monitor program, followed by "=".

2. The value of the parameters, which uses the same values as the Monitor program.

3. An optional comment. If used, the comment should start with a ";" character.

An unknown parameter will be ignored. A known parameter with a value that is invalid or out of range will be set by the unit to its default value.

Use the SNMP write community string (the default is "private") to define both the uploaded file (put) and the downloaded file (get). The file should be transferred in ASCII mode.

Use the extension .cfg for a configuration file.

Use the extension .cmr for the Operator Defaults file.

Use the extension .fln for a Feature License file.

Use the extension .ccf for a Country Code file.

Feature license and country code files include multiple strings, where each string is applicable only for a certain unit identified by its MAC address. When uploading a feature license or a country code file to multiple units, each unit will accept only the parts that are applicable for itself.

Examples:

1. To upload the configuration file using a DOS based TFTP Client to an RB whose IP address is 206.25.63.65, enter:
   tftp 206.25.63.65 put Suconf private.cfg

2. To download the Operator Defaults file from the same unit, enter:
   tftp 206.25.63.65 get private.cmr Suconf

3. To upload the Feature Upgrade file to the same unit, enter:
   tftp 206.25.63.65 put private.fln Suconf

4. To upload the Country Code file from to same unit, enter:
   tftp 206.25.63.65 put private.ccf Suconf

NOTE

The Configuration File Loading mechanism is common to BreezeACCESS VL and BreezeNET B product lines. The Configuration File includes also parameters that are applicable only to BreezeACCESS VL products: Maximum Number of Associations, Maximum Multicast Rate, AIFS, RTS Threshold, Minimum Contention Window, Maximum Contention Window, VLAN Relaying Support, VLAN Relaying IDs, Broadcast Relaying, Unicast Relaying, Default Multicast Key. Do not attempt to change the default values of these parameters.

This page left intentionally blank.

C

Appendix C - Using the Set Factory Defaults Utility

The Set Factory Defaults Utility is intended to enable management access to a unit in cases where such access is not possible due to wrong or unknown configuration of certain parameters. This includes cases such as unknown Management VLAN ID and wrong management access filtering.
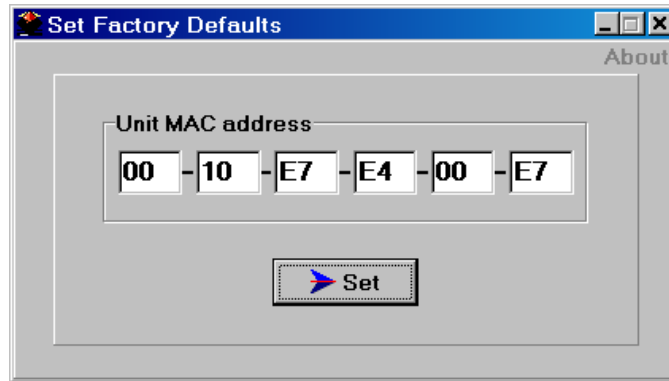
The utility accesses the unit by sending a special packet. Access to the unit is based on its MAC address, which must be entered in the **Unit MAC address** field.

The set unit defaults feature is only available via the Ethernet port.

To set factory defaults:

1. Connect the PC with the Set Factory Defaults utility to the Ethernet port of the unit.

2. Enter the unit's MAC address.

3. Click on the **Set** button.

This utility performs the same operation as Set Complete Factory Defaults, restoring the default factory configuration of all parameters, except to Passwords, general FTP parameters and BU's Frequency.
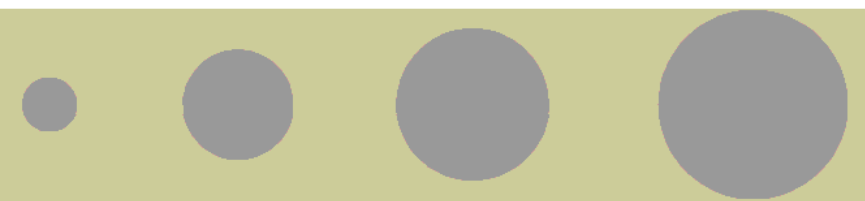
D

Appendix D - Preparing the Indoor to Outdoor Cable

The Indoor-to-Outdoor cable provides pin-to-pin connection on both ends.

