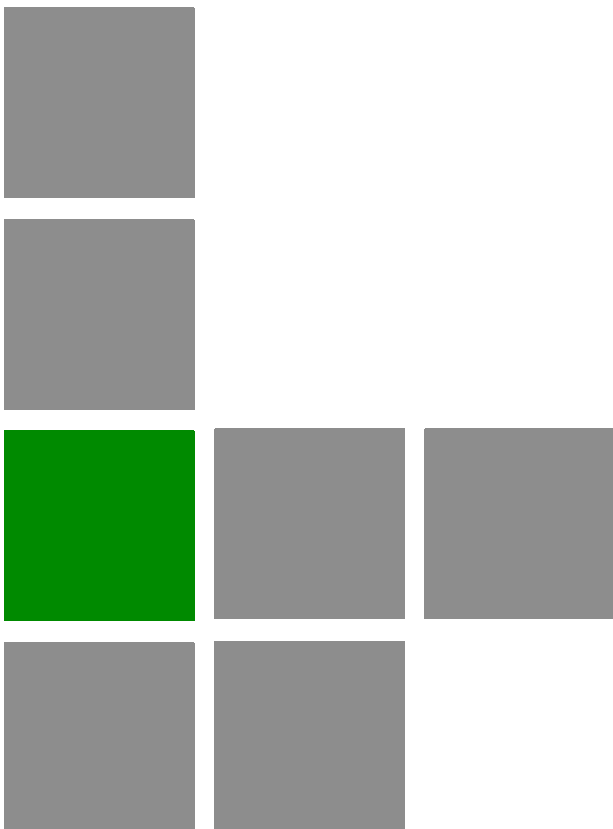


BreezeACCESS[®] EZ AU-EZ



System Manual

Software Version 5.5M
April 2009
P/N 215249

Document History

Changed Item	Description	Date
New Document	First Release	SW Version 4.5 October 2007
Correct Run-Time update of Unit Control Parameters Appendix E - Parameters Summary Section E.1.1	FTP Server IP Address, FTP Gateway IP Address, FTP User Name, FTP Password are updated in run-time (reset not required)	SW Version 5.0 November 2007
Correct Run-Time update of Air Interface Parameters Appendix E - Parameters Summary Section E.1.3	Arbitration Inter-Frame Spacing, Wireless Trap Threshold are not updated in run-time (reset is required). Frequency, DFS Required by Regulations, Frequency Subset Definition, Channel Check Time, Channel Avoidance Period, SU Waiting Option, Minimum Pulses to Detect, Channel Reuse Option, Radar Activity Assessment Period, Maximum Number of Detections in Assessment Period, are updated in run-time (reset is not required). Spectrum Analysis parameters are applicable in run-time (configured per test)	SW Version 5.0 November 2007
Update Run-Time update of Service Parameters Appendix E - Parameters Summary Section E.1.7	MIR: Downlink for SU-EZ us updated in run-time (reset is not required).	SW Version 5.0 November 2007
Unit Control Menu Section 4.2.3	Re-apply Country Codes Values option has been removed (available in Basic and Advanced Configuration, Country Code Parameters.	SW Version 5.0 November 2007
Basic Configuration Menu Section 4.2.4	Added Country Code Parameters	SW Version 5.0 November 2007
Country Code Parameters Section 4.2.6.8 , 3.1.1 , 3.1.2	New	SW Version 5.0 November 2007
Set Complete/Partial Defaults Table 4-2 , Table 4-3	Selected Country Code does not change after Set Complete/Partial Defaults	SW Version 5.0 November 2007
AIFS Section 4.2.6.2.8	Range has been increased from 1-2 to 1-50 time slots.	SW Version 5.0 November 2007
Data Encryption Option Section 4.2.6.7.2	AU with Data Encryption Option enabled can accept non-encrypted data	SW Version 5.0 December 2007

Changed Item	Description	Date
Regulation Max EIRP Table 3-2	Updated	SW Version 5.0 December 2007
Pulse Detection Sensitivity Section 4.2.6.2.14.5	Updated description	SW Version 5.0 December 2007
Antenna Gain Section 4.2.6.2.6	Range updated	SW Version 5.0 December 2007
Mixed Mode Sections 4.2.4.15 ,	New feature	SW Version 5.2 May 2008
Display Bridging and Association Info, Section 4.2.5.3.1	Updated (including changes associated with Mixed Mode)	SW Version 5.2 May 2008
Display Association Info, Section 4.2.5.3.2	Updated (including changes associated with Mixed Mode)	SW Version 5.2 May 2008
Display MIR/CIR Database, Section 4.2.5.3.4	Updated (including changes associated with Mixed Mode)	SW Version 5.2 May 2008
Link Capability, Section 4.2.5.6	Updated (including changes associated with Mixed Mode)	SW Version 5.2 May 2008
FIPS 197 Sections: 4.2.6.7 , 4.2.6.7.3 , 4.2.4.15 , Table 1-4	Support of FIPS 197 compliant encryption	SW Version 5.2 May 2008
Continuous Noise Floor Display, Section 4.2.5.4	New feature	SW Version 5.2 May 2008
Operator ESSID Section 4.2.6.2.1	New feature (Mixed Mode)	SW Version 5.2 May 2008
DFS in Universal Country Codes in the 5.4 and 5.8 GHz band. Section 4.2.6.2.2.5	New feature	SW Version 5.2 May 2008
DFS Required By Regulations	Updated default: Yes for Country Codes where required by regulations, No for Universal Country Codes in the 5.4 and 5.8 GHz bands	SW Version 5.2 May 2008
SU Waiting Option	New feature (DFS in Mixed Mode)	SW Version 5.2 May 2008

Changed Item	Description	Date
Country Code Learning By SU	New feature (Mixed Mode)	SW Version 5.2 May 2008
ATPC Section 4.2.6.2.4	New feature	SW Version 5.2 May 2008
Fairness Factor Section 4.2.6.2.7	Updated manual	SW Version 5.2 May 2008
Show Cell Distance Parameters, Section 4.2.6.2.7	Updated manual	SW Version 5.2 May 2008
Spectrum Analysis Information Display, Section 4.2.6.2.11.7	Added new parameters	SW Version 5.2 May 2008
Show Spectrum Analysis Parameters & Data, Section 4.2.6.2.11.8	Updated manual	SW Version 5.2 May 2008
Noise Floor Calculation Section 4.2.6.2.15	New feature	SW Version 5.2 May 2008
Average SNR Memory Factor, Section 4.2.6.5.6	New feature (Mixed Mode)	SW Version 5.2 May 2008
Minimum Interval Between Adaptive Modulation Messages	New feature (Mixed Mode)	SW Version 5.2 May 2008
Concatenation	New feature (Mixed Mode)	SW Version 5.2 May 2008
User Filtering, Section 4.2.6.6.1	New feature	SW Version 5.2 May 2008
Promiscuous Authentication, Section 4.2.4.15	New feature (Mixed Mode)	SW Version 5.2 May 2008
Protecting ODU Connections Section 2.3.2	New section	SW Version 5.2 May 2008
Calibration of Noise Floor Indication Section 4.2.6.2.16	New feature	SW Version 5.2 May 2008

Changed Item	Description	Date
Appendix A - BreezeACCESS-VL SUs in Mixed Mode	New Appendix	SW Version 5.2 May 2008
Initial Configuration Table 3-1	Updated to reflect all changes of version 5.2	SW Version 5.2 May 2008
Parameters that are not changed after Set Partial Factory/Operator Defaults, Table 4-3	Updated to reflect all changes of version 5.2	SW Version 5.2 May 2008
Appendix E - Parameters Summary	Updated to reflect all changes of version 5.2	SW Version 5.2 May 2008
RESET Button Functionality Section 2.4.1	Updated	SW Version 5.2 June 2008
Association Database in AU Sections 4.2.2.1, 4.2.5.3.1, 4.2.5.3.2, 4.2.6.2.9	Updated: Association SNAP from another AU is not used for removal of SU from the database.	SW Version 5.2 June 2008
MAC Address List Section 4.2.6.4.6	Corrected (supplier's OUI is 00-10-E7)	SW Version 5.2 June 2008
File Loading Appendix B	Updated: A known parameter with a value that is invalid or out of range will be ignored	SW Version 5.2 June 2008
Fairness Factor Section 4.2.6.2.7	Removed (not applicable for AU-EZ)	SW Version 5.2 July 2008
Equipment Positioning Guidelines Section 2.2	Minimum distance of 10 cm between the ODU and antenna.	SW Version 5.2 July 2008
Appendix F	Removed (Mixed Mode no longer supported)	SW Version 5.5 October 2008
Mixed mode Chapter 1 - System Description	Removed references to Mixed Mode	SW Version 5.5 October 2008
Cable supplier Table 2-1	Updated supplier name for approved category 5E Ethernet Cables from Superior Cables Ltd. to Synergy Cables Ltd.	SW Version 5.5 October 2008
Basic Parameters Table 3-1	Updated basic parameters description according to the new menu structure	SW Version 5.5 October 2008
Unit Control Menu Section 4.2.3	Updated according to new menu structure. Removed references to Mixed Mode.	SW Version 5.5 October 2008

Changed Item	Description	Date
Basic Configuration Menu Section 4.2.4	Updated according to new menu structure. New entries: ESSID, Maximum Modulation Level, Cell Distance Parameters, Country Code Parameters, Frequency Definition, Antenna Gain, Tx Control, VLAN Support	SW Version 5.5 October 2008
Bridging and Association Info Sections 4.2.5.3.1 , 4.2.5.3.2	Removed references to Mixed Mode	SW Version 5.5 October 2008
CIR/MIR Info Section 4.2.5.3.4	Removed references to Mixed Mode	SW Version 5.5 October 2008
Link Capability Section 4.2.5.6	Removed reference to Mixed Mode	SW Version 5.5 October 2008
Advanced Configuration Menu Section 4.2.6	Updated according to new menu structure. Removed references to Mixed Mode and Promiscuous Authentication.	SW Version 5.5 October 2008
DFS Mechanism update Section 4.2.6.2.2	Updated DFS mechanism for ETSI based country codes	SW Version 5.5M April 2009

Legal Rights

© Copyright 2009 Alvarion Ltd. All rights reserved.

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

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

Trade Names

Alvarion[®], BreezeCOM[®], WALKair[®], WALKnet[®], BreezeNET[®], BreezeACCESS[®], BreezeLINK[®], BreezeMAX[®], BreezeLITE[®], BreezePHONE[®], 4Motion[®], BreezeCONFIG[™], AlvariSTAR[™], AlvariCRAFT[™], MGW[™], eMGW[™] and/or other products and/or services referenced here in are either registered trademarks, trademarks or service marks of Alvarion Ltd.

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

Statement of Conditions

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

Warranties and Disclaimers

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

Exclusive Warranty

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

(b) With respect to the Firmware, Alvarion warrants the correct functionality according to the attached documentation, for a period of fourteen (14) month from

invoice date (the "Warranty Period"). During the Warranty Period, Alvarion may release to its Customers firmware updates, which include additional performance improvements and/or bug fixes, upon availability (the "Warranty"). Bug fixes, temporary patches and/or workarounds may be supplied as Firmware updates.

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

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

Disclaimer

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

(b) PURCHASER'S SOLE REMEDY FOR BREACH OF THE EXPRESS WARRANTIES ABOVE SHALL BE REPLACEMENT OR REFUND OF THE PURCHASE PRICE AS SPECIFIED ABOVE, AT ALVARION'S OPTION. TO THE FULLEST EXTENT ALLOWED BY LAW, THE WARRANTIES AND REMEDIES SET FORTH IN THIS AGREEMENT ARE EXCLUSIVE AND IN LIEU OF ALL OTHER

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

Limitation of Liability

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

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

Electronic Emission Notices

This device complies with Part 15 of the FCC rules.

