alvarion
We're on your wavelength.

PRELIMINARY

BreezeNET® B

System Manual

SW Version 1.1
July 2003
P/N 213527

Legal Rights

Trade Names

Alvarion®, BreezeACCESS®, BreezeCOM®, BreezeLINK®, BreezePHONE®, BreezeNET®, WALKair®, WALKnet®, MGW®, eMGW® Alvari, AlvariX, AlvariSTAR, AlvariBASE, BreezeGATE, BreezeIP, BreezeLAN, BreezeWEB, BrezEXCHANGE, BreezeCONFIG, BreezeWIZARD, BreezeSECURE, BreezeVIEW, BreezeMANAGE, BreezeACCESS II, BreezeACCESS II CX, BreezeACCESS XL, BreezeACCESS MMDS, BreezeACCESS OFDM, BreezeACCESS LB, BreezeACCESS TM, BreezeACCESS VL, BreezeACCESS V, BreezeACCESS GO, WALKair 1000, WALKair 3000, BreezeNET Pro.11, BreezeNET, DS.11, BreezeNET DS.11b, BreezeNET DS.5800, BreezeNET B, are trade names or trademarks of Alvarion Ltd. Other brand and product names are trade names or trademarks of their respective owners.

Statement of Conditions

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

Warranties and Disclaimers

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

Exclusive Warranty

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

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 EN300385 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 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

Be sure that the outdoor unit, the antenna and the supporting structure are properly installed to eliminate any physical hazard to either people or property. Verify that the outdoor unit and the antenna mast (when using external antenna) are grounded so as to provide protection against voltage surges and static charges. 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.

Important Notice

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

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

Some of the equipment provided by Alvarion and specified in this manual, is manufactured and warranted by third parties. All such equipment must be installed and handled in full compliance with the instructions provided by such manufacturers as attached to this manual or provided thereafter by Alvarion or the manufacturers. Non-compliance with such instructions may result in serious damage and/or bodily harm and/or void the user’s authority to operate the equipment and/or revoke the warranty provided by such manufacturer.

About this Guide

This manual describes the BreezeNET B Point-to-Point Wireless Bridge Release 1.1 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** – **Configuration Download and Upload Using TFTP:** Describes how to download and upload configuration files using TFTP.
- **Appendix C** – **Preparing the indoor to outdoor cable:** Provides details on preparation of the indoor to outdoor Ethernet cable.
- **Appendix D** – **Parameters Summary:** Provides an at a glance summary of the configuration parameters, value ranges and default values.

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 operates in the unlicensed UNII band of 5.8 GHz and utilizes advanced technologies to support optimal performance in spectrally poluuted 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.

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 5.725-5.850 GHz frequency band. 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 28 Mbps.

The ODUs 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 1-1: Detached Antennas

Antenna	Band (GHz)	Horizontal Beam Width	Gain
UNI-23-9	5.725-5.850	9°	23 dBi
UNI-24-4	5.725-5.850	4.5°	28 dBi

Specifications

Radio specifications

Table 1-2: Radio Specifications

Item	**Description**
Frequency	5.725 – 5.850 GHz
Operation Mode	Time Division Duplex (TDD)
Channel Bandwidth	20 MHz
Central Frequency Resolution	10 MHz
ODU Integral Antenna	21dBi, 5.150-5.875 GHz, 10.5° horizontal x 10.5° vertical, vertical polarization, compliant with EN 302 085 V1.1.1 Range 1, Class TS 1, 2, 3, 4, 5
Detached Antennas	■ UNI-23-9: 23dBi, 5.725-5.850 GHz, 9° horizontal x 9° vertical, vertical polarization, compliant with EN 302 085 V1.1.2 (2001-2002) ■ UNI-28-4: 28dBi, 5.725-5.850 GHz, 4.5° horizontal x 4.5° 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)	-48dBm typical
Output Power (at antenna port)	RB: -10 to 21dBm, automatically adjustable by ATPC BU: -10 to 21dBm.

Table 1-2: Radio Specifications

Item	Description		
Sensitivity, typical (dBm at antenna port, PER<10%)	Modulation Level*	Sensitivity	Min. SNR
	1	-87 dBm	6 dB
	2	-86 dBm	7 dB
	3	-85 dBm	9 dB
	4	-83 dBm	11 dB
	5	-80 dBm	14 dB
	6	-76 dBm	18 dB
	7	-71 dBm	22 dB
Modulation	OFDM modulation, 64 FFT points; BPSK, QPSK, QAM16, QAM64		

* 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 1-3: Data Communication

Item	Description
Standard compliance	IEEE 802.3 CSMA/CD
VLAN Support	Based on IEEE 802.1Q
Layer-2 Traffic Prioritization	Based on IEEE 802.1p
Layer-3 Traffic Prioritization	IP ToS according to RFC791

Configuration and Management

Table 1-4: Configuration and Management

Type	Standard
Management	■ Via Telnet ■ SNMP based Configuration Utility ■ Configuration upload/download
Management Access	From Wired LAN, Wireless Link
Management access protection	■ Multilevel password ■ Configuration of remote access direction (from Ethernet only, from wireless link only or from both sides) ■ Configuration of IP addresses of authorized stations
Security	■ Authentication messages encryption option ■ Data encryption option ■ Selection between WEP and AES 128-bit encryption standards ■ ESSID
SNMP Agents	SNMP ver 1 client, MIB II, Bridge MIB, Private MIB
Allocation of IP parameters	Configurable or automatic (DHCP client)
Software upgrade	■ FTP ■ TFTP
Configuration upload/download	■ FTP ■ TFTP