Figure D-1 shows the wire pair connections required for the Indoor-to-Outdoor cable.
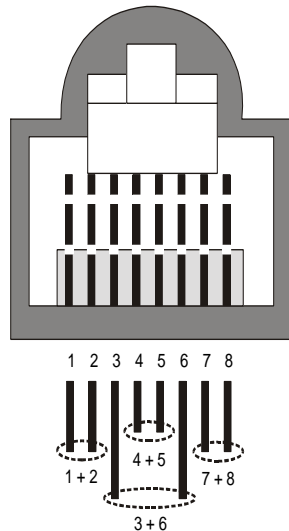
Figure D-1: Ethernet Connector Pin Assignments

The color codes used in cables that are supplied by Alvarion with crimped connectors are as listed in the following table:

Table D-1: Cable Color Codes	
Wire color	**Pin**
Blue	1
Blue/white	2
Orange	3
Orange/white	6
Brown	4
Brown/white	5
Green	7
Green/white	8

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

1. Remove as small a length as possible of the external jacket. Verify that the external jacket is well inside the service box to ensure good sealing.

2. Take back the shield drain wire before inserting the cable into the RJ-45 connector, to ensure a good connection with the connector's shield after crimping.

This page left intentionally blank.

E

Appendix E - Parameters Summary

In this Appendix:

- The tables provide an at a glance summary of the configurable parameters, value ranges, and default values. In addition, each parameter entry also includes an indication as to whether the parameter is updated in run-time or whether the unit must be reset before the modification takes effect.

Parameters Summary

Unit Control Parameters

<table>
<tr><td colspan="5">Table E-1: Unit Control Parameters</td></tr>
<tr><td>Parameter</td><td>Unit</td><td>Range</td><td>Default</td><td>Run-Time</td></tr>
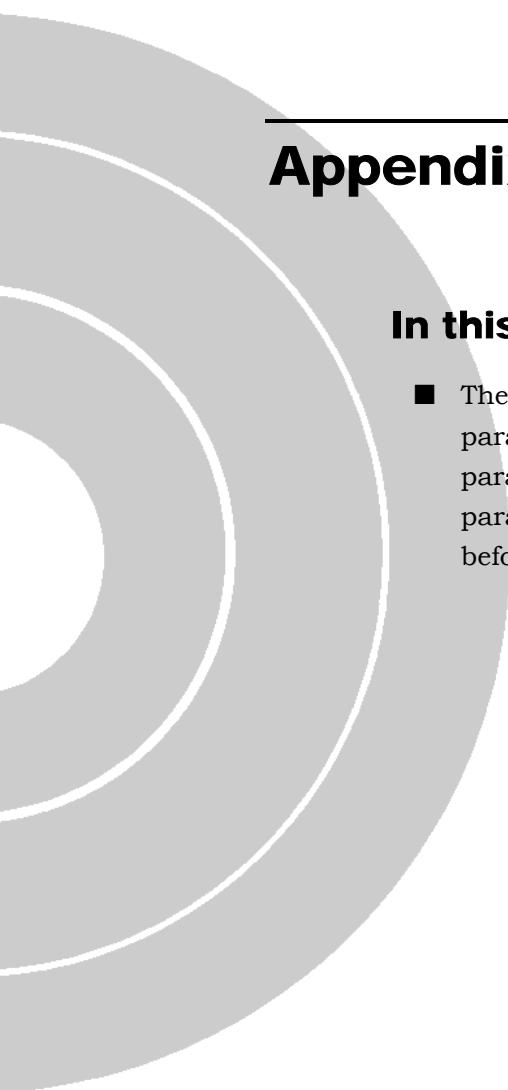<tr><td>Change Unit Name</td><td>BU, RB</td><td>Up to 32 printable ASCII characters</td><td>None</td><td>Yes</td></tr>
<tr><td>Change Read Only Password</td><td>BU, RB</td><td>Up to 8 printable ASCII characters</td><td>public</td><td>No</td></tr>
<tr><td>Change Installer Password</td><td>BU, RB</td><td>Up to 8 printable ASCII characters</td><td>user</td><td>No</td></tr>
<tr><td>Change Administrator Password</td><td>BU, RB</td><td>Up to 8 printable ASCII characters</td><td>private</td><td>No</td></tr>
<tr><td>FTP SW Version File Name</td><td>BU, RB</td><td>Up to 20 printable ASCII characters. An empty string is not allowed.</td><td>VxWorks.bz</td><td>Yes</td></tr>
<tr><td>Configuration File Name</td><td>BU, RB</td><td>Up to 20 printable ASCII characters. An empty string is not allowed.</td><td>config.cfg</td><td>Yes</td></tr>
<tr><td>Operator Defaults File Name</td><td>BU, RB</td><td>Up to 20 printable ASCII characters. An empty string is not allowed.</td><td>operator.cmr</td><td>Yes</td></tr>
<tr><td>FTP Source Dir</td><td>BU, RB</td><td>Up to 80 printable ASCII characters. Use "." to clear.</td><td>None (empty)</td><td>Yes</td></tr>
<tr><td>FTP Client IP Address</td><td>BU, RB</td><td>IP address</td><td>1.1.1.3</td><td>No</td></tr>
<tr><td>FTP Client IP Mask</td><td>BU, RB</td><td>IP address</td><td>255.255.255.0</td><td>No</td></tr>
<tr><td>FTP Server IP Address</td><td>BU, RB</td><td>IP address</td><td>1.1.1.4</td><td>No</td></tr>
<tr><td>FTP Gateway IP Address</td><td>BU, RB</td><td>IP address</td><td>None (empty)</td><td>No</td></tr>
<tr><td>FTP User Name</td><td>BU, RB</td><td>Up to 18 printable ASCII characters</td><td>vx</td><td>No</td></tr>
<tr><td>FTP Password</td><td>BU, RB</td><td>Up to 18 printable ASCII characters</td><td>Vx</td><td>No</td></tr>
<tr><td>FTP Log File Name</td><td>BU, RB</td><td>Up to 20 printable ASCII characters</td><td>logfile.log</td><td>Yes</td></tr>
<tr><td>FTP Log File Destination Directory</td><td>BU, RB</td><td>Up to 80 printable ASCII characters. Use "." to clear.</td><td>None (empty)</td><td>Yes</td></tr>
<tr><td>Event Log Policy</td><td>BU, RB</td><td>Message
Warning
Error
Fatal
Log None</td><td>Warning</td><td>Yes</td></tr>
<tr><td>Log Out Timer</td><td>BU, RB</td><td>1-999 minutes</td><td>5</td><td>Yes</td></tr>
</table>