Operation is subject to the following two conditions:

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

Radio Frequency Interference Statement

The AU-EZ Access Unit has been tested and found to comply with the limits for a class A digital device, pursuant to part 15 of the FCC rules and to EN 301 489-1 rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in 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. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at the user's own expense.

FCC Radiation Hazard Warning

To comply with FCC RF exposure requirement, the antenna used for this transmitter must be fixed-mounted on outdoor permanent structures with a separation distance of at least 2 meter from all persons for antennas with a gain up to 28 dBi.

Antenna Compliance Statement

This device has been designed to operate with the antennas listed in Table 1 2, and having a maximum gain of 28dbi. Antennas not included in this list or having a gain greater than 28dBi are strictly prohibited for use with this device. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the Equivalent Isotropically Radiated Power (EIRP) is not more than that permitted for successful communication.

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 BreezeACCESS AU-EZ units' components and their cables.

Caution

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

Line Voltage

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

Radio

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

effects of Radio Frequency Electromagnetic fields have not been yet fully investigated.

Outdoor Unit and Antenna Installation and Grounding

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

Disposal of Electronic and Electrical Waste



Disposal of Electronic and Electrical Waste

Pursuant to the WEEE EU Directive electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Important Notice

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

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

Any changes or modifications of equipment, including opening of the equipment not expressly approved by Alvarion Ltd. will void equipment warranty and any repair thereafter shall be charged for. It could also void the user's authority to operate the equipment.

About this Manual

This manual describes the BreezeACCESS AU-EZ Broadband Wireless Access Unit Release 5.5 and how to install, operate and manage it.

This manual is intended for technicians responsible for installing, setting up and operating the BreezeACCESS-EZ system, and for system administrators responsible for managing the system.

This manual contains the following chapters and appendices:

- **Chapter 1** - System description: Describes the BreezeACCESS-EZ system and its components.
- **Chapter 2** - Installation: Describes how to install the system components.
- **Chapter 3** - Commissioning: Describes how to configure basic parameters and validate unit operation.
- **Chapter 4** - Operation and Administration: Describes how to use the AU-EZ Monitor application for configuring parameters, checking system status and monitoring performance.
- **Appendix A** - Software Version Loading Using TFTP: Describes how to load a new software version using TFTP.
- **Appendix B** - File Download and Upload Using TFTP: Describes how to download and upload configuration files using TFTP. This procedure is also applicable for uploading country code and feature license files.
- **Appendix C** - Using the Set Factory Defaults Utility: Describes how to use the Set Factory Defaults utility to enable management access to units where wrong or unknown configuration disables regular access to the unit for management purposes.
- **Appendix D** - Preparing the indoor to outdoor cable: Provides details on preparation of the indoor to outdoor Ethernet cable.

- **Appendix E** - Parameters Summary: Provides an at a glance summary of the configuration parameters, value ranges, default values and whether the parameter is applied in run-time or only after reset.

Contents

Chapter 1 - System Description	1
1.1 Introducing BreezeACCESS-EZ	3
1.2 The AU-EZ Access Unit	5
1.3 Specifications	6
1.3.1 Radio	6
1.3.2 Configuration and Management	9
1.3.3 Standards Compliance, General	9
1.3.4 Mechanical	11
1.3.5 Connectors	11
1.3.6 Electrical	12
1.3.7 Environmental	12
Chapter 2 - Installation.....	13
2.1 Installation Requirements	15
2.1.1 Packing List	15
2.1.2 Indoor-to-Outdoor Cables	16
2.2 Equipment Positioning Guidelines	17
2.3 Installing the Outdoor Unit	18
2.3.1 Pole Mounting the Outdoor Unit	18
2.3.2 Protecting ODU Connections	19
2.3.3 Connecting the Grounding and Antenna Cables	20
2.3.4 Connecting the Indoor-to-Outdoor Cable	21
2.4 Installing the Universal IDU Indoor Unit.....	22
2.4.1 RESET Button Functionality	23
Chapter 3 - Commissioning	24
3.1 Configuring Basic Parameters	26
3.1.1 Initial Configuration	26

3.1.2	Country Code Selection	27
3.2	Transmit Power Compliance With Regulations.....	28
3.3	Operation Verification.....	29
3.3.1	Outdoor Unit Verification	29
3.3.2	Indoor Unit Verification	30
Chapter 4	- Operation and Administration	31
4.1	Working with the Monitor Program	33
4.1.1	Accessing the Monitor Program Using Telnet.....	33
4.1.2	Common Operations	34
4.2	Menus and Parameters	36
4.2.1	Main Menu	36
4.2.2	Info Screens Menu	36
4.2.3	Unit Control Menu	41
4.2.4	Basic Configuration Menu	53
4.2.5	Site Survey Menu.....	56
4.2.6	Advanced Configuration Menu.....	68
Appendix A	- Software Version Loading Using TFTP	124
Appendix B	- File Download and Upload Using TFTP	128
Appendix C	- Using the Set Factory Defaults Utility	131
Appendix D	- Preparing the Indoor to Outdoor Cable	133
Appendix E	- Parameters Summary	136
E.1	Parameters Summary	138
E.1.1	Unit Control Parameters.....	138
E.1.2	IP Parameters	140
E.1.3	Air Interface Parameters	140
E.1.4	Network Management Parameters	144
E.1.5	Bridge Parameters	144
E.1.6	Performance Parameters	147
E.1.7	Service Parameters.....	148
E.1.8	Security Parameters.....	149

Figures

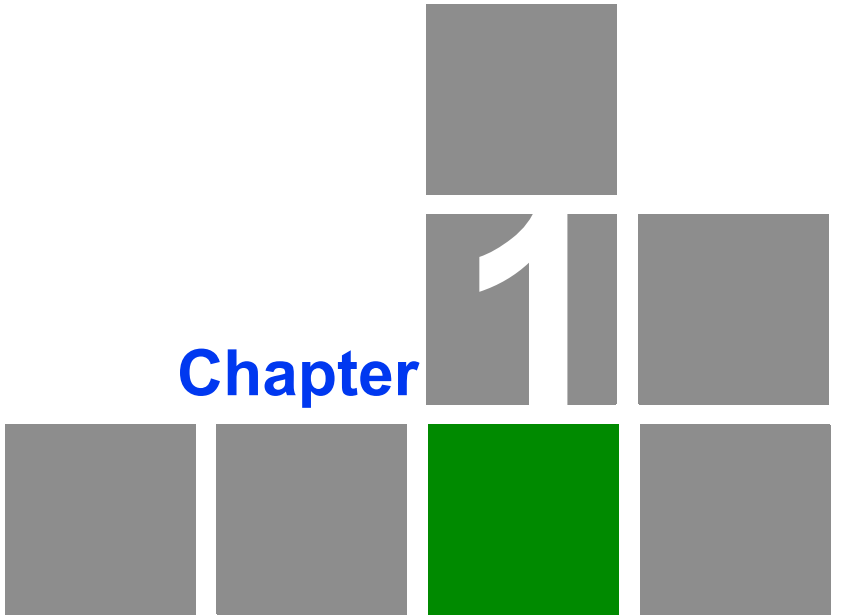
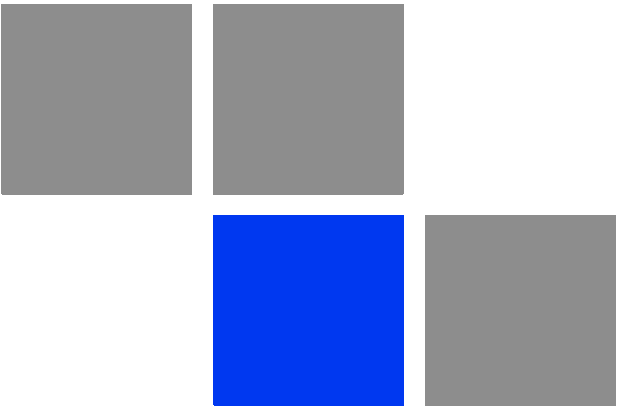
Figure 1-1: IDU and ODU.....	5
Figure 2-1: Threaded Holes/Grooves.....	18
Figure 2-2: Pole Installation Using Special Clamps	19
Figure 2-3: Bottom Panel of the ODU (shown without the sealing assembly).....	20
Figure 2-4: The Waterproof Seal.....	21
Figure 2-5: IDU PS 1073 Front Panel	22
Figure 4-1: Main Menu (Administrator Level).....	34
Figure C-1: Set Factory Defaults window.....	132
Figure D-1: Ethernet Connector Pin Assignments	134

Tables

Table 1-1: Frequency Bands	3
Table 1-2: AU-EZ Detached Antennas	5
Table 1-3: Radio Specifications	6
Table 1-4: Configuration and Management	9
Table 1-5: Standards Compliance, General	9
Table 1-6: Mechanical Specifications, Stand Alone Access Unit	11
Table 1-7: Connectors, Stand Alone Access Unit	11
Table 1-8: Electrical Specifications, Stand Alone Access Unit	12
Table 1-9: Environmental Specifications	12
Table 2-1: Approved Category 5E Ethernet Cables	16
Table 3-1: AU-EZ Basic Parameters	26
Table 3-2: Regulation Maximum EIRP	28
Table 3-3: AU-ODU LEDs	29
Table 3-4: PS1073 IDU LEDs	30
Table 4-1: Default Passwords	33
Table 4-2: Parameters that are not changed after Set Complete Factory/Operator Defaults	43
Table 4-3: Parameters that are not changed after Set Partial Factory/Operator Defaults	44
Table 4-4: Authentication and Association Process	63
Table 4-5: DFS behavior on SUs using ETSI based country codes	73
Table 4-6: Comparison between DFS implementations for various country codes on the SU	74
Table 4-7: VLAN Management Port Functionality	97
Table 4-8: VLAN Data Port Functionality - Trunk Link	98
Table 4-9: VLAN Data Port Functionality - Hybrid Link	99

Table 4-10: Recommended Maximum Modulation Level 108

Table D-1: Cable Color Codes 134



System Description

In This Chapter:

- [“Introducing BreezeACCESS-EZ” on page 3](#)
- [“The AU-EZ Access Unit” on page 5](#)
- [“Specifications” on page 6](#)

1.1 Introducing BreezeACCESS-EZ

BreezeACCESS EZ is a high capacity, IP services oriented Broadband Wireless Access system. The system provides network connections that are always on, supporting immediate access to the Internet and other IP services at high data rates.

Part of Alvarion's extended and field-proven product portfolio, BreezeACCESS EZ is an integral part of the BreezeACCESS family, one of the most widely deployed broadband wireless access systems in the world.

With capacity of up to 24 Mbps per Access Unit, BreezeACCESS EZ enables the delivery of powerful broadband services to subscribers using the SU-EZ Subscriber Units that operate as IEEE 802.11a wireless clients. With a range of up to 12 Km and lower equipment and deployment costs, BreezeACCESS EZ enables service providers to wirelessly extend their services to customers who were previously unable to afford them, while securing rapid ROI. Remote residential areas can now benefit from high-speed Internet access, Web browsing and e-mail, and advanced applications such as multi-media services.

An out-of-the-box solution with immediate available local stock, BreezeACCESS EZ enables virtually instant network expansion and simplified deployment. BreezeACCESS presents a step forward in overcoming the digital divide by providing an affordable solution that offers vast opportunities for enhanced communication, education, business, social development and improved quality of life.

BreezeACCESS EZ products operate in unlicensed frequency bands 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, the system 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.