Mechanical

Table 1-5: Mechanical Specifications

Unit	Structure	Dimensions (cm)	Weight (kg)
General	An IDU indoor unit and an ODU outdoor unit		
IDU	Plastic box, desktop or wall mountable	16 x 9 x 6	0.55
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.	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.	60 x 60 x 5.5	5

Connectors

Table 1-6: Connectors

Unit	Connector	Description
IDU	ETHERNET	10/100BaseT Ethernet (RJ-45) with 2 embedded LEDs. Cable connection to a PC: crossed Cable connection to a hub: Straight
	RADIO	10/100BaseT Ethernet (RJ-45): Ethernet + power for outdoor connection over a CAT-5 shielded cable
	AC IN	3 pin AC power plug
ODU	INDOOR	10/100BaseT Ethernet (RJ-45), protected by a waterproof sealing assembly
	ANT (D models)	N-Type jack, 50 ohm, lightning protected
Antenna	RF	N-Type jack (on a 35cm LMR-240 cable)

Electrical

Table 1-7: Electrical Specifications

Unit	Details
General	Power consumption: 25W
IDU	AC power input: 100-240 VAC, 50-60 Hz
ODU	54VDC from the IDU over the indoor-outdoor Cat-5 shielded Ethernet cable

Environmental

Table 1-8: Environmental Specifications

Type	Unit	Details
Operating temperature	Outdoor units	-40 °C to 55 °C
	Indoor equipment	0 °C to 40 °C
Operating humidity	Outdoor units	5%-95% non condensing, Weather protected
	Indoor equipment	5%-95% non condensing

Standards Compliance, General

Table 1-9: Standards Compliance, General

Type	Standard	
EMC	FCC part 15 class B, CE EN55022 class B	
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, ETS 301 253	

This page left intentionally blank.

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)
- 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.

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.

NOTE

The system complies with the ETS 300 385 standard and is protected against secondary lightning strikes when the Outdoor Unit is properly grounded according to the relevant country specific industry standards for protection of structures against lightning. The system complies with EN 61000 4 5 test level 3 (2kV).

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.

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.

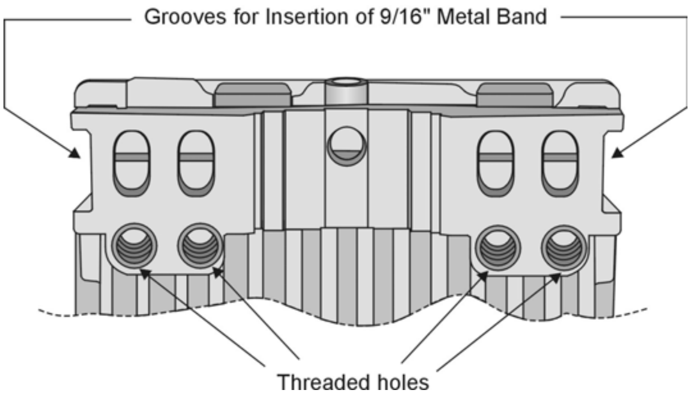


Figure 2-1: Threaded Holes/Grooves

Figure 2-2 illustrates the method of installing an outdoor unit on a pole, using the brackets and open-ended bolts.

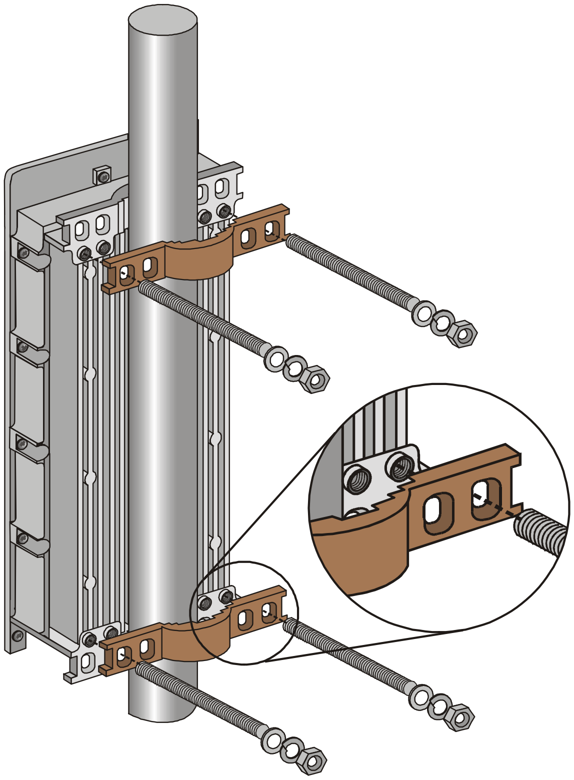


Figure 2-2: 3" Pole Installation Using Special Brackets

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 Y) 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

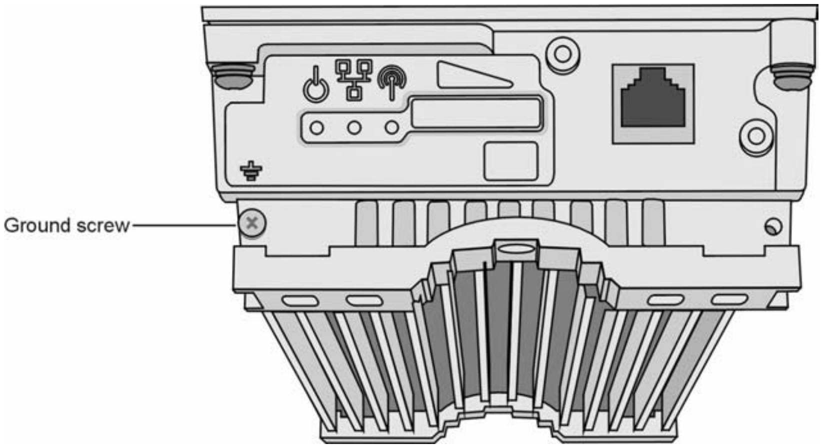


Figure 2-3: Bottom Panel of the Outdoor Unit (without the seal assembly)

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.