Table E-1: Unit Control Parameters				
Parameter	**Unit**	**Range**	**Default**	**Run-Time**
Ethernet Port Negotiation Mode	BU, RB	■ Force 10 Mbps and Half-Duplex ■ Force 10 Mbps and Full-Duplex ■ Force 100 Mbps and Half-Duplex ■ Force 100 Mbps and Full-Duplex ■ Auto Negotiation	Auto Negotiation	No
Change System Location	BU, RB	Up to 34 printable ASCII characters	None	Yes
Manual Feature Upgrade	BU, RB	License string: 32 to 64 hexadecimal digits	None	No

IP Parameters

<table>
<tr><td colspan="6">Table E-2: IP Parameters</td></tr>
<tr><th>Parameter</th><th>Unit</th><th>Range</th><th>Default</th><th>Run-Time</th></tr>
<tr><td>IP Address</td><td>BU, RB</td><td>IP address</td><td>10.0.0.1</td><td>No</td></tr>
<tr><td>Subnet Mask</td><td>BU, RB</td><td>IP address</td><td>255.0.0.0</td><td>No</td></tr>
<tr><td>Default Gateway Address</td><td>BU, RB</td><td>IP address</td><td>0.0.0.0</td><td>No</td></tr>
<tr><td>DHCP Option</td><td>BU, RB</td><td>■   Disable

■   DHCP Only

■   Automatic</td><td>Disable</td><td>No</td></tr>
<tr><td>Access to DHCP</td><td>BU, RB</td><td>■   From Wireless Only