BreezeACCESS EZ Access Units are currently available in the following frequency bands:

Table 1-1: Frequency Bands

Band	Frequency Range (GHz)
5.2	5.150 - 5.350
5.3	5.250 - 5.350
5.4	5.470 - 5.725

Table 1-1: Frequency Bands

Band	Frequency Range (GHz)
5.8	5.725 - 5.875

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

The SU-EZ CPEs support the entire range from 5.150 to 5.875 GHz with automatic frequency detection, enabling fast and simple plug-and-play installation. For details on installing, managing and using the SU-EZ CPEs, refer to the SU-A-EZ Manual.

1.2 The AU-EZ Access Unit

The Access Unit provides all the functionality necessary to communicate with the Subscriber Units and to connect to the backbone of the Service Provider.

The standalone AU-EZ Access Unit includes the following components:

- Indoor Unit (IDU)
- Outdoor Unit (ODU)
- Antenna

The IDU connects to the network through a standard IEEE 802.3 Ethernet 10/100BaseT (RJ 45) interfaces and is powered from the 110/240 VAC mains. The IDU is connected to the ODU 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 ODU outdoor unit contains the processing and radio modules and connects to an external antenna using a short RF cable.



Figure 1-1: IDU and ODU

The following antennas are available:

Table 1-2: AU-EZ Detached Antennas

Antenna	Band (GHz)	Horizontal Beam Width	Gain (dBi)
AU-Ant-5G-16-60	5.150-5.875	60°	16
AU-Ant-5G-17-90	5.150-5.875	90°	17
AU-Ant-5G-15-120	5.150-5.875	120°	15
AU-Ant-5.4G-8-Omni	5.150-5.725	360°	8
AU-Ant-5.8G-8-Omni	5.725-5.875	360°	8

* In certain countries the AU-EZ may be certified only with specific antenna(s).

1.3 Specifications

1.3.1 Radio

Table 1-3: Radio Specifications

Item	Description
Frequency ¹	<ul style="list-style-type: none">■ 5.2 GHz Family: 5.150 - 5.350 GHz■ 5.3 GHz Family: 5.250 - 5.350 GHz■ 5.4 GHz Family: 5.470 - 5.725 GHz■ 5.8 GHz Family: 5.725 - 5.875 GHz
Operation Mode	Time Division Duplex (TDD)
Channel Bandwidth	20 MHz
Central Frequency Resolution	5 MHz
Antenna Port	N-Type jack, 50 ohm
Max. Input Power (at antenna port)	-30 dBm typical
Maximum Output Power ²	21 dBm

Table 1-3: Radio Specifications

Item	Description		
Detached Antenna	<ul style="list-style-type: none"> ■ AU-Ant-5G-16-60: 16 dBi typical, 5.150-5.875 GHz, ■ 60° horizontal x 10° vertical sector antenna, vertical polarization, compliant with ETSI EN 302 326-3 V1.2.1 (2007-01) ■ AU-Ant-5G-17-90: 17 dBi typical, 5.150-5.875 GHz, ■ 90° horizontal x 6° vertical sector antenna, ■ vertical polarization, compliant with ETSI EN 302 326-3 V1.2.1 (2007-01) ■ AU-Ant-5G-15-120: 15 dBi typical, 5.150-5.875 GHz, ■ 120° horizontal x 6° vertical sector antenna, vertical polarization, compliant with ETSI EN 302 326-3 V1.2.1 (2007-01) ■ AU-Ant-5.4G-8-Omni: 8 dBi typical, 5.150-5.725 GHz, ■ 360° horizontal x 4.5° vertical, vertical polarization. ■ AU-Ant-5.8G-8-Omni: 8 dBi typical, 5.725-5.875 GHz, ■ 360° horizontal x 9° vertical, vertical polarization. 		
Sensitivity, Minimum (dBm at antenna port, PER<10%, 20 MHz bandwidth)	Modulation Level ³	Sensitivity	Minimum SNR
	1	-89 dBm	6 dB
	2	-88 dBm	7 dB
	3	-86 dBm	9 dB
	4	-84 dBm	11 dB
	5	-81 dBm	14 dB
	6	-77 dBm	18 dB
	7	-73 dBm	22 dB
8	-71 dBm	23 dB	
Modulation	OFDM modulation, 64 FFT points; BPSK, QPSK, QAM16, QAM64		

¹The actual available frequency channels and bandwidth are defined by the selected Sub-Band, which reflects the applicable regulatory constraints. For more details refer to [Section 4.2.2.4](#)).

² The actual maximum available output power for each modulation level is defined by the selected Sub-Band, which reflects the applicable regulatory constraints. For some countries the maximum power may also be affected by limitations on the maximum EIRP (also included in the Sub-Band parameters) and the Antenna Gain parameter. For more details refer to [Section 4.2.2.4](#) and to [Section 3.2](#). For information on specific HW and Country Code

limitations, see the Country Codes document.

³ Modulation Level indicates the radio transmission rate and the modulation scheme. Modulation Level 1 is for the lowest radio rate and modulation scheme.

1.3.2 Configuration and Management

Table 1-4: Configuration and Management

Item	Description
Management	<ul style="list-style-type: none"> ■ Monitor program via Telnet ■ SNMP ■ Configuration upload/download
Management Access	From Wired LAN, Wireless Link
Management access protection	<ul style="list-style-type: none"> ■ Multilevel password ■ Configuration of remote access direction (from Ethernet only, from wireless link only or from both) ■ Configuration of IP addresses of authorized stations
Security	<ul style="list-style-type: none"> ■ Authentication messages encryption option ■ Data encryption option ■ WEP 152-bit encryption ■ FIPS 197 certified encryption ■ ESSID
SNMP Agents	SNMP ver 1 client MIB II, Bridge MIB, Private MIB
Allocation of IP parameters	Configurable or automatic (DHCP client)
Software upgrade	<ul style="list-style-type: none"> ■ FTP ■ TFTP
Configuration upload/download	<ul style="list-style-type: none"> ■ FTP ■ TFTP

1.3.3 Standards Compliance, General

Table 1-5: Standards Compliance, General

Type	Standard
EMC	<ul style="list-style-type: none"> ■ FCC Part 15 class B ■ ETSI EN 300 489-1

Table 1-5: Standards Compliance, General

Type	Standard	
Safety	<ul style="list-style-type: none"> ■ UL 1950 ■ EN 60950 	
Environmental	Operation	<ul style="list-style-type: none"> ■ ETS 300 019 part 2-3 class 3.2E for indoor ■ ETS 300 019 part 2-4 class 4.1E for outdoor ■ ETS 300 019-2-2 class 2.3
	Storage	ETS 300 019-2-1 class 1.2E
	Transportation	ETS 300 019-2-2 class 2.3
Lightning protection (AU-ODU Antenna connection)	EN 61000-4-5, Class 3 (2kV)	
Radio	<ul style="list-style-type: none"> ■ FCC Part 15.247 ■ ETSI EN 300 328 ■ ETSI EN 301 893 (2003-04) 	

1.3.4 Mechanical

Table 1-6: Mechanical Specifications, Stand Alone Access Unit

Unit	Structure	Dimensions (cm)	Weight (kg)
General	An IDU (indoor unit) and an ODU (outdoor unit) connected to a detached antenna		
IDU (PS1073)	Plastic box (black), desktop or wall mountable	14 x 6.6 x 3.5	0.3
ODU	Pole or wall mountable	30.5 x 11.7 x 5.7	1.8
AU-Ant-5G-16-60	2"-3.5" pole mountable	43.6 x 25 x 1.0	2.2
AU-Ant-5G-17-90	2"-3.5" pole mountable	55 x 25 x 1.1	1.5
AU-Ant-5G-15-120	2"-3.5" pole mountable	53 x 26 x 1.1	2.5
AU-Ant-5.4G-8-Omni	2.5"-4.5" pole mountable	70 cm high, 6 cm base diameter	1.5
AU-Ant-5.8G-8-Omni	Surface or pole mountable	40 cm high, 3.2 cm base diameter	0.23

1.3.5 Connectors

Table 1-7: Connectors, Stand Alone Access Unit

Unit	Connector	Description
IDU	ETHERNET	10/100BaseT Ethernet (RJ-45) Cable connection to a PC: crossed Cable connection to a hub: straight
	RADIO	10/100BaseT Ethernet (RJ-45)
	AC IN	3-PIN AC power plug
ODU	INDOOR	10/100BaseT Ethernet (RJ-45), protected by a waterproof sealing assembly
	ANT	N-Type jack, 50 ohm, lightning protected
Antenna	RF	N-Type jack (on a 1.5m cable in the Omni-8-5.8)

1.3.6 Electrical

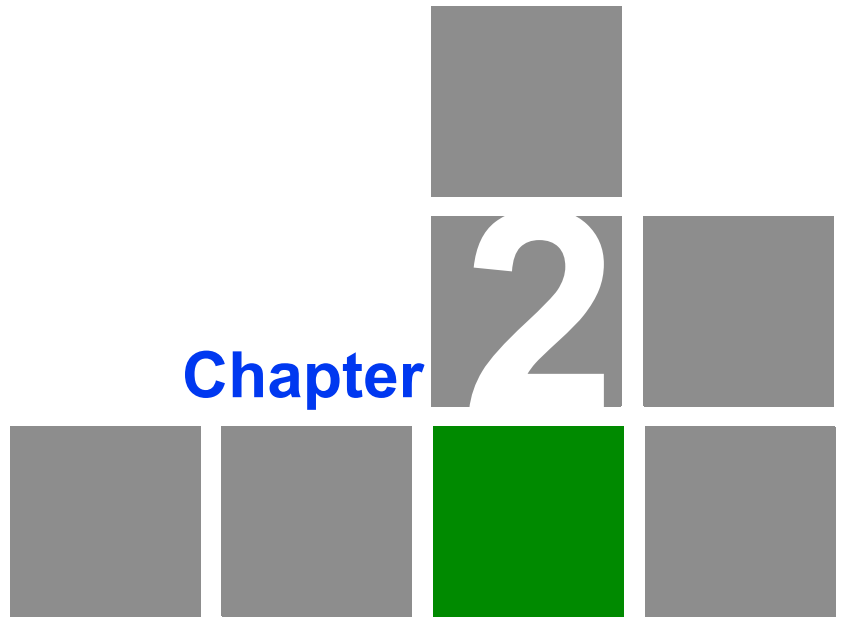
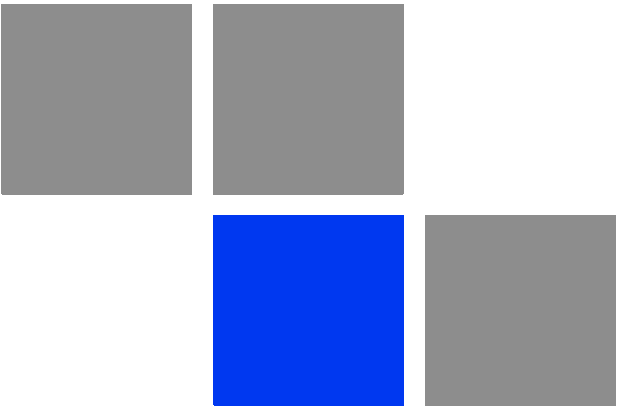
Table 1-8: Electrical Specifications, Stand Alone Access Unit

Unit	Details
General	Power consumption: 25W
IDU	AC power input: 85-265 VAC, 50-60 Hz
ODU	54 VDC from the IDU over the indoor-outdoor Ethernet cable

1.3.7 Environmental

Table 1-9: Environmental Specifications

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



Chapter 2

Installation

A decorative graphic consisting of a 3x4 grid of squares. The square in the bottom-right position is highlighted in a vibrant green color. The text "Chapter 2" is positioned to the left of the grid, and the text "Installation" is positioned below the grid.