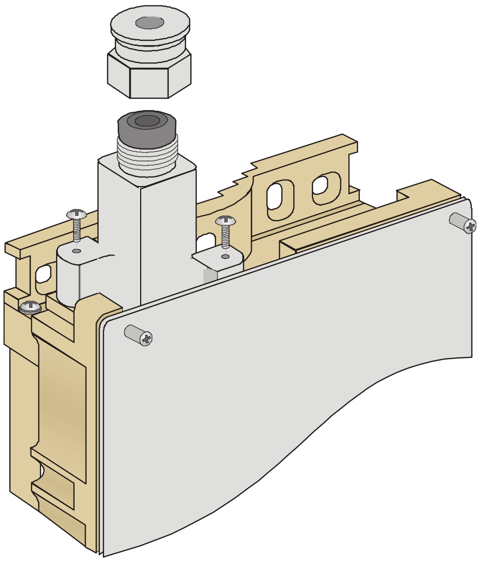


Figure 2-4: The Waterproof Seal

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

NOTE

The 8-wire cable should be shielded.

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 process1

To install the IDU:

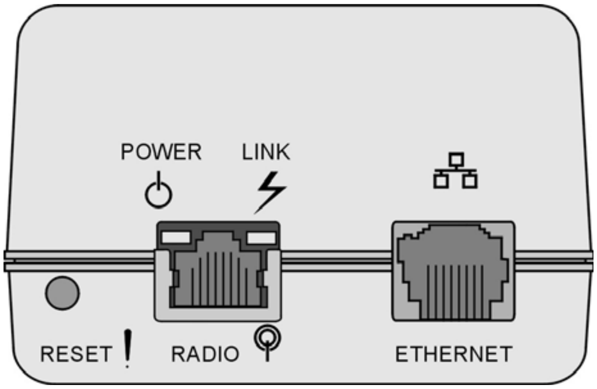


Figure 2-5: IDU Front Panel

1. Connect the Indoor-to-Outdoor cable to the RADIO connector, located on the front panel of the indoor unit shown in Figure 2-5.
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 after verifying that the unit is rated for the voltage in the country of use; the AC raing is indicated on the rear panel of the Indoor unit.

NOTE

The color codes of the power cable are as follows:

Brown	Phase	~
Blue	Neutral	0
Yellow/Green	Ground	⏚

3. Verify that the yellow POWER LED located on the front panel is lit, indicating that the unit is supplying power to the radio port.
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 unit 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.

NOTE

Reset the unit using the RESET recessed push button after connecting or reconnecting the indoor and outdoor units with the indoor-to-outdoor cable.

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.

Table 3-1: Basic Parameters

Parameter	Default Value	Comment
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	
ESSID	ESSID1	
Frequency (BU)	5740 MHz	
Sub Band Lower Frequency (RB)	5740 MHz	
Sub Band Upper Frequency (RB)	5830 MHz	
Scanning Step (RB)	10 MHz	

Table 3-1: Basic Parameters

Parameter	Default Value	Comment
Frequency Subset Definition (RB)	A (All)	
Tx Power for Modulation Levels 1 to 5	21	Tx Power setting must be in accordance with applicable regulations. For example, for compliance with FCC regulations the maximum EIRP in the AU (Tx Power + Antenna Gain) cannot exceed 36 dBm
Tx Power for Modulation Level 6	21	
Tx Power for Modulation Level 7	21	
ATPC Option	Enable	
Best BU Support (RB)	Disable	
Preferred BU MAC Address (RB)	00-00-00-00-00-00 (none)	Applicable only when Best BU Support is enabled
Maximum Cell Distance (BU)	0 (No Compensation)	
Maximum Modulation Level	7	Refer Configuring the Maximum Modulation Level on page 3-7
VLAN Link Type	Hybrid	
VLAN ID-Management	65535	
Authentication Algorithm*	Open System	
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)	

* Some or all of the Security parameters may not be available in units that do not support the Authentication Security and/or Data Encryption feature.

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 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 antennas:

1. Align the antennas (integrated into the front side of the ODU unit, or detached) by pointing each antenna it in the general direction of the other unit.
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 antennas at higher or alternate locations.
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.

7. Repeat steps 4 - 6 for the antenna of the BU.

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 applicable 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 sensitivity 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> 22 dB	7
18 dB< SNR < 22 dB	6
14 dB < SNR < 18 dB	5
11 dB < SNR < 14 dB	4
9 dB < SNR < 11 dB	3
7 dB < SNR < 9 dB	2
6 dB<SNR < 7 dB	1

Operation Verification

The following sections describe how to verify the correct functioning of the Outdoor Units, Indoor Units, 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
LED 1 (red) is On	Signal is too low (SNR < 4dB)
LED 2 (green) is On	SNR > 4 dB
LEDs 2-3 (green) are On	SNR > 10 dB
LEDs 2-4 (green) are On	SNR > 16 dB
LEDs 2-5 (green) are On	SNR > 22 dB
LEDs 2-6 (green) are On	SNR > 28 dB
LEDs 2-7 (green) are On	SNR > 34 dB
LEDs 2-8 (green) are On	SNR > 40 dB
LEDs 2-9 (green) are On	SNR > 46 dB
LEDs 2-9 (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.

Error! Reference source not found. lists the LEDs of the IDU and their associated indications.

Table 3-6: IDU Indoor Unit LEDs

Name	Description	Functionality
POWER	Power Indication	■ Green - 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. ■ Orange– Self-test passed and Ethernet connection confirmed by the outdoor unit (Ethernet integrity check passed).