■   From Ethernet Only

■   From Both Wireless and Ethernet</td><td>BU: From Ethernet Only

RB: From Wireless Only</td><td>No</td></tr>
</table>

Air Interface Parameters

		Table E-3: Air Interface Parameters		
Parameter	**Unit**	**Range**	**Default**	**Run-Time**
ESSID	BU, RB	Up to 31 printable ASCII characters	ESSID1	No
Operator ESSID Option	BU	■ Disable ■ Enable	Enable	No
Operator ESSID	BU	Up to 31 printable ASCII characters	ESSID1	No
Best BU Support	RB	■ Disable ■ Enable	Disable	No
Number of Scanning Attempts	RB	1 – 255	4	No
Preferred BU MAC Address	RB	MAC Address	00-00-00-00-00-00 (no preferred BU)	Yes
Scanning Mode	RB	Passive, Active	Passive	No
Wireless Link Trap Threshold	BU	1-100 (%)	30 (%)	Yes
Sub Band Select*	BU, RB	According to the Country Code	1	No
Frequency	BU	According to the Sub Band	The lowest frequency in the Sub Band	No
DFS Option**	BU	■ Disable ■ Enable	Dependent on Country DFS Support: If DFS is supported by the country code then the default will be Enable, else it will be Disable.	No
Frequency Subset Definition (in BU)**	BU	According to the Sub Band. A list of frequency indexes or A for all frequencies supported by the Sub Band	A (All)	No
Frequency Subset Definition (in RB)	RB	According to the Sub Band. A list of frequency indexes or A for all frequencies supported by the Sub Band	A (All)	No
Channel Check Time**	BU	1 – 3600 (seconds)	60 (seconds)	No
Channel Avoidance Period**	BU	1 – 60 (minutes)	30 (minutes)	No
SU Waiting Option**	BU	■ Disable ■ Enable	Enable	No

Table E-3: Air Interface Parameters				
Parameter	**Unit**	**Range**	**Default**	**Run-Time**
Minimum Pulses to Detect**	BU	1-100	6	No
Clear radar Detected Channels After Reset**	BU	■ Disable ■ Enable	Disable	Yes
Channel Reuse Option**	AU	■ Disable ■ Enable	Disable	No
Radar Activity Assessment Period**	AU	1 – 12 hours	5 hours	No
Maximum Number of Detections in Assessment Period**	AU	1 – 10 detections	5 detections	No
Tx Power For Modulation Levels 1 to 5	BU, RB	-10 dBm to a value determined by the HW, Country Code and other parameters	The highest allowed value	Yes
Tx Power For Modulation Level 6	BU, RB	-10 dBm to a value determined by the HW, Country Code and other parameters	The highest allowed value	Yes
Tx Power For Modulation Level 7	BU, RB	-10 dBm to a value determined by the HW, Country Code and other parameters	The highest allowed value	Yes
Tx Power For Modulation Level 8	BU, RB	-10 dBm to a value determined by the HW, Country Code and other parameters	The highest allowed value	Yes
Max Tx Power For Modulation Levels 1 to 5	RB	-10 dBm to a value determined by the HW, Country Code and other parameters	The highest allowed value	Yes
Max Tx Power For Modulation Level 6	RB	-10 dBm to a value determined by the HW, Country Code and other parameters	The highest allowed value	Yes
Max Tx Power For Modulation Level 7	RB	-10 dBm to a value determined by the HW, Country Code and other parameters	The highest allowed value	Yes
Max Tx Power For Modulation Level 8	RB	-10 dBm to a value determined by the HW, Country Code and other parameters	The highest allowed value	Yes
ATPC Option	BU, RB	■ Disable ■ Enable	Enable	Yes
Delta from Minimum SNR Level	BU	4-20 (dB)	Units in 5.4 or 5.8 GHz bands: 5 Units in 5.2 or 5.3 GHz bands: 11	Yes
Minimum SNR Level	BU	4-60 (dB)	28 (dB)	Yes

Table E-3: Air Interface Parameters				
Parameter	**Unit**	**Range**	**Default**	**Run-Time**
Minimum Interval Between ATPC Messages	BU	1-3600 (seconds)	30 (seconds)	Yes
ATPC Power Level Steps	BU	1-20 (dB)	4	Yes
Link Distance Mode	BU	Automatic, Manual	Automatic	No
Maximum Link Distance	BU	0-54 (Km) 0 means no compensation	0 (no compensation)	Yes
Tx Control	BU	■ Off ■ On	On	Yes (unit is reset automatically)
Antenna Gain***	BU, RB	0 – 50 (dB)	"Don't Care" or "Not Set Yet" or 21 (depending on unit type and regulations)	No
Spectrum Analysis Channel Scan Period	BU, RB	2 – 30 seconds	5 seconds	No
Spectrum Analysis Scan Cycles	BU, RB	1 – 100 cycles	2 cycles	No
Automatic Channel Selection	BU	■ Disable ■ Enable	Disable	No (Configured per analysis)