In This Chapter:

- “Installation Requirements” on page 15
- “Equipment Positioning Guidelines” on page 17
- “Installing the Outdoor Unit” on page 18
- “Installing the Universal IDU Indoor Unit” on page 22

2.1 Installation Requirements

This section describes all the supplies required to install the AU-EZ and the items included in each installation package.

2.1.1 Packing List

2.1.1.1 AU-EZ Standalone Access Unit

- The AU-EZ installation kit includes the following components:
- DU (indoor unit) with a wall mounting kit
- Mains power cord
- ODU (outdoor unit)
- Pole mounting kit for the ODU
- IDU-ODU cable kit that includes a Waterproof Seal (Service Box) and 3 RJ-45 shielded connectors (cable is not included).

2.1.1.2 Additional Items Available from Alvarion

- IDU to ODU Category 5 Ethernet cable (available in different lengths). For more details refer to [Section 2.1.2](#)
- Antenna kit, including a 0.5 m RF cable.

2.1.1.3 Additional Installation Requirements

The following items are also required to install the AU-EZ:

- Ethernet cable (straight for connecting to a hub/switch etc.)
- 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 Telnet software and a crossed Ethernet cable
- Installation tools and materials, including appropriate means (e.g. a pole) for installing the outdoor unit and antenna.

2.1.2 Indoor-to-Outdoor Cables

NOTE



The length of the indoor-to-outdoor Ethernet cable should not exceed 90 meters. The length of the Ethernet cable connecting the indoor unit to the user's equipment, together with the length of the Indoor-to-Outdoor cable, should not exceed 100 meters.

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

Table 2-1: Approved Category 5E Ethernet Cables

Manufacturer	Part Number
Synergy Cables Ltd. www.synergy-cables.com	612098
HES Cabling Systems www.hescs.com	H5E-00481
Teldor www.teldor.com	8393204101
Southbay Holdings Limited 11th Fl., 15, Lane 347, Jong Jeng Rd. Shin Juang City, Taipei County Taiwan, R.O.C Attn: Eva Lin Tel. 886-2-2832 3339 Fax. 886-2-2206 0081 E-mail: eva@south-bay.com.tw	TSM2404A0D

NOTE



In case of missing information (product specifications, ordering information, etc.) regarding these products on the manufacturer's web site, it is highly recommended to contact the manufacturer's sales representative directly.

2.2 Equipment Positioning Guidelines

This section provides key guidelines for selecting the optimal installation locations for the various AU-EZ components.

CAUTION



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 product warranty and may expose the end user or Service Provider to legal and financial liabilities. AlvarionThe Supplier 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 should be installed as close as possible to the antenna (to ensure that the antenna's characteristics are not affected by the ODU the distance must be higher than 10 cm).
- The antenna connected to the ODU unit, should be installed so as to provide coverage to all Subscriber Units (SUs) within its service area.

NOTE



The recommended minimum distance between any two antennas serving adjacent sectors is 2 meters. The recommended minimum distance between two antennas serving opposite cells (installed back-to-back) is 5 meters.

- 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 networking equipment.

2.3 Installing the Outdoor Unit

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

NOTE



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

2.3.1 Pole Mounting the Outdoor Unit

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

- Special clamps and threaded rods are supplied with each unit. There are two pairs of threaded holes on the back of the unit, enabling to use the special clamps for mounting the unit on diverse pole diameters.
- 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.

NOTE



Be sure to mount the unit with the bottom panel, which includes the LED indicators, facing downward.

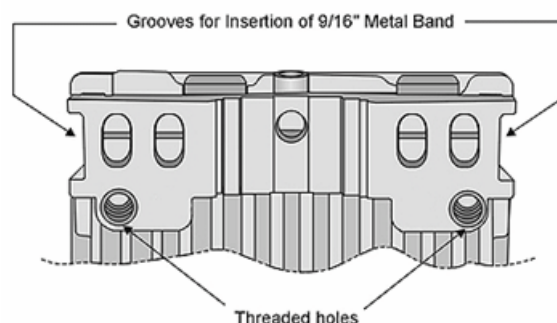


Figure 2-1: Threaded Holes/Grooves

Figure 2-2 illustrates the method of mounting an outdoor unit on a pole, using the clamps and threaded rods.

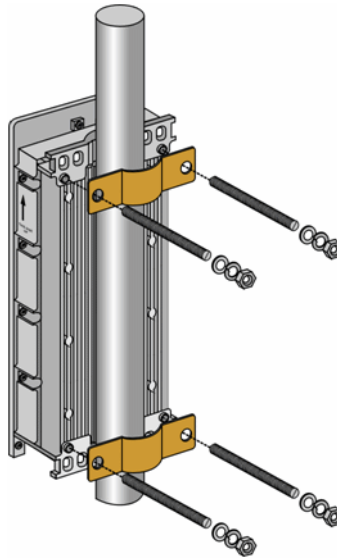


Figure 2-2: Pole Installation Using Special Clamps

NOTE



There is a groove on one end of the threaded rod. Be sure to insert the threaded rods with the grooves pointing outward, as these grooves enable you to use a screwdriver to fasten the rods to the unit.

2.3.2 Protecting ODU Connections

Use appropriate sealing material to protect the connection against moisture and humidity. Use removable sealing material, such as a tar seal, to enable future access to the connector.

NOTE



Use high quality sealing material such as Scotch® 130C Linerless Rubber Splicing Tape from 3M to ensure IP-67 compliant protection against dust and water.

Loop & tie the cable near the unit for strain relief and for routing water away from the unit: use additional cable strips to route the cable such that water can accumulate on the cable bends, away from the unit.

2.3.3 Connecting the Grounding and Antenna Cables

The Grounding screw (marked \perp) is located on the bottom panel of the outdoor unit. The Antenna RF connector (marked ∇) is located on the top panel of the ODU.



To connect the grounding cable:

- 1 Connect one end of a grounding cable to the grounding terminal and tighten the grounding screw firmly.
- 2 Connect the other end of the grounding cable to a good ground (earth) connection.



To connect the RF cable:

- 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 properly sealed to protect against rain and moisture.

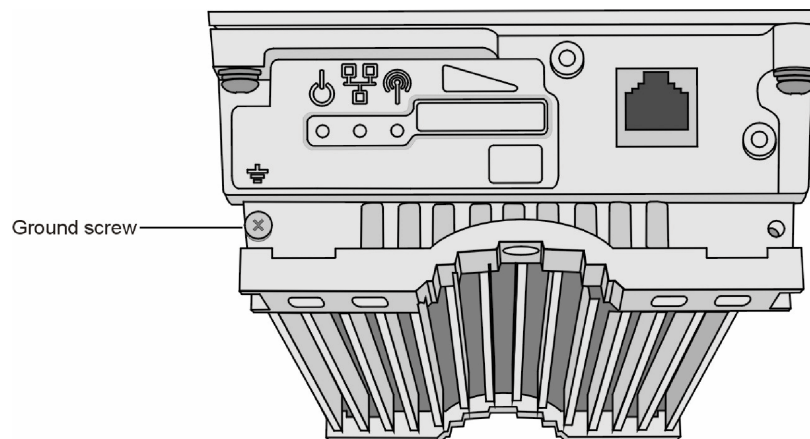


Figure 2-3: Bottom Panel of the ODU (shown without the sealing assembly)

NOTE



The MAC Address of the unit is marked on both the ODU and the indoor unit (on the bottom side of the Universal IDU). If for any reason the ODU is not used with the IDU with which it was shipped, the MAC Address of the system is in accordance with the marking on the ODU.

2.3.4 Connecting the Indoor-to-Outdoor Cable



To connect the indoor-to-outdoor cable:

- 1 Unscrew the top nut from the waterproof seal.

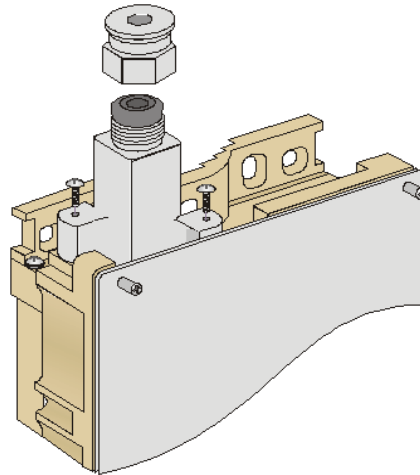


Figure 2-4: The Waterproof Seal

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

NOTE



Use only Category 5E 4x2x24# FTP outdoor cables from an approved manufacturer. See list of approved cables and length limitations in [Section 2.1.2](#).

- 3 Insert and crimp the RJ-45 connector. Refer to [Appendix D](#) for instructions on preparing the cable.
- 4 Connect the Ethernet cable to the outdoor unit RJ-45 connector.
- 5 Verify that the o-ring supplied with the waterproof seal is in place. Attach the waterproof seal to the unit, and then tighten the top nut. Make sure that the external jack of the cable is well inside the waterproof seal to guarantee a good seal.
- 6 Route the cable to the location selected for the indoor equipment.
- 7 Assemble an RJ-45 connector with a protective cover on the indoor end of the indoor-to-outdoor cable.

2.4 Installing the Universal IDU Indoor Unit

The unit can be placed on a desktop or a shelf. Alternatively, it may be wall mounted using the kit supplied with the unit.

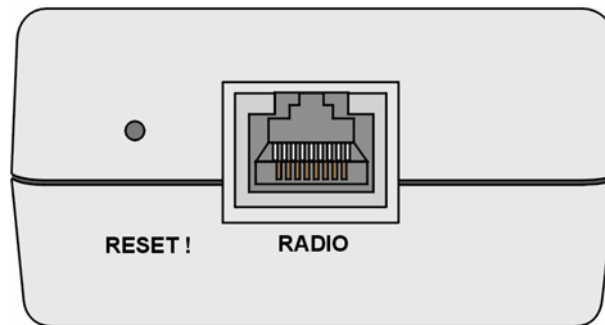


Figure 2-5: IDU PS 1073 Front Panel

The RADIO connector and RESET button are located on the front panel, the ETHERNET connector is located on the side panel and LEDs are located on the top panel.

CAUTION



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



To install the IDU:

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

NOTE



The color codes of the power cable are as follows:

Brown	Phase	~
Blue	Neutral	0
Yellow/Green	Ground	⊕

- 3 Verify that the POWER LED is lit, indicating that power is supplied to the unit.
- 4 Configure the basic parameters as described in [Section 3.1](#).

- 5 Connect the 10/100 BaseT ETHERNET connector 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).

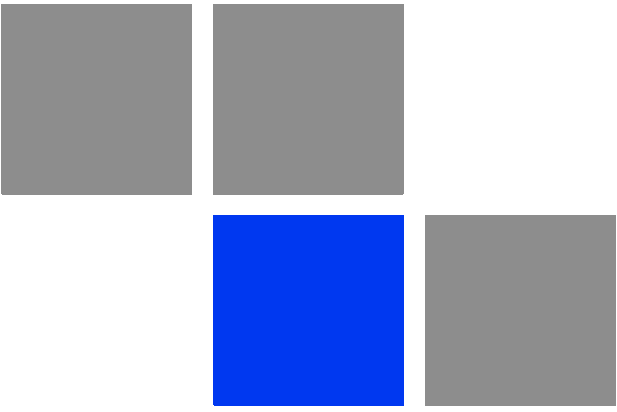
NOTE

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.

2.4.1 RESET Button Functionality

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

The RESET button can be used for setting the unit to its factory defaults. Press the button for at least 5 seconds (until the ETH LED of the IDU stops blinking): the unit will reboot with the factory default configuration.