Verifying the Ethernet Connection

Once you have connected the unit to an Ethernet outlet, verify that the Ethernet Integrity Indicator, which is the yellow LED embedded in the 10/100 BaseT connector, is **On**. This indicates that the unit is connected to an Ethernet segment. The Ethernet Activity Indicator, which is the green embedded LED, should blink whenever the unit receives or transmits traffic on the 10/100 BaseT port.

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

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.

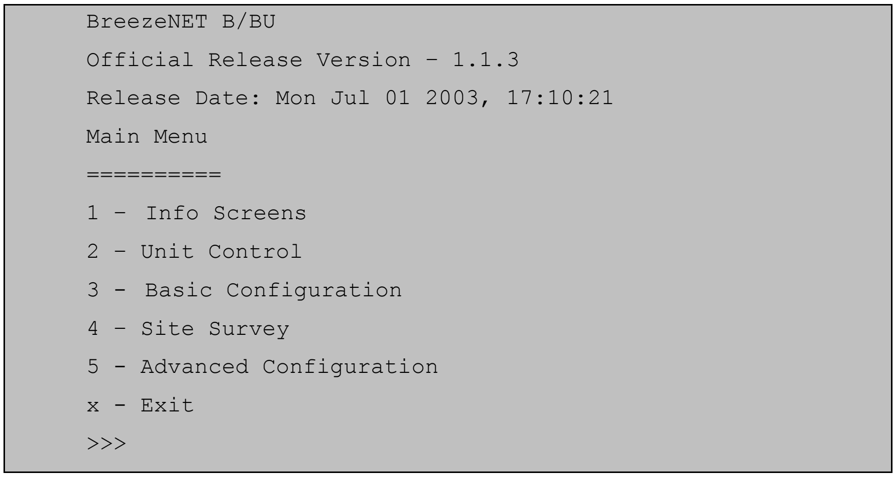
Table 4-1: Default Passwords

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.

NOTE

The program is automatically terminated following a determined period of inactivity. The default time out is 5 minutes and is configured with the Log Out Timer parameter.

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 Working with the Monitor Program, 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.

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.
- **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 (5.8 GHz)
- **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
- **FTPSoftware Version Download Parameters:** The parameters for SW download using FTP, as defined in Unit Control menu.
  - FTP Source Dir
  - FTP File Name
- **Configuration File Download/Upload Parameters:** The parameters for Configuration file upload/download using FTP, as defined in Unit Control menu.
  - Configuration File Source Dir
  - Configuration File Name
  - Operator Defaults File Name
-
- **FTP Log File Upload Parameters:** The parameters for Event Log file upload using FTP, as defined in Unit Control menu.
  - Event Log File Name
  - Event Log destination Directory
- **Event Log Policy**

The following parameters are displayed for RB only:

- **Unit Status:** The current status of the RB. There are two status options:
  - **SCANNING:** The RB is searching for a BU with which to associate.
  - **ASSOCIATED:** The RB is associated with a BU.

- **BU MAC Address:** 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 00-00-00-00-00-00. broadcast address, which is FF-FF-FF-FF-FF-FF.

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 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

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 available options are:

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 4-16. These files can also be uploaded/downloaded remotely using TFTP (see Appendix B - Configuration Download and Upload Using TFTP).

The available options in the Set Defaults submenu are:

- **Set Complete Factory Defaults:** Available only with Administrator access rights. Resets 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

Parameters Group	Parameter
Unit Control Parameters	Passwords
	FTP Server IP address
	FTP Gateway IP address
	FTP Client IP address
	FTP Client IP Mask
	FTP Use Name
	FTP Password
Air Interface Parameters	Frequency (BU)
	Sub Band Lower Frequency (RB)
	Sub Band Upper Frequency (RB)
	Frequency Subset definition (RB)
	Scanning Step (RB)

- **Set Partial Factory defaults:** Resets 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 with Administrator access rights are listed in Table 4-3.

Table 4-3: Parameters that are not reset after Set Partial Factory/Operator Defaults (Using Administrator Access Rights)

Parameters Group	Parameter
Unit Control parameters	Passwords
	FTP Server IP address
	FTP Gateway IP address
	FTP Client IP address
	FTP Client IP Mask
	FTP Use Name
	FTP Password
IP Parameters	IP Address
	Subnet Mask
	Default Gateway Address
	DHCP Option
	Access to DHCP
Air Interface Parameters	ESSID
	Operator ESSID Option (BU)
	Operator ESSID (BU)
	Frequency (BU)
	Sub Band Lower Frequency (RB)
	Sub Band Upper Frequency (RB)
	Scanning Step (RB)
	Frequency Subset definition (RB)
	Best BU Support (RB)
	Preferred BU MAC Address (RB)

Table 4-3: Parameters that are not reset after Set Partial Factory/Operator Defaults (Using Administrator Access Rights)

Parameters Group	Parameter
Security Parameters	Authentication Algorithm
	Default Key (RB)
	Data Encryption Mode
	Security Mode
	Key # 1 to Key # 4
Bridge Parameters	VLAN ID - Data (RB)
	VLAN ID - Management
	VLAN Link Type
	VLAN Forwarding Support
	VLAN Forwarding ID (1 - 20)
	VLAN Priority - Data (RB)
	VLAN Priority - Management
	VLAN Priority Threshold

NOTE

This table details all the parameters that do not change after Set Partial Factory/Operator Defaults using Administrator access rights. When performing Set Partial Factory/Operator Defaults using Installer access rights, only parameters accessible to Installers are reset to their default values (provided they are not included in the list of parameters necessary to ensure connectivity and management access). The parameters that are reset to their default values in this case are Unit Name, SW Version File Name, Configuration File Name, Operator Defaults File Name, FTP Source Dir, Ethernet Port Negotiation Mode and Log Out Timer. All other parameters are not changed after Set Partial Factory/Operator Defaults using Installer access rights.