* Not applicable if only one Sub Band is available for the applicable Country Code

** Applicable only if DFS is supported by the Sub Band

*** Configurable only in units without an integral antenna.

Network Management Parameters

<table>
<tr><td colspan="5" align="center">Table E-4: Network Management Parameters</td></tr>
<tr><td>Parameter</td><td>Unit</td><td>Range</td><td>Default</td><td>Run-Time</td></tr>
<tr>
<td>Access to Network Management</td>
<td>BU, RB</td>
<td>■ From Wireless Link Only

■ From Ethernet Only

■ From Both Ethernet and Wireless Link</td>
<td>From Both Ethernet and Wireless Link</td>
<td>No</td>
</tr>
<tr>
<td>Network Management Filtering</td>
<td>BU, RB</td>
<td>■ Disable

■ Activate Management IP Filter On Ethernet Port

■ Activate Management IP Filter On Wireless Port

■ Activate Management IP Filter On Both Ethernet and Wireless Ports</td>
<td>Disable</td>
<td>No</td>
</tr>
<tr>
<td>Set Network Management IP Address</td>
<td>BU, RB</td>
<td>IP address</td>
<td>0.0.0.0 (all 10 entries)</td>
<td>No</td>
</tr>
<tr>
<td>Send SNMP Traps</td>
<td>BU, RB</td>
<td>■ Disable

■ Enable</td>
<td>Disable</td>
<td>Yes</td>
</tr>
<tr>
<td>SNPM Traps IP Destination</td>
<td>BU, RB</td>
<td>IP address</td>
<td>0.0.0.0 (all 10 entries)</td>
<td>No</td>
</tr>
<tr>
<td>SNMP Traps Community</td>
<td>BU, RB</td>
<td>Up to 14 printable ASCII characters</td>
<td>public (all 10 entries)</td>
<td>No</td>
</tr>
</table>

Bridge Parameters

Table E-5: Bridge Parameters				
Parameter	**Unit**	**Range**	**Default**	**Run-Time**
VLAN ID-Data	RB	1 – 4094	1	No
VLAN ID – Management	BU, RB	1 – 4094, 65535	65535 (no VLAN)	No
VLAN Link Type	BU, RB	■ Hybrid Link ■ Trunk Link ■ Access Link (only in RB)	Hybrid Link	No
VLAN Forwarding Support	BU, RB	Disable, Enable	Disable	No
VLAN Forwarding ID	BU, RB	1 – 4094 (up to 20 entries)	Empty list	No
VLAN Priority – Data	RB	0 – 7	0	No
VLAN Priority – Management	BU, RB	0 – 7	0	No
VLAN Priority Threshold	BU, RB	0 – 7	3	Yes
ToS Precedence Threshold	BU, RB	0 – 7	3	Yes
Bridge Aging Time	BU, RB	20 – 2000 seconds	300	No
Ethernet Broadcast Filtering Options	RB	■ Disable, ■ On Ethernet Port Only ■ On Wireless Port Only ■ On Both Wireless and Ethernet Ports	Disable	Yes
DHCP Broadcast Override Filter	RB	■ Disable ■ Enable	Disable	Yes
PPPoE Broadcast Override Filter	RB	■ Disable ■ Enable	Disable	Yes
ARP Broadcast Override Filter	RB	■ Disable ■ Enable	Enable	Yes
Roaming Option`	SU	■ Disable ■ Enable	Disable	No

Performance Parameters

<table>
<tr><td colspan="5">Table E-6: Performance Parameters</td></tr>
<tr><td>Parameter</td><td>Unit</td><td>Range</td><td>Default</td><td>Run-Time</td></tr>
<tr><td>Maximum Modulation Level</td><td>BU, RB</td><td>According to the Min/Max Modulation Level defined for the Sub Band</td><td>The highest available value</td><td>Yes</td></tr>
<tr><td>Multicast Modulation Level</td><td>BU</td><td>According to the Min/Max Modulation Level defined for the Sub Band</td><td>The lowest available value</td><td>Yes</td></tr>
<tr><td>Number of HW Retries</td><td>BU, RB</td><td>1 - 15</td><td>10</td><td>Yes</td></tr>
<tr><td>Average SNR Memory Factor</td><td>BU, RB</td><td>-1 to 32</td><td>5</td><td>Yes</td></tr>
<tr><td>Burst Mode Option*</td><td>BU, RB</td><td>■   Disable