In This Chapter:

- [“Configuring Basic Parameters” on page 26](#)
- [“Transmit Power Compliance With Regulations” on page 28](#)
- [“Operation Verification” on page 29](#)

3.1 Configuring Basic Parameters

3.1.1 Initial Configuration

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

Refer to [Section 4.1](#) for information on how to access the Monitor program using Telnet and how to use it.

The Basic Configuration menu includes all the parameters necessary for the initial installation and operation of the Access 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 [Chapter 4](#) for detailed information on the applicable parameters.

Table 3-1: AU-EZ 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	In DHCP Client
Access to DHCP	From Ethernet Only	In DHCP Client
ESSID	ESSID1	
Select Country Code	Depends on factory configuration	In Country Code Parameters. Applicable only for 5.4 and 5.8 GHz units. See Section 3.1.2 below.
Frequency	The lowest frequency in the sub band	In Frequency Definition
DFS Required By Regulations (if DFS is supported by Country Code)	Depends on Country Code	In Frequency Definition > DFS Parameters
Frequency Subset Definition	All frequencies	In Frequency Definition > DFS Parameters. Applicable only if DFS is enabled

Table 3-1: AU-EZ Basic Parameters

Parameter	Default Value	Comment
DFS Detection Algorithm	ETSI	Applicable only for Universal Country Code in 5.4 or 5.8 GHz band if DFS is enabled
ATPC Option for EZ	Disable	In ATPC Parameters
Transmit Power	Dependent on Country Code	
Tx Control	On	
Antenna Gain	According to the antenna supplied with the unit and the Country Code.	If set to "Not Set Yet", must be configured according to actual value, taking into account cable's attenuation.
Maximum Distance	0 (No Compensation)	In Cell Distance Parameters
VLAN ID-Management	65535	In VLAN Support
Authentication Algorithm	Open System	In Security Parameters. Availability of security parameters depends on support according to the country code.
Data Encryption Option	Disable	
Security Mode	WEP	
Default Multicast Key	Key 1	
Key 1 to Key 4	00.....0 (32 zeros, meaning no key)	

NOTE

Some parameters are changed to their new values only after reset (refer to [Appendix E](#) for more details). After the basic parameters are configured, the unit should be reset in order to activate the new configuration.

3.1.2 Country Code Selection

CAUTION

The selected Country Code must comply with applicable local radio regulations.

3.2 Transmit Power Compliance With Regulations

CAUTION



In regions where local radio regulations limit the maximum transmit power of the unit the installer is responsible to properly set the Antenna Gain parameter (if configurable) according to the actual antenna being used. This will limit the upper limits of the Tx Power parameter in the AU to the value of "Permitted EIRP-Antenna Gain".

The Tx Power parameter should not exceed the Permitted EIRP-Antenna Gain, according to the following table:

Table 3-2: Regulation Maximum EIRP

Country Code	Maximum EIRP (dBm)
FCC 5.3 GHz	30 (See NOTE Below)
FCC 5.4 GHz	30
ETSI 5.4 GHz	30
ETSI-F 5.4 GHz	30
Australia 5.4 GHz	30
Universal 5.4 GHz	38
FCC 5.8 GHz	36
UK 5.8 GHz	36
Australia 5.8 GHz	36
India 5.8 GHz	36
Germany 5.8 GHz	36
Universal 5.8 GHz	36

NOTE: (FCC 5.3 GHz units)

For full compliance with FCC regulations, if you wish to include one or more of frequency channels 5270, 5275 and 5330 MHz in the set of frequencies to be used, then the Transmit Power parameter in the AU should not be set to a value above "20-Antenna Gain". If there is a need to use a higher value for this parameter, these frequencies should not be used.

3.3 Operation Verification

The following sections describe how to verify the correct functioning of the ODU and IDU.

3.3.1 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.



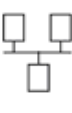
The following tables list the provided LEDs and their associated indications.

NOTE



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

Table 3-3: AU-ODU LEDs

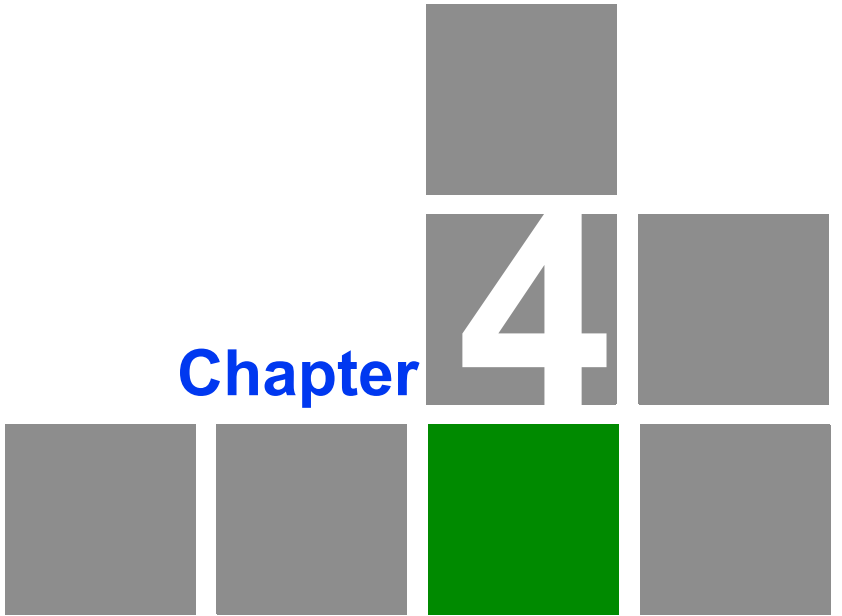
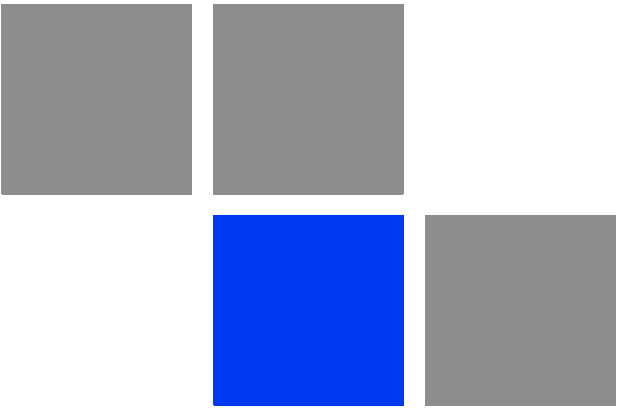
Name		Description	Functionality
W-LINK		Wireless Link Indicator	<ul style="list-style-type: none"> ■ Green - Unit is associated with one or more SUs ■ Blinking red - No associations ■ Off - Wireless link is disabled
Status		Self-test and power indication	<ul style="list-style-type: none"> ■ Green - Power is available and self-test passed. ■ Blinking Amber - Testing (not ready for operation) ■ Red - Self-test failed - fatal error
ETH		Ethernet activity/ connectivity indication	<ul style="list-style-type: none"> ■ Green -Ethernet link detected. ■ Amber - No Ethernet connectivity between the indoor and outdoor units.

3.3.2 Indoor Unit Verification

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

Table 3-4: PS1073 IDU LEDs

Name	Description	Functionality
POWER 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.	Power Indication	<ul style="list-style-type: none"> ■ Green - IDU power is OK ■ Off - No power or power failure
ETH	Self test and end-to-end Ethernet connectivity	<ul style="list-style-type: none"> ■ Off - No Ethernet connectivity has been detected between the outdoor unit and the device connected to the indoor unit. ■ Green - Self-test passed and Ethernet connection confirmed by the outdoor unit (Ethernet integrity check passed).



Operation and Administration

In This Chapter:

- [“Working with the Monitor Program” on page 33](#)
- [“Menus and Parameters” on page 36](#)

4.1 Working with the Monitor Program

4.1.1 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.

If you forgot the password, type "h" at the Access Level selection prompt. Type "Recover" at the prompt to get a challenge string consisting of 8 characters. Contact Alvarions Customer Service and give them the challenge string (after user identification) to receive a one-time password. After entering this password at the prompt, the unit will reboot with the default Administrator password (private). Three consecutive errors in entering the one-time password will invalidate it and block the monitor program. A new challenge string should be used to receive a new one-time password.

- 5 Enter your password and press **Enter**. The *Main Menu* is displayed as shown in [Figure 4-1](#). The unit type (AU-EZ) and location (if configured), SW version