- **Set Complete Operators Defaults:** Available only with Administrator access rights. Resets the unit to the Operator Defaults configuration, excluding several parameters that are listed in Table 4-2.

- **Set Partial Operator defaults:** Resets 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 with Administrator access rights are listed in Table 4-3.

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 Working with the Monitor Program, 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.

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

  Valid values: A string of up to 80 printable ASCII characters.

  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: None (empty)

- **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 procedure.

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 Get 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.

  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.

  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: None (empty)

- **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 procedure.

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 & Half-Duplex
- Force 10 Mbps & Full-Duplex
- Force 100 Mbps & Half-Duplex
- Force 100 Mbps & Full-Duplex
- Auto Negotiation (10/100 Mbps and Half/Full Duplex)

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

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 displayed). 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

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: None (empty)
- **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 procedure.

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 IP Parameters, on page 4-32, for a description of these parameters.

Air Interface Parameters

- ESSID
- Operator ESSID Parameters (BU)
  - Operator ESSID Option
  - Operator ESSID
- Frequency Definition
  - Frequency (BU)
  - Sub Band Lower Frequency (RB)
  - Sub Band Lower Frequency (RB)
  - Scanning Step (RB)
  - Frequency Subset Definition (RB)

- Best BU Parameters (RB)
  - Best BU Support
  - Number of Scanning Attempts
  - Preferred BU MAC Address
- Maximum Link Distance (BU)
- ATPC
  - ATPC Option
  - Tx Power parameters

Refer to Air Interface Parameters, on page 4-35, for a description of these parameters.

Performance Parameters

- Maximum Modulation Level

Refer to Performance Parameters on page 4-58, for a description of these parameters.

Bridge Parameters

- VLAN Support
  - VLAN ID   Management
  - VLAN Link Type

Refer to VLAN Support, on page 4-48, for a description of these parameters.

Security Parameters

- Authentication Algorithm
- Data Encryption Option
- Security Mode
- Promiscuous Authentication (BU)
- Default Key (RB)
- Key 1 to Key 4

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 4-65, 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 following sections describe each option of the Site Survey menu.

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 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 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.

Wireless Link 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, which is determined by the **Maximum Link distance** parameter, 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
  - Data and Other Management 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 Low, Mid and High (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 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:
  - Excessive Retries (Exces RTx): The number of dropped frames, which are the frames unsuccessfully retransmitted until the maximum permitted number of retransmissions without being acknowledged.
  - Delayed: The number of frames whose transmission was delayed because they were in the queue for transmission when the SW Retry mechanism was activated for a previous frame designated to the same address. (refer to Adaptive Modulation Algorithm on page 4-60 for more information)
  - 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: The number of frames that were not received properly due to a hardware problem.
  - 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.

- **Bad frames received:** The number of frames 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.

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 200 to 2000 ms, in increments of 200 milliseconds. For example, 200, 400, 600…2000. 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.

Continuous Link Quality Display (RB only)

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

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

MAC Address Database

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 applicable RB is also displayed (in parenthesis).
- **St (Static):** An associated RB. For these 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 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.
  - 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.

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

  - 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 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 → RB	-
RB Status: Synchronized		
Authentication Request	RB → BU	Not authenticated
Authentication Successful	BU → RB	Authenticated
RB Status: Authenticated		
Association Request	RB → BU	Authenticated
Association Successful	BU → RB	Associated
RB Status: Associated		
ACK	RB → BU	Associated
Data Traffic	RB ↔ BU	Associated

- The SNR measured at the RB
- The SW version of the RB.

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.

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):** 7 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.
    - 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 1017.

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 frames at the applicable modulation level.

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 enables configuring the following parameters:

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 addres 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

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. The units as management frames handle DHCP messages.
- 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 searched for and communicate 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.

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 network 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

Frequency Definition Submenu in BU

The Frequency Definition submenu in BU includes a single parameter for setting the transmit/receive frequency:

Frequency

The Frequency parameter defines the transmit/receive frequency. The minimum distance between frequencies used by two neighboring BUs is the Channel bandwidth, which is 20 MHz.

The range is from 5740 to 5830 MHz, using a 10 MHz resolution.

The default is 5740 MHz.

Frequency Definition Submenu in RB

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. During the scanning process, the RB stays for 640 milliseconds on each of the frequencies in the defined set. If no BU is found, the RB will start another scanning cycle. If no BU is found after a certain number of scanning cycles or after 5 minutes (whichever event occurs first), the RB is reset and the process is resumed.

The Frequency Definition submenu in RB includes the following parameters:

Sub Band Lower Frequency

The Sub Band Lower Frequency parameter defines the lowest frequency to be used during the scanning process.

The range is from 5740 to 5830 MHz, using a 10 MHz resolution.

The default is 5740 MHz.

Sub Band Upper Frequency

The Sub Band Upper Frequency parameter defines the highest frequency to be used during the scanning process.

The range is from 5740 to 5830 MHz, using a 10 MHz resolution.

The default is 5830 MHz.

Scanning Step

The Scanning Step parameter defines the resolution used for selecting frequencies in the sub band defined by the **Sub Band Lower Frequency** and the **Sub Band Upper Frequency**.

Valid values: 10, 20 MHz.

Default value: 10 MHz.

Frequency Subset Definition

The previous parameters define a sub band of frequencies between the **Sub Band Lower Frequency** and the **Sub Band Upper Frequency** using the **Scanning Step** resolution. The Frequency Subset Definition option enables defining a specific subset of frequencies within this sub band to be used during scanning. When selected, a list of all valid frequencies in the band is displayed, and an index is given to each frequency. The current defined subset is also displayed. The defined subset is modified by entering a list of desired indexes, separated by commas (no spaces). Enter A to select all frequencies in the subset.