■   Enable</td><td>Enable (If Burst Mode is supported by the Sub Band)</td><td>No</td></tr>
<tr><td>Burst Mode Time Interval*</td><td>BU, RB</td><td>1 to the value defined in the Sub Band for Maximum Burst Duration (milliseconds)</td><td>5 milliseconds or the value of Maximum Burst Duration defined for the Sub Band (the lower of the two values).</td><td>Yes</td></tr>
<tr><td>Adaptive Modulation Option</td><td>BU, RB</td><td>■   Disable

■   Enable</td><td>Enable</td><td>No</td></tr>
<tr><td>Minimum Interval Between Adaptive Modulation Messages</td><td>BU, RB</td><td>1-3600 (seconds)</td><td>4 (seconds)</td><td>Yes</td></tr>
<tr><td>Adaptive Modulation Decisión Thresholds</td><td>BU, RB</td><td>■   Normal

■   High</td><td>Normal</td><td>No</td></tr>
<tr><td>Concatenation Option</td><td>BU, RB</td><td>■   Disable

■   Enable</td><td>Enable</td><td>No</td></tr>
</table>

* Applicable only if Burst Mode is supported by the Sub Band.

Service Parameters

<table>
<tr><th colspan="5">Table E-7: Service Parameters</th></tr>
<tr><th>Parameter</th><th>Unit</th><th>Range</th><th>Default</th><th>Run-Time</th></tr>
<tr>
<td>User Filtering Option</td>
<td>RB</td>
<td>■   Disable

■   IP Protocol Only

■   User Defined Addresses Only

■   PPPoE Protocol Only</td>
<td>Disable</td>
<td>Yes</td>
</tr>
<tr>
<td>Set User Filter Address</td>
<td>RB</td>
<td>IP address (8 entries)</td>
<td>0.0.0.0
(all 8 entries)</td>
<td>Yes</td>
</tr>
<tr>
<td>Set User Filter Mask</td>
<td>RB</td>
<td>IP address (8 entries)</td>
<td>255.255.255.255
(all 8 entries)</td>
<td>Yes</td>
</tr>
<tr>
<td>Set User Filter Range</td>
<td>RB</td>
<td>0 – 255. 0 means that the range is not used.</td>
<td>0
(all 8 entries)</td>
<td>Yes</td>
</tr>
<tr>
<td>DHCP Unicast Override Filter</td>
<td>RB</td>
<td>■   Disable DHCP Unicast

■   Enable DHCP Unicast</td>
<td>Disable DHCP Unicast</td>
<td>Yes</td>
</tr>
<tr>
<td>MIR: Downlink</td>
<td>RB</td>
<td>RB-14: 128 - 6912 (Kbps)

RB-28: 128 – 22016 (Kbps)</td>
<td>RB-14: 6912

RB-28: 22016</td>
<td>No</td>
</tr>
<tr>
<td>MIR: Uplink</td>
<td>RB</td>
<td>RB-14: 128 - 6912 (Kbps)

RB-28: 128 – 22016 (Kbps)</td>
<td>RB-14: 6912

RB-28: 22016</td>
<td>No</td>
</tr>
</table>

Security Parameters

<table>
<tr><td colspan="5">Table E-8: Security Parameters</td></tr>
<tr><td>Parameter</td><td>Unit</td><td>Range</td><td>Default</td><td>Run-Time</td></tr>
<tr><td>Authentication Algorithm*</td><td>BU, RB</td><td>■ Open system

■ Shared Key</td><td>Open system</td><td>No</td></tr>
<tr><td>Data Encryption Option*</td><td>BU, RB</td><td>■ Disable

■ Enable</td><td>Disable</td><td>No</td></tr>
<tr><td>Security Mode*</td><td>BU, RB</td><td>■ WEP