number and SW release date displayed in the header vary according to the selected unit and SW version.

```
BreezeACCESS/AU-EZ/<Unit Location>
Official Release Version - <Version #>
Release Date: <Date and Time>
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 by using the "Exit Telnet" feature via SNMP or management application or by disconnecting/reconnecting power.

The display 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 menu items.

4.1.2 Common Operations

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

- Type an option number to open or activate the option. In certain cases you may need to press **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 having to reset the unit. Refer to [Appendix E](#) for *information* on which parameters are applied in run time (no need to reset the unit), and which parameters are not run-time updated (the change takes effect only after unit's reset).

4.2 Menus and Parameters

NOTE



AU-EZ is a member of the BreezeACCESS-VL family. Certain parameters available in the Monitor program are applicable only for BreezeACCESS-VL units. These parameters are marked accordingly in this manual.

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

4.2.1 Main Menu

The Main Menu enables to access the following menus, depending on your access level, as described in [Section 4.1](#).

- **Info Screens:** Provides a read only display of current parameter values. Available at all access levels.
- **Unit Control:** Enables 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 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 to activate certain tests and view various system counters. Available at the Installer and Administrator access levels.
- **Advanced Configuration:** Enables to access all system parameters, including the *Basic Configuration* parameters. Available only at the Administrator access level.

4.2.2 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 such as the ESSID are only displayed to users with Administrator access rights.

The Info Screens menu includes the following options:

- Show Unit Status
- Show Basic Configuration
- Show Advanced Configuration
- Show Country Dependent Parameters
- Show All Parameters

4.2.2.1 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 the Unit Control menu.
- **Unit Type:** AU-EZ.
- **Unit MAC Address:** The unit's unique IEEE MAC address.
- **Current Number of Associations:** The total number of SUs associated with this AU. This number may include units that are not currently active as there is no aging algorithm for associated SUs.

NOTE



An SU is only removed from the list of associated SUs under the following condition:

- The SU failed to respond to a certain number of consecutive frames transmitted by the AU and is considered to have "aged out".
- **Number of Associations Since Last Reset:** The number of SUs that have associated with the AU since the last reset, including duplicate associations with the same SU.
- **Unit Hardware Version:** The version of the outdoor unit hardware.
- **Unit Boot Version:** The version of the Boot SW.

- **Time Since Last Reset**

- **Flash Versions:**
 - » **Running from:** Shows whether the unit is running from the Main or from the Shadow Version.
 - » **Main Version File Name:** The name of the compressed file (with a ".bz" extension) of the version currently defined as the main version.
 - » **Main Version Number:** The software version currently defined as the main version.
 - » **Shadow Version File Name:** The name of the compressed file (with a ".bz" extension) of the version currently defined as the shadow (backup) version.
 - » **Shadow Version Number:** The software version currently defined as the shadow (backup) version.

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

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

- **Country Code:** The 3 or 4 digits Country Code used by the unit and its general description.

- **Ethernet Port Negotiation Mode:** The Ethernet port negotiation mode as defined in the 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 Server IP Address
 - » FTP Gateway IP Address
 - » FTP User Name
 - » FTP Password

- **FTP Software Download Parameters:** The parameters for SW download using FTP, as defined in Unit Control menu.
 - » FTP SW Version File Name
 - » FTP Source Directory

- **Configuration File Download/Upload Parameters:** The parameters for Configuration file upload/download using FTP, as defined in the Unit Control menu.
 - » Configuration File Name
 - » Configuration File Source Directory
 - » Operator Defaults File Name

- **FTP Log File Upload Parameters:** The parameters for Event Log file upload using FTP, as defined in the Unit Control menu.
 - » FTP Log File Name
 - » FTP Log File Destination Directory

- **Event Log Minimum Severity**

- **ATE Test Status:** Indicates the result of the unit's final testing in production. Should always be PASS.

- **Serial Number:** The Serial Number of the unit.

4.2.2.2 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.

4.2.2.3 Show Advanced Configuration

The Show Advanced Configuration menu enables 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.

4.2.2.4 Show Country Dependent Parameters

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

- **Country Code:** The 3 digits country code according to ISO 3166 and the country name. Some regulatory requirements apply to more than one country. In these cases the Country Code includes a 4 digits proprietary group code and the Country Group name (for example FCC).
- **Data Encryption Support:** Indicates whether data encryption is supported for the applicable country.
- **AES Encryption Support:** Indicates whether encryption using AES is supported for the applicable country. In AU-EZ AES is not supported.
- **Authentication Encryption Support:** Indicates whether authentication encryption is supported for the applicable country.

In the current release of AU-EZ, only a single Sub-Band is available. The following Sub-Band information is provided:

- **Sub-Band ID (1) and Frequencies**
- **Allowed Bandwidth:** In current release, Allowed Bandwidth is 20 MHz.
- **Regulation Max Tx Power at Antenna Port:** The maximum transmit power allowed at the antenna port of the unit.
- **Regulation Max EIRP:** The maximum allowed EIRP (Effective Isotropic Radiated Power) in dBm, or No Limit.
- **Min Modulation Level:** The lowest allowed modulation level.
- **Max Modulation Level:** The highest allowed modulation level.
- **Burst Mode:** Indicates whether Burst Mode operation is allowed.

- **Maximum Burst Duration:** If Burst Mode is allowed, this parameter displays the upper limit for the Maximum Burst Duration.
- **DFS Option:** Indicates whether the DFS (Dynamic Frequency Selection) mechanism for identification and avoidance of channels with radar activity is supported.
- **Minimum HW Revision Support:** The minimum HW revision required to support the Sub-Band.

New Country Code files can be uploaded remotely using TFTP (see Appendix B).

4.2.2.5 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 such as the ESSID are available only with Administrator access rights.

4.2.3 Unit Control Menu

The Unit Control menu enables configuring control parameters for the unit. The Unit Control menu includes the following options:

-
- Default Settings
- Change Unit Name
- Change Password
- Flash Memory Control
- Log Out Timer
- Ethernet Negotiation Mode
- Change System Location
- Event Log Menu

- Feature Upgrade
- SW Version Download
- Configuration File Upload/Download

4.2.3.1

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

4.2.3.2 Default Settings

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

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

The available options are:

- Set Defaults
- Save Current Configuration As Operator Defaults

4.2.3.2.1 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 [Section 4.2.3.12](#) option. These files can also be uploaded/downloaded remotely using TFTP (see [Appendix B](#)).

The available options in the Set Defaults submenu are:

- Set Complete Factory Defaults

- Set Partial Factory Defaults
- Set Complete Operator Defaults
- Set Partial Operator Defaults
- Cancel Current Pending Request

4.2.3.2.1.1 Set Complete Factory Defaults

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

Table 4-2: Parameters that are not changed after Set Complete Factory/Operator Defaults

Parameters Group	Parameter
Unit Control Parameters	All Passwords
	FTP Server IP address* (see note below)
	FTP Gateway IP address* (see note below)
	FTP User Name* (see note below)
	FTP Password* (see note below)
	Ethernet Port Negotiation Mode
Air Interface Parameters	Frequency
	DFS Required by Regulations
	Frequency Subset
	Antenna Gain
Country Code Parameters	Selected Country Code

NOTE



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

4.2.3.2.1.2 Set Partial Factory Defaults

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

Table 4-3: Parameters that are not changed after Set Partial Factory/Operator Defaults

Parameters Group	Parameter
Unit Control parameters	Passwords
	Ethernet Port Negotiation Mode
	FTP Server IP address
	FTP Gateway IP Address
	FTP User Name
	FTP Password
	AP Working Mode
IP Parameters	IP Address
	Subnet Mask
	Default Gateway Address
	DHCP Option
	Access to DHCP
Security Parameters	Authentication Algorithm
	Default Multicast Key
	Data Encryption Option
	Security Mode
	Key # 1 to Key # 4
Air Interface Parameters	ESSID
	Maximum Cell Distance
	Frequency
	DFS Required by Regulations
	Channel Reuse Option
	Radar Activity Assessment Period
	Maximum Number of Detections in Assessment Period
	Frequency Subset
	ATPC Option for EZ
	Transmit Power
	Tx Control
	All Noise Immunity Control parameters
	All Noise Floor Calculation parameters

Table 4-3: Parameters that are not changed after Set Partial Factory/Operator Defaults

Parameters Group	Parameter
Performance Parameters	Adaptive Modulation Decision Thresholds
Bridge Parameters	VLAN ID - Management
	MAC Address List
	MAC Address List Action
Country Code Parameters	Selected Country Code

4.2.3.2.1.3 Set Complete Operators Defaults

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

4.2.3.2.1.4 Set Partial Operator Defaults

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

4.2.3.2.1.5 Cancel Current Pending Request

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

4.2.3.2.2 Save Current Configuration As Operator Defaults

The Save Current Configuration As Operator Defaults enables defining the current configuration of the unit as the Operator Defaults configuration.

4.2.3.3 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.

4.2.3.4 Change Password

The Change Password submenu enables changing the access password(s). The Change Password submenu is available only to users with Administrator access rights.

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

Refer to [Section 4.1](#) for a list of the default passwords for each of the access levels.

4.2.3.5 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.

4.2.3.6 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.

4.2.3.7 Ethernet Negotiation Mode

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

- **Force 10 Mbps and Half-Duplex**

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

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

4.2.3.8 Change System Location

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

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

The default system location is an empty string.

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

The Event Log Menu includes the following options:

- Event Log Minimum Severity
- Display Event Log
- Erase Event Log
- Event Load Upload

- Show Log File Configuration

4.2.3.9.1 Event Log Minimum Severity

The Event Log Minimum Severity parameter 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.

4.2.3.9.2 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 according to the time at which they were generated, with the most recent event displayed last (first in - first out).

4.2.3.9.3 Erase Event Log

The Erase Event Log option enables clearing the event log.

4.2.3.9.4 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: 10.0.0.253

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

- The default is: 0.0.0.0.

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

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

The default is: vx

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

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

The default is: vx

- **Show FTP Event Log File Upload:** 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 User Name and FTP Password). This set (or relevant parts of the set) serves the SW Download procedure, the Configuration File Upload/Download procedure and the Event Log File Upload procedure. Changing any of these parameters in the menu for either procedure will automatically change its value in the menu for the other procedures.

4.2.3.9.5 Show Log File Configuration

Select this option to display the current Event Log Minimum Severity and the Total Number of Events Logged.

4.2.3.10 Feature Upgrade

The Feature Upgrade option enables to enter a license string for upgrading the unit to support new features and/or options. Upon selecting the Manual Feature Upgrade option the user will be requested to enter the license string. Each license

string is associated with a unique MAC Address and one feature/option. If the encrypted MAC Address in the license string does not match the unit's MAC Address, the string will be rejected. If there is a match, a message notifying of the new feature/option will be displayed. The unit must be reset for the change to take effect.

The license string should comprise 32 to 64 hexadecimal digits.

New Feature License files can be uploaded remotely using TFTP (see Appendix B).

In the current release of AU-EZ, no upgrade options are available.

4.2.3.11 SW Version Download

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

- **Execute FTP GET SW Version:** The Execute FTP GET SW Version option executes the SW Version FTP download according to the parameters defined below.
- **FTP SW Source Dir:** The FTP SW Source Dir option enables defining the source directory of the SW version file.

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

The default is an empty string.

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

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

The default is VxWorks.bz.

- **FTP 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: 10.0.0.253.

- **FTP Gateway IP Address:** The FTP Gateway IP Address option enables defining the FTP default gateway address.
- The default is: 0.0.0.0.
- **FTP User Name:** The FTP User Name option enables defining the user name to be used for accessing the FTP server that is hosting the SW Version file.

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

The default is: vx

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

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

The default is: vx

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

NOTE



There is one set of general FTP parameters (FTP Server IP Address, FTP Gateway IP Address, FTP 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 any procedure will automatically change its value in the menu for the other procedures.

4.2.3.12 Configuration File Upload/Download

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

- **Execute FTP GET/PUT Configuration File:** The Execute FTP GET/PUT Configuration File executes the upload/download of a Configuration file or an

Operator Defaults file according to the parameters defined below. The following options are available:

- » Execute FTP Get Configuration File (cfg)