The default is **A**, which is the list that includes all indexes of frequencies defined by the previous parameters.

Show Frequency Definition Parameters

The Show Frequency Definition Parameters option displays all the Frequency Definition parameters, including the defined subset and the **Current Frequency Subset**, which is the subset currently in use. It also displays the **Current Operating Frequency**, which is the discreet frequency currently used by the unit.

Best BU Parameters (RB)

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 same limitation also exists if only one BU in the neighborhood has an ESSID identical to the one used by the RB, since it is not always necessarily the best choice.

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.

The total scanning time can be calculated based on the following formula:

Scanning Time (secs) = N * F * 2

N = Number of scanning attempts.

F = Number of frequencies in the Frequency Subset defined in the **Frequency Definition** submenu.

2 seconds is the time spent on each frequency while in scanning mode.

Preferred BU MAC Address

The Preferred BU MAC Address parameter defines a specific BU with which the RB should associate. Gaining control of the RBs 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)

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 all units.

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 typically the maximum supported transmit power is used to enable maximum coverage. However, there may be a need to decrease the transmitted power level in order to support relatively small cells and to minimize the interference with the operation of neighboring cells.

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 in BU

The Transmit Power parameters define the transmit power level of the BU. These parameters are not part of the ATPC algorithm.

Transmit Power for Modulation Levels 1 to 5

Valid range: -10 to 21 (dBm), using a 1dBm resolution.

The default is 21 (dBm).

Transmit Power for Modulation Level 6

Valid range: -10 to 21 (dBm), using a 1dBm resolution.

The default is 21 (dBm).

Transmit Power for Modulation Level 7

Valid range: -10 to 21 (dBm), using a 1dBm resolution.

The default is 21 (dBm).

Transmit Power in 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.

Transmit Power for Modulation Levels 1 to 5

Valid range: -10 to 21 (dBm), using a 1dBm resolution.

The default is 21 (dBm).

Transmit Power for Modulation Level 6

Valid range: -10 to 21 (dBm), using a 1dBm resolution.

The default is 21 (dBm).

Transmit Power for Modulation Level 7

Valid range: -10 to 21 (dBm), using a 1dBm resolution.

The default is 21 (dBm).

ATPC Parameters in BU

ATPC Option

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

The default is Enable.

Minimum SNR Level

The Minimum SNR Level defines the lowest SNR at which you want each 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).

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: 4 (dB).

Minimum Interval Between ATPC Messages

The Minimum Interval Between ATPC Messages parameter sets the minimal time between consecutive power-up/power-down messages to a specific 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 RBs 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 RBs 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.

Maximum Link distance (BU only)

The distance between the BU and the RB it should serve. The Maximum Link Distance affects the maximum time that a unit will wait for a response message (including acknowledgements of data frames and response messages during the authentication and association process) by taking into account the round trip propagation delay (the one-way propagation delay at 5 GHz is 3.3 microsecond/km). This parameter is configured in the BU, and the RB learns it during the association process.

The range is 1-50,000 (meters) or 0 for No Compensation. No Compensation means an acknowledge time-out of 138 microseconds.

The default is 0 (No Compensation**)**.

Wireless Trap Threshold (BU only)

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

The default is 30 (%).

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

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 & Wireless Link

The default selection is From Both Ethernet & 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.

- **Enable Management IP Filtering on Ethernet Port:** Applicable only if the Access to Network Management parameter is configured to either From Ethernet Only or From Both Ethernet & 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 & Wireless Link then no IP address based filtering is configured for the wireless port.
- **Enable Management IP Filtering 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 & 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 & Wireless Link then no IP address based filtering is configured for the Ethernet port.
- **Enable Management IP filtering on Both Ethernet & Wireless Link Port:** 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 Addresses

The **Set Network Management IP Addresses** option enables defining up to 3 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 3 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 3 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 following options are available:

- Enable Traps Sending
- Disable Traps Sending

The default selection is Disable Traps Sending.

SNMP Traps IP Destination

The SNMP Traps IP Destination option enables defining up to 3 IP addresses of devices to which the SNMP Traps are to be sent.

The default of all three 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 3 addresses is public, which is the default Read community.

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.

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 enables configuring the following parameters:

VLAN ID-Data (RB only)

The VLAN ID-Data is applicable for Access Links only. 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.

If VLAN Relaying Support and VLAN Forwarding Support are both enabled, then all VLAN IDs configured in the Relaying List must also be configured in the Forwarding List.

VLAN Traffic Priority

Each packet to be transmitted to the wireless link is transferred to one of three queues: Low, Mid and High. Packets in the High queue have the highest priority for transmission, and those in the Low queue have the lowest priority.

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 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 Mid 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 Mid queue. This is applicable to both tagged and untagged frames.

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 another BreezeNET B unit via the wireless port, is sent to the High queue, regardless of the priority configuration.

The VLAN Traffic Priority menu provides the following parameters:

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 Mid 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 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 Mid 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.

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 Broadcasting Filtering menu enables configuring the following parameters:

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.
- **From Ethernet Only**, which filters broadcast messages received from the Ethernet port.
- **From Wireless Link Only**, which filters broadcast messages received from the wireless link port.
- **Both From Ethernet & Wireless Link**, 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.

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 provides the following parameters:

Maximum Modulation Level

When the Adaptive Modulation Adaptation (see Adaptive Modulation Algorithm on page 4-60) is enabled, it changes the modulation level dynamically according to link conditions 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 elevates 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 reduce 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 default is Modulation Level 7.