■ AES</td><td>WEP</td><td>No</td></tr>
<tr><td>Default Key</td><td>RB</td><td>1-4</td><td>1</td><td>No</td></tr>
<tr><td>Default Multicast Key</td><td>BU</td><td>1-4</td><td>1</td><td>No</td></tr>
<tr><td>Key # 1 to Key # 4</td><td>BU, RB</td><td>32 hexadecimal digits</td><td>0…0 (all 0=no key)</td><td>No</td></tr>
<tr><td>Promiscuous Authentication</td><td>BU</td><td>■ Disable

■ Enable</td><td>Disable</td><td>Yes (Disable after reset)</td></tr>
</table>

* Applicable only if supported by the Sub Band.
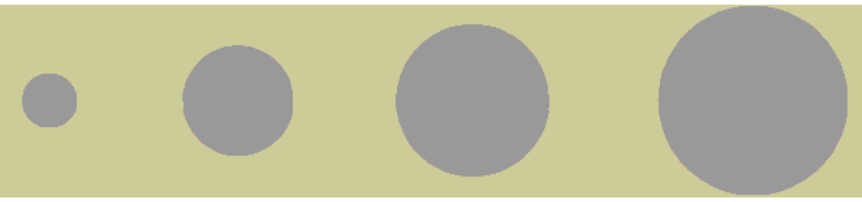
F

Appendix F - Using the Feature
License Web Application

The Feature License Web Application

Certain features of BreezeNET B products may be upgraded through loading special feature license strings. Once you receive the invoice for new license(s) purchased, use the Alvarion web site for getting license strings for specific products.

To access the Feature License Application:

1. In the Alvarion web site (www.alvarion.com), select the Customer Service option.

2. In the Customer Service page, select the Service Call Entry option.

3. In the User Login form, enter your User ID and Password and click Login.

4. Select SSM - Customer Service Area.

5. Select the Feature License option.

The Get Feature License Key form with the current status of your license(s) is displayed:

To get details on the updated status of your licenses:

Check on the License Key Enquiry button to get the updated status of the licenses:

The displayed information includes account history with details on all license strings that were provided.

To get a License Key for a single device:

1. Check the required feature license entry and click on the Get Key button. The Enter MAC Address form will be displayed:

2. Enter the MAC Address of the device you want to upgrade.

3. Click on the Get Key button. The License Key for the device will be displayed.

NOTE

An error message will be displayed upon requesting a key for a non-valid MAC address.

To get License Keys for multiple devices:

This feature enables you to load a list of MAC Addresses from a pre-prepared Excel file.

NOTE

The Excel file should contain a single column of MAC addresses (no empty cells). This must be column A, starting at row 1, which is the title row.

1. Check the required feature license entry and click on Upload MAC Address List from Excel button. The Get MAC Addresses from Excel File form will be displayed:

NOTE

You may need to change your Browser security settings. For details press the Change Security Level link in the form.

2. Use the browser or enter the path to the Excel file holding the MAC Addresses. Enter the MAC Address of the device you want to upgrade.

3. Click on the Import File button to get a list of License Keys for the devices included in the Excel file.

NOTE
An error message will be displayed upon requesting a key for a non-valid MAC address.

Loading License Strings to Devices

To upgrade a single device:

There are several options to load a feature license string to a single device:

■ **Using Telnet:** Use the Feature Upgrade option in the Unit Control menu.

■ **Using TFTP:** Use the file with the extension ".fln" for feature license strings. Refer to Appendix B (File Upload and Download Using TFTP) for more details.

■ **Using BreezeCONFIG:** Enter the license string in the Feature Upgrade field of the Unit Control window. Refer to the BreezeCONFIG User's Guide for more details.

To upgrade multiple devices using a feature licenses file:

■ **Using TFTP:** Use the file with the extension ".fln" for feature license strings. Refer to Appendix B (File Upload and Download Using TFTP) for more details. Note that Feature license files include multiple strings, where each string is applicable only for a certain unit identified by its MAC address. When uploading a feature license or a country code file to multiple units, each unit will accept only the parts that are applicable for it.

■ **Using BreezeCONFIG:** Use the File Loading Utility. Refer to the BreezeCONFIG User's Guide for more details.

> **NOTE**
>
> After completing the license string loading process, reset the unit(s) to apply the change. Use the Info Screens menu (Show Unit Status) to verify that the unit has been upgraded.