- » Execute FTP Put Configuration File (cfg)
- » Execute FTP Get Operator Defaults File (cmr)
- » Execute FTP Put Operator Defaults File (cmr)

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

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

The default is an empty string.

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

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

The default is config.cfg.

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

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

The default is operator.cmr.

- **FTP 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: 10.0.0.253

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

The default is: 0.0.0.0.

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

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

The default is: vx

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

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

The default is: vx

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

NOTE



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

4.2.4 Basic Configuration Menu

The Basic Configuration menu includes all parameters required for the initial installation and operation of the unit. After 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:

4.2.4.1 IP Address

4.2.4.2 Subnet Mask

4.2.4.3 Default Gateway Address

4.2.4.4 ESSID

4.2.4.5 Maximum Modulation Level

4.2.4.6 Cell Distance Parameters

- Maximum Distance
- Show Cell Distance Parameters

4.2.4.7 Country Code Parameters

- Select Country Code
- Re-Apply Country Code values

4.2.4.8 DHCP Client

- DHCP Option
- Access to DHCP

Refer to [Section 4.2.6.1](#) for a description of these parameters.

4.2.4.9 Frequency Definition

- Sub Band Select
- Frequency

- DFS Parameters
 - » DFS Required by Regulations
 - » Frequency Subset Definition
 - » Channel Check Time
 - » Channel Avoidance Period
 - » Minimum Pulses to Detect
 - » Remote Radar Event Reports (ETSI Country Codes in 5.4/5.8 GHz bands)
 - » Remote Radar Events Monitoring Period (ETSI Country Codes in 5.4/5.8 GHz bands)
 - » Clear Radar Detected Channels after Reset
 - » Show DFS Setting and Data

- Show Frequency Definitions

4.2.4.10 **ATPC Parameters:**

- ATPC Option for EZ

4.2.4.11 **Transmit Power**

- Transmit Power

- Show Transmit Power Parameters

Refer to [Section 4.2.6.2](#) for a description of these parameters.

4.2.4.12 **Antenna Gain**

4.2.4.13 **Tx Control**

4.2.4.14 **VLAN Support**

- VLAN ID - Management

4.2.4.15 Security Parameters

- Authentication Algorithm
- Data Encryption Option
- Security Mode
- Default Multicast Key
- Key 1 to Key 4
- Show Security Parameters

Some or all of the security parameters may not be available in units that do not support the applicable features. Refer to [Section 4.2.6.7](#) for a description of these parameters.

4.2.4.16 Show Basic Configuration

4.2.5 Site Survey Menu

The Site Survey menu displays the results of various tests and counters for verifying the quality of the wireless link. The counters can serve for evaluating performance and identifying potential problems. There is also an extensive database for all SUs served by the AU.

The Site Survey menu includes the following options:

- Traffic Statistics
- Ping Test
- MAC Address Database
- Continuous Noise Floor Display
- Per Modulation Level Counters
- Link Capability

4.2.5.1 Traffic Statistics

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

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

4.2.5.1.1 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 medium. Frames discarded by the unit's hardware filter are not counted by the Ethernet counters. The maximum length of an Ethernet packet that can be accepted from or transmitted to the Ethernet port (excluding CRC) is 1600 bytes, including VLAN(s) for tagged packets.

The unit transmits valid data frames received from the wireless medium to the Ethernet port, as well as internally generated frames, such as responses to management queries and pings received via the Ethernet port.

The Ethernet Counters include the following statistics:

- **Total received frames via Ethernet:** The total number of frames received from the Ethernet port. This counter includes both invalid frames (with errors) and valid frames (without errors).
- **Transmitted wireless to Ethernet:** The number of frames transmitted by the unit to the Ethernet port. These are generally frames received from the wireless side, but also include frames generated by the unit itself.

4.2.5.1.2 WLAN Counters

The unit submits data frames received from the Ethernet port to the internal bridge, as well as self generated control and wireless management frames. After a unicast data frame is transmitted, the unit waits for an acknowledgement (ACK) message from the receiving unit. Some control and wireless management frames, as well as broadcast and multicast frames sent to more than one unit, are not acknowledged. If an ACK is not received after a predefined time, which is determined by the **Maximum Cell 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** parameter, the frame is dropped.

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

Data packets are routed to either the High or Low queue, according to the queue selected for them before the MIR mechanism (for more information see [Section 4.2.6.6.3](#)).

Broadcasts/multicasts are routed to the Medium 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 BreezeACCESS unit via the wireless port (as opposed to messages intended for stations behind other BreezeACCESS units), is sent to the High queue, regardless of the priority configuration.

The Wireless Link Counters include the following statistics:

- **Total transmitted frames to wireless:** The number of frames transmitted to the wireless medium. The total includes one count for each successfully transmitted unicast frame (excluding retransmissions), and the number of transmitted multicast and broadcast frames, including control and wireless management frames. In the AU, there are also separate counters for the following:
 - » Beacons
 - » Management and Other Data frames, including successfully transmitted unicast frames and multicast/broadcast data frames (excluding retransmissions, excluding Beacons)
- **Total Transmitted Unicasts:** The number of unicast frames successfully transmitted to the wireless medium, excluding retransmissions. This count is useful for calculating the rates of retransmissions or dropped frames, as only unicast frames are retransmitted if not acknowledged.

- **Total submitted frames (bridge):** The total number of data frames submitted to the internal bridge for transmission to the wireless medium. The count does not include control and wireless management frames, or retransmissions. There are also separate counts for each priority queue through which the frames were routed (High, Mid and Low).
- **Frames dropped (too many retries):** The number of dropped frames, which are unsuccessfully retransmitted without being acknowledged until the maximum permitted number of retransmissions. This count includes dropped data frames as well as dropped control and wireless management frames.
- **Total retransmitted frames:** The total number of retransmissions, including all unsuccessful transmissions and retransmissions.
- **Total transmitted concatenated frames:** Applicable only in Mixed Mode. The total number of concatenated frames transmitted successfully to the wireless medium, excluding retransmissions. There are also separate counts for concatenated frames that include one frame (Single), two frames (Double) or more than two frames (More). For more details, refer to [Section 4.2.6.5.10](#).
- **Total Tx events:** The total number of transmit events. Typically, transmission events include cases where transmission of a frame was delayed or was aborted before completion. The following additional counters are displayed to indicate the reason for and the nature of the event:
 - » Dropped: The number of dropped frames, which are unsuccessfully retransmitted without being acknowledged until the maximum permitted number of retransmissions.
 - » 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 medium. 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 frames received from the wireless medium, 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 Phy errors (unidentified signals).
 - » CRC: The number of frames received from the wireless medium 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.
 - » Other

- **Total received concatenated frames:** Applicable only in Mixed Mode. The total number of concatenated frames transmitted successfully to the wireless medium, excluding retransmissions. There are also separate counts for concatenated frames that include one frame (Single), two frames (Double) or more than two frames (More). For more details, refer to [Section 4.2.6.5.10](#).

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

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

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

4.2.5.2 Ping Test

The *Ping Test* submenu is used to control ping 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 ping.
- **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 (in ms), after which an ICMP packet is considered "request timed out". The available range is from 100 to 60,000 ms. The default value is 200 ms.
- **Start Sending:** Starts the transmission of ping frames.
- **Stop Sending:** Stops the transmission of ping frames. The test is automatically ended when 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 ping 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.

4.2.5.3 MAC Address Database

The **MAC Address Database** option in the AU displays information regarding the Subscriber Units associated with the AU, as well as bridging (forwarding) information. When DRAP is supported, it enables viewing details on the active Gateways in the sector. The following options are available:

4.2.5.3.1 Display Bridging and Association Info:

The Display Bridging and Association Info option displays a list of all the Subscriber Units and stations in the AU's Forwarding Database. For stations behind an SU, the SU's MAC address is also displayed (SU 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 SU. For these addresses, learned from the wireless port, the address of the applicable SU is also displayed (in parenthesis).
- **St (Static):** An associated SU. For these entries, the following details of the associated SU are also displayed:
 - » Unit Name: As configured in the SU (applicable only for VL SUs in Mixed Mode. For SU-EZ units the Unit Name is Not Available).
 - » SW version: The running SW version of the SU (applicable only for VL SUs in Mixed Mode. For SU-EZ units the SW version is NA).
 - » SU Unit Type
 - » Distance: The measured distance from the AU (applicable only for VL SUs in Mixed Mode. For SU-EZ units the Distance Name is Not Measured).
 - » IP Address
 - » Wi2 IP Address as defined in the SU (or 0.0.0.0 for none). For SU-EZ units the Wi2 IP Address is always none (0.0.0.0).
 - » ESSID: The ESSID used by the SU.
- **X:** An SU that is included in the Deny List.
- **Sp (Special):** 3 addresses that are always present, including:
 - » The MAC address of the AU.
 - » Alvarion's Multicast address (01-20-D6-00-00-01).
 - » 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 Subscriber Units 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 the currently associated SUs.
- 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 1021 (1024 minus the number of special Sp addresses as defined above) for Bridging Info and as specified by the Maximum Number of Associations parameter for Association Info. The default value of the Maximum Number of Associations parameter is 48.

4.2.5.3.2 Display Association Info

Displays information regarding the Subscriber Units associated with the AU. Each list entry includes the following information:

- The MAC Address of the associated Subscriber Unit
- Age in seconds, indicating the elapsed time since receiving the last packet from the Subscriber Unit.
- The value configured for the Maximum Modulation Level parameter of the Subscriber Unit. Applicable only for VL SUs in Mixed Mode.
- The Status of the Subscriber Unit. There are three options:
 - 1 Associated
 - 2 Authenticated
 - 3 Not Authenticated (a temporary status)

The various status states are described below (this is a simplified description of the association process without the effects of the Best AU algorithm).

Table 4-4: Authentication and Association Process

Message	Direction	Status in AU
SU Status: Scanning		
A Beacon with correct ESSID	AU → SU	
SU Status: Synchronized		

Table 4-4: Authentication and Association Process

Message	Direction	Status in AU
Authentication Request Not authenticated	SU → AU	
Authentication Successful	AU → SU	Authenticated
SU Status: Authenticated		
Association Request	SU → AU	Authenticated
Association Successful	AU → SU	Associated
SU Status: Associated		
ACK	SU → AU	Associated
Data Traffic	SU ↔ AU	Associated

- The SNR of the SU measured at the AU, in dB
- The RSSI of the SU measured at the AU, in dBm
- Unit Name: As configured in the SU. For SU-EZ units the Unit Name is Not Available.
- SW version: The running SW version of the SU. For SU-EZ units the SW version is NA.
- SU Unit Type
- Distance: The measured distance from the AU. For SU-EZ units the Distance Name is Not Measured).
- IP Address
- Wi2 IP Address as defined in the SU (or 0.0.0.0 for none). For SU-EZ units the Wi2 IP Address is always none (0.0.0.0).
- ESSID: The ESSID used by the SU. For SU-EZ units the displayed ESSID is null.

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 SUs.
- The maximum number of entries permitted for this table, which is specified by the **Maximum Number of Associations** parameter. The default value of the **Maximum Number of Associations** parameter is 48.

4.2.5.3.3 Display MAC Pinpoint Table

The MAC Pinpoint table provides for each of the Ethernet stations (identified by the MAC Address) connected to either the AU or to any of the SUs served by it, the identity (MAC Address) of the wireless device to which they are connected.

4.2.5.3.4 Display CIR/MIR Info

Displays information on the MIR/CIR and some other parameter for associated Subscriber Units:

- CIR TX: The Downlink CIR configured in a VL SU. Always 0 for SU-EZ.
- MIR TX: For all SU-EZ units this is the value of MIR: Downlink for SU-EZ.
- CIR RX: The Downlink CIR configured in a VL SU. Always 0 for SU-EZ.
- MIR RX: Uplink MIR configured in the SU.
- CIR Delay: This is the configured value of the Maximum Delay parameter in the SU.
- SU Name: Not Available for SU-EZ.
- Ver: NA for SU-EZ.
- Type: The Unit Type of the SU.
- IP: The IP address of the SU.

4.2.5.3.5 Gateways Table

When the DRAP option is supported, the Gateways Table provides details on the active Gateways connected to any of the SUs served by the AU. For each Gateway, the displayed information includes:

- Gateway Type (VG-1D1V, VG-1D2V, NG-4D1W)

- IP Address
- Number of Voice Calls (applicable only to Voice Gateways)

4.2.5.4 Continuous Noise Floor Display

The **Continuous Noise Floor** Display option displays continuously updated information regarding the average noise floor in the wireless link.

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

4.2.5.5 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 Per Modulation Level Counters:** Select this option to display the current values of the Per Modulation Level Counters.
- **Reset Per Modulation Level 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 **SUCCESS** and **FAILED** counts are provided for each of the associated SUs, which are identified by their MAC address.

- **SUCCESS:** The total number of successfully transmitted unicasts to the SU at the applicable modulation level.
- **FAILED:** The total number of failures to successfully transmit unicast frame to the SU during a HW Retry cycle at the applicable modulation level.

4.2.5.6 Link Capability

The Link Capability option provides information on HW and SW capabilities of associated SUs. Most of these features are not supported in SU-EZ.

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

The Link Capability submenu includes the following options:

4.2.5.6.1 Show Link Capability-General

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

- **HwVer:** the hardware version of the unit.
- **CpldVer:** The version of the Complex Programmable Logic Device (CPLD) used in the unit.
- **Country:** The 3 or 4 digits country code supported by the unit.
- **BootVer:** The Boot Version of the unit.

4.2.5.6.2 Show Link Capability-Wireless Link Configuration

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

- **ATPC Option:** Enable or Disable.
- **Adaptive Modulation Option:** Enable or Disable.
- **Burst Mode Option:** Enable or Disable.
- **Concatenation Option:** Enable or Disable.

4.2.5.6.3 Show Link Capability-Security Configuration

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

- **Security Mode:** WEP or FIPS 197.
- **Authentication Algorithm:** Shared Key or Open System.
- **Data Encryption Option:** Enable or Disable.

4.2.5.6.4 Show Link Capability by SU

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

4.2.6 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
- Security Parameters
- Country Code Parameters

4.2.6.1 IP Parameters

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

The IP Parameters menu includes the following options:

- IP Address
- Subnet Mask
- Default Gateway Address
- DHCP Client
- Show IP Parameters

4.2.6.1.1 IP Address

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

The default IP address is 10.0.0.1.

4.2.6.1.2 Subnet Mask

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

The default mask is 255.0.0.0.

4.2.6.1.3 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.

4.2.6.1.4 DHCP Client

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

The DHCP Client submenu includes the following options:

- DHCP Option
- Access to DHCP

4.2.6.1.4.1 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 [Section 4.2.6.1.4.2](#). You do not have to configure static IP parameters for the unit. DHCP messages are handled by the units as management frames.
- Select **Automatic** to cause the unit to search for a DHCP server and acquire its IP parameters from the server. If a DHCP 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 [Section 4.2.6.1.4.2](#).

The default is Disable.

4.2.6.1.4.2 Access to DHCP

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

- From Wireless Link Only
- From Ethernet Only
- From Both Ethernet and Wireless Link

The default is From Ethernet Only.

4.2.6.1.5 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**.

4.2.6.2 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.

4.2.6.2.1 ESSID

The ESSID (Extended Service Set ID) of the AU.

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

The default value is ESSID1.

NOTE



The ESSID string is case sensitive.

4.2.6.2.2 Frequency Definition

4.2.6.2.2.1 Sub-Bands and Frequency Selection

Each unit is delivered with one or more pre-configured Sub-Bands, according to the country code. These sets of parameters include also the frequencies that can be used and the bandwidth.

The parameters that determine the frequency to be used are set in the AU. If more than one Sub-Band is available, the sub-band to be used can be selected. If only one Sub-Band is supported, then the sub-band selection option is not available. The SU should be configured with a minimal set of parameters to ensure that it will be able to automatically detect and use the frequency/bandwidth used by the AU, including possible changes in this frequency (Automatic Sub Band Select feature).

To simplify the installation process the SU scans a definable frequencies subset after power-up. The defined frequencies subsets may include frequencies from more than one Sub-Band, enabling automatic detection of both frequency and bandwidth. If the Best AU feature is enabled, the SU will scan the defined subset and the operating frequency/bandwidth will be determined by the Best AU mechanism (including the optional use of the Preferred AU feature). Otherwise the SU will try to associate with the first AU it finds. If no AU is found, the SU will start another scanning cycle.

4.2.6.2.2.2 Avoiding Frequencies with Radar Activity

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

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

NOTE



Radar detection parameters that are enforced by Country Code specific regulations are editable only by users with Administrator privileges. When enabling a Country Code that requires particular DFS settings, the unit automatically applies these settings. Users with Installer privileges will be able to set a particular Country Code, but they will not be able to change its default DFS settings.

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

4.2.6.2.2.2.1 DFS implementation on the AU

The AU maintains a continuously updated database of all applicable frequencies, where each frequency is marked as Radar Free, Radar Detected or Adjacent to

Radar. The AU attempts to check a new frequency only if it is marked as Radar Free. If there is no radar activity detected, the units in the sector may use this frequency to communicate. If a radar activity was detected on a certain frequency, it will be marked in the database as a Radar Detected frequency. The frequency will remain tagged as Radar Detected for a predefined period of time called Channel Avoidance Period. After this period expires, the frequency will be marked as Radar Free.

If radar activity was detected on a certain frequency, adjacent channels should not be used as well, according to the bandwidth. For instance, if the bandwidth is 20 MHz, then if radar activity was detected in 5800 MHz, frequencies 5790 MHz and 5810 MHz should not be used as well. These frequencies are marked in the database as Adjacent to Radar, and will be treated the same as Radar Detected frequencies.

4.2.6.2.2.2 DFS implementation on the SU

When DFS is enabled on the SU, the unit uses a channel availability check mechanism that is similar to the AU's. Before associating to the AU, the SU picks a Radar Free frequency and:

- If the frequency was previously scanned and tagged as available, it immediately associates to the AU.

NOTE



Some country codes require a periodical revalidation of the Radar Free frequencies. So additionally, it might be required for the channel validation period not to have expired as well.

- If the frequency is currently tagged as Radar Free as a result of a Radar Detected status that expired, or in some cases if the Radar Free validation has expired (see the note above), the SU will initiate its own channel availability check. As a result:
 - » If no radar signal is detected, the SU associates to the AU
 - » If the SU detects a radar, it will tag the frequency in its own database as Radar Detected, notify the AU and attempt to connect on another channel

While associated, the SU also performs In-Service Monitoring, meaning that it periodically scans the operating channel for radar signals. If radar is detected, it will notify the AU and stop transmitting on the respective frequency.

ETSI requirements enforce particular implementations for the DFS functionality on CPEs. Implementations of DFS on the SU for ETSI 5.8 and ETSI 5.4 based country codes are compared in [Table 4-5](#).

Table 4-5: DFS behavior on SUs using ETSI based country codes

Feature	ETSI 5.8 based country codes	ETSI 5.4 based country codes
Applicable country codes	<ul style="list-style-type: none"> ■ ETSI 5.8 ■ Other country codes based on ETSI 5.8 (UK 5.8, Germany 5.8 and Universal 5.8 with Detection Algorithm set to ETSI) 	<ul style="list-style-type: none"> ■ ETSI 5.4 ■ Other country codes based on ETSI 5.4 (ETSI F 5.4 and Universal 5.4 with Detection Algorithm set to ETSI)
Startup	SU checks each frequency and tags it as either Radar Free or Radar Detected.	All frequencies are tagged as Radar Free by default
Operating Frequency	SU performs In-Service Monitoring and disassociates when radar is detected.	SU performs In-Service Monitoring and disassociates when radar is detected.
Radar Detected or Adjacent to Radar frequency	Expires after a predefined Channel Avoidance Period. The frequency's status is then set to Radar Free, but SUs need to check for radar before using it to associate.	Expires after a predefined Channel Avoidance Period. The frequency's status is then set to Radar Free, but SUs need to check for radar before using it to associate.
Radar Free frequency	Expires. Afterward, the frequency is still tagged as Radar Free, but SUs need to check for radar before using it to associate.	No revalidation required. SUs may use the frequency to associate at any time.

4.2.6.2.2.2.3 Channel shutdown

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

On sectors where SUs have the DFS functionality enabled, it is possible to trigger a channel shutdown even if the AU hasn't detected any radar activity on that channel. If an AU receives from the SUs a particular number of DFS notifications (Remote Radar Event Reports) in a specified period of time (Remote Radar Events Monitoring Period), it will initiate a channel shutdown on that frequency, and tag it as Radar Detected.

Typically, operators prefer to preserve the original frequency planning and to avoid moving to a new channel unless they are sure that there is a continuous

radar activity in the original channel. It should be noted that detection of radar activity does not necessarily indicate a continuous radar activity in the channel. A channel reuse algorithm enables returning to the original channel under certain conditions that indicates low radar activity on the channel.

Table 4-6: Comparison between DFS implementations for various country codes on the SU

Action	Parameter	ETSI 5.4 GHz	ETSI 5.8 GHz	Universal	FCC
When reverting the unit to factory default settings	DFS Option	According to country code definition	According to country code definition	false	According to country code definition
When upgrading from a previous software version	DFS Option	false	According to country code definition	false	Unchanged
When changing the country code	DFS Option	According to country code definition	According to country code definition	false	<ul style="list-style-type: none"> ■ AU - According to country code definition ■ SU - false
	Channel Check Time	60 sec. (600 sec. for freq. between 5600 and 5650 MHz)	60 sec. (600 sec. for freq. between 5600 and 5650 MHz)	60 sec.	60 sec.
	Channel Avoidance Period	30 min.	30 min.	30 min.	30 min.
	Minimum Pulses to Detect	4	4	4	4
	Frequency Subset Definition	According to country code definition	According to country code definition	According to corresponding ETSI 5.4/5.8	ALL

The Frequency Definition submenu includes the following options:

4.2.6.2.2.3 Sub-Bands Select

Each unit is delivered with a pre-configured Sub-Band, according to the applicable Country Code. This set of parameters includes also the frequencies that can be used.

The parameters that determine the frequency to be used are set in the AU. The SU should be configured with a minimal set of parameters to ensure that it will be

able to automatically detect and use the frequency used by the AU, including possible changes in this frequency.

4.2.6.2.2.4 Frequency

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

The range depends on the Sub-Band.

The default is the lowest frequency in the Sub-Band.

NOTE: (FCC 5.3 GHz units)

For full compliance with FCC regulations, if you wish to include one or more of frequency channels 5270, 5275 and 5330 MHz in the set of frequencies to be used, then the Transmit Power parameter in the AU should not be set to a value above "20-Antenna Gain". If there is a need to use a higher value for this parameter, these frequencies should not be used.

4.2.6.2.2.5 DFS Parameters

The DFS Parameters submenu is available only if DFS is supported by the current Sub-Band.

Note that starting on SW version 5.2, the DFS feature is supported (although disabled by default) for units using Country Codes 1060 and 1064 (Universal 5.4 GHz and Universal 5.8 GHz). When a unit using either one of these Country Codes is upgraded from a SW version lower than 5.2 the feature will not be automatically applicable. If the user wants to use the DFS feature he must re-apply the Country Code values (see [Section 4.2.6.8.2](#)). Note also that for these units, if the user changes the working sub-band the DFS Option will be automatically be set to No. For other Country Codes that support DFS when sub-band is changed the DFS Option is forced to Yes.

The DFS Parameters submenu includes the following parameters:

4.2.6.2.2.5.1 DFS Required by Regulations

The DFS Required by Regulations option enables defining whether DFS should be used for compliance with applicable local regulations. The options are Yes or No. Selection of the No option will disable the radar detection and dynamic frequency selection mechanism.

The default depends on the Country Code (No for Universal Country Codes in the 5.4 and 5.8 GHz bands, Yes for all other Country Codes that support DFS as required by applicable regulations).

4.2.6.2.2.5.2 Frequency Subset Definition

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

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

4.2.6.2.2.5.3 Channel Check Time

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

The range is 1 to 3600 seconds.

The default is 60 seconds.

NOTE



When ETSI country codes are applied, on operating channels overlapping partially or totally with frequency range 5600 - 5650 MHz, the Channel Check Time is forced to minimum 600 seconds (10 minutes).

4.2.6.2.2.5.4 Channel Avoidance Period

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

The range is 1 to 60 minutes.

The default is 30 minutes.

4.2.6.2.2.5.5 Minimum Pulses to Detect

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

The range is from 1 to 100 pulses.

The default is 4 pulses.

4.2.6.2.2.5.6 Channel Reuse Parameters

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

The Channel Reuse Parameters submenu includes the following options:

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

The default is Disable.

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

The range is 1 to 12 hours.

The default is 5 hours.

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

The range is 1 to 10 radar detections.

The default is 5 radar detections.

4.2.6.2.2.5.7 DFS Detection Algorithm

The DFS Detection Algorithm option is applicable only to units using a Universal Country Code in either the 5.4 GHz or the 5.8 GHz band (Country Codes 1060 and 1064), enabling to select the DFS detection algorithm if DFS should be enabled.

The available options are ETSI and FCC.

The default is ETSI.

4.2.6.2.2.5.8 Remote Radar Event Reports (ETSI Country Codes in 5.4/5.8 GHz bands)

If a minimum number of SUs in the sector report a radar presence on a particular channel in a limited period of time, the AU will initiate the DFS mechanism on that channel. The Remote Radar Event Reports defines this minimum number of radar reports required for the AU to initiate the DFS.

The range is 0 to 512 radar detections. When set to 0, the mechanism is disabled.

The default is 0.

4.2.6.2.2.5.9 Remote Radar Events Monitoring Period (ETSI Country Codes in 5.4/5.8 GHz bands)

The Remote Radar Events Monitoring Period defines the maximal time interval in which the Remote