Table 4-9: Recommended Maximum Modulation Level

SNR	Maximum Modulation Level
SNR> 22 dB	7
18 dB< SNR < 22 dB	6
14 dB < SNR < 18 dB	5
11 dB < SNR < 14 dB	4
9 dB < SNR < 11 dB	3
7 dB < SNR < 9 dB	2
6 dB<SNR < 7 dB	1

Average SNR Memory Factor

The 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, or when it is enabled but the Software Retry Support 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 both the Adaptive Modulation Algorithm and the Software Retry Support options are enabled, refer to Adaptive Modulation Algorithm, on page 4-60.

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.

Burst Mode Option

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

The default is Enable.

NOTE

When Burst Mode Option is enabled, do not change the SW Retry Support parameter in the Adaptive Modulation menu from its default setting of Disable.

Burst Period

The Burst Period 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 10 milliseconds.

The default is 5 milliseconds

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 relate to the modulation level selected for transmission of new frames (first trial attempt) as well as the modulation level for retransmissions. The decisions 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.

C. If the frame was not acknowledged and the Software Retry Support option is disabled, the frame will be dropped. If the Software Retry Option is enabled, the frame will be moved to the end of the queue. All other frames in the queue that are intended to the same destination will be moved as well, to preserve the original order. This process is referred to as a Software Retry.

D. The frame will be retransmitted at the modulation level selected by the algorithm for the new retrials sequence. Each retrial sequence comprises a number of attempts defined by the Number of HW Retries.

E. The process will be repeated up to a maximum number of Software Retries defined by the Number of SW Retries parameter.

The Adaptive Modulation Parameters 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, which is 1, to the value configured for the Maximum Modulation Level parameter. If the Maximum Modulation Level is set at 1, which is the lowest possible level, the Adaptive Modulation algorithm has no effect.

The default selection is Enable.

Software Retry Support

The Software Retry Support option enables or disables the software retry mechanism in the Adaptive Modulation algorithm. When enabled, the mechanism supports changes of modulation level in accordance with the Adaptive Modulation algorithm as described above.

The default selection is Disable.

Number of SW Retries

The Number of SW Retries parameter defines the maximum number of times to use the software Retrial mechanism when the Software Retry Support option is enabled.

The available values range from 0 to 14.

The default value is 3.

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.

Service Parameters (RB Only)

The Service Parameters menu enables defining user filtering parameters.

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

You can enter 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.

Show All 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.

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

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.

NOTE

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 Mode

The Data Encryption Mode 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 Mode 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.

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.

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 mode 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.

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 Sus.

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 - Configuration Download and Upload Using TFTP

The BreezeNET B Configuration 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.

When multiple configurations are being done simultaneously, which means that the file is being uploaded to several units, it is recommended that the file only include 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). Use the extension cfg for a configuration file. Use the extension cmr for the Operator Defaults file. The file should be transferred in ASCII mode.

For Example:

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

To download the Operator Defaults file from the same unit, enter:

tftp 206.25.63.65 get private.cmr Suconf

C

Appendix C - Preparing the Indoor to Outdoor Cable

The Indoor-to-Outdoor cable provides pin-to-pin connection on both ends.

Figure C-1 shows the wire pair connections required for the Indoor-to-Outdoor cable.

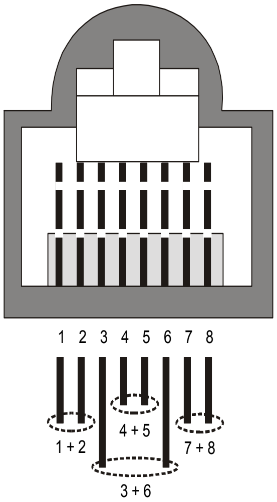


Figure C-1: Ethernet Connector Pin Assignments

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

Table C-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.

D

Appendix D - 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 D-1: Unit Control Parameters

Parameter	Unit	Range	Default	Run-Time
Change Unit Name	BU, RB	Up to 32 printable ASCII characters	None	Yes
Change Read Only Password	BU, RB	Up to 8 printable ASCII characters	public	No
Change Installer Password	BU, RB	Up to 8 printable ASCII characters	user	No
Change Administrator Password	BU, RB	Up to 8 printable ASCII characters	private	No
SW Version FTP File Name	BU, RB	Up to 20 printable ASCII characters		Yes
Configuration File Name	BU, RB	Up to 20 printable ASCII characters	config.cfg	Yes
Operator Defaults File Name	BU, RB	Up to 20 printable ASCII characters	operator.cmr	Yes
FTP Source Dir	BU, RB	Up to 80 printable ASCII characters. Use “.” to clear.	None (empty)	Yes
FTP Client IP Address	BU, RB	IP address	1.1.1.3	No
FTP Client IP Mask	BU, RB	IP address	255.255.255.0	No
FTP Server IP Address	BU, RB	IP address	1.1.1.4	No
FTP Gateway IP Address	BU, RB	IP address	None (empty)	No
FTP User Name	BU, RB	Up to 18 printable ASCII characters	vx	No
FTP Password	BU, RB	Up to 18 printable ASCII characters	Vx	No
Event Log File Name	BU, RB	Up to 20 printable ASCII characters	logfile.log	Yes
Event Log Destination Directory	BU, RB	Up to 80 printable ASCII characters. Use “.” to clear.	None (empty)	Yes
Event Log Policy	BU, RB	■ Message ■ Warning ■ Error ■ Fatal ■ Log None	Warning	Yes
Log Out Timer	BU, RB	1-999 minutes	5	Yes

Table D-1: Unit Control Parameters

Parameter	Unit	Range	Default	Run-Time
Ethernet Port Negotiation Mode	BU, RB	■ Force 10 Mbps & Half-Duplex ■ Force 10 Mbps & Full-Duplex ■ Force 100 Mbps & Half-Duplex ■ Force 100 Mbps & Full-Duplex ■ Auto Negotiation	Auto Negotiation	No

IP Parameters

Table D-2: IP Parameters

Parameter	Unit	Range	Default	Run-Time
IP Address	BU, RB	IP address	10.0.0.1	No
Subnet Mask	BU, RB	IP address	255.0.0.0	No
Default Gateway Address	BU, RB	IP address	0.0.0.0	No
DHCP Option	BU, RB	■ Disable ■ DHCP Only ■ Automatic	Disable	No
Access to DHCP	BU, RB	■ From Wireless Only ■ From Ethernet Only ■ From Both Wireless and Ethernet	■ BU: From Ethernet Only ■ RB: From Wireless Only	No

Air Interface Parameters

Table D-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

Table D-3: Air Interface Parameters

Parameter	Unit	Range	Default	Run-Time
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
Maximum Link Distance	BU	0-50,000 (meter) 0 means no compensation	0 (no compensation)	Yes
Wireless Trap Threshold	BU	1-100 (%)	30 (%)	Yes
Frequency	BU	5740 – 5830 MHz	5740 MHz	No
Sub Band Lower Frequency	RB	5740 – 5830 MHz	5740 MHz	No
Sub Band Upper Frequency	RB	5740 – 5830 MHz	5830 MHz	No
Scanning Step	RB	■ 10MHz ■ 20 MHz	10 MHz	No
Frequency Subset Definition	RB	Depends on selected Sub Band Lower and Upper Frequency and Scanning Step	A (All)	No
Tx Power For Modulation Levels 1 to 5	BU, RB	-10-21 (dB)	21 (dB)	Yes
Tx Power For Modulation Level 6	BU, RB	-10-21 (dB)	21 (dB)	Yes
Tx Power For Modulation Level 7	BU, RB	-10-21 (dB)	21 (dB)	Yes
ATPC Option	BU, RB	■ Disable ■ Enable	Enable	Yes
Delta From Minimum SNR Level	BU	4-20 (dB)	4 (dB)	Yes
Minimum SNR Level	BU	4-60 (dB)	20 (dB)	Yes
Minimum Interval Between ATPC Messages	BU	1-3600 (seconds)	30 (seconds)	Yes
ATPC Power Level Steps	BU	1-20 (dB)	5	Yes

Network Management Parameters

Table D-4: Network Management Parameters

Parameter	Unit	Range	Default	Run-Time
Access to Network Management	BU, RB	■ From Wireless Link Only ■ From Ethernet Only ■ From Both Ethernet and Wireless Link	From Both Ethernet and Wireless Link	No
Network Management Filtering	BU, RB	■ Disable ■ Activate Management IP Filter On Ethernet Port ■ Activate Management IP Filter On Wireless Port ■ Activate Management IP Filter On Both Ethernet & Wireless Ports	Disable	No
Set Network Management IP Address	BU, RB	IP address	0.0.0.0 (all 3 entries)	Yes
Send SNMP Traps	BU, RB	■ Disable Traps Sending ■ Enable Traps Sending	Disable Traps Sending	Yes
SNPM Traps IP Destination	BU, RB	IP address	0.0.0.0 (all 3 entries)	No
SNMP Traps Community	BU, RB	Up to 14 printable ASCII characters	public (all 3 entries)	No

Bridge Parameters

Table D-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	AU, SU	20 – 2000 seconds	300	No
Ethernet Broadcast Filtering Options	RB	■ Disable, ■ From Ethernet Only ■ From Wireless Only ■ Both From Wireless and Ethernet	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

Performance Parameters

Table D-6: Performance Parameters

Parameter	Unit	Range	Default	Run-Time
Maximum Modulation Level	BU, RB	1 to 7	7	Yes
Number of HW Retries	BU, RB	1 - 15	4	Yes
Average SNR Memory Factor	BU, RB	-1 to 32	5	Yes
Burst Mode Option	BU, RB	■ Disable ■ Enable	Enable	Yes
Burst Period	BU, RB	1-10 (milliseconds)	5 (milliseconds)	Yes
Adaptive Modulation Option	BU, RB	■ Disable ■ Enable	Enable	Yes
Software Retry Support	BU, RB	■ Disable ■ Enable	Disable	Yes
Number of SW retries	BU, RB	0 - 14	3	No
Minimum Interval Between Adaptive Modulation Messages	BU, RB	1-3600 (seconds)	4 (seconds)	Yes

Service Parameters

Table D-7: Service Parameters

Parameter	Unit	Range	Default	Run-Time
User Filtering Option	RB	■ Disable ■ IP Only ■ User Defined Addresses Only ■ PPPoE Protocol Only	Disable	Yes
Set User Filter Address	RB	IP address (8 entries)	0.0.0.0 (all 8 entries)	Yes
Set User Filter Mask	RB	IP address (8 entries)	255.255.255.255 (all 8 entries)	Yes
Set User Filter Range	RB	0 – 255. 0 means that the range is not used.	0 (all 8 entries)	Yes

Security Parameters

Table D-8: Security Parameters

Parameter	Unit	Range	Default	Run-Time
Authentication Algorithm	BU, RB	■ Open system ■ Shared Key	Open system	No
Data Encryption Option	BU, RB	■ Disable ■ Enable	Disable	No
Security Mode	BU, RB	■ WEP ■ AES	WEP	No
Default Key	RB	1-4	1	No
Key # 1 to Key # 4	BU, RB	32 hexadecimal digits	0…0 (all 0=no key)	No
Promiscuous Authentication	BU	■ Disable ■ Enable	Disable	Yes (Disable after reset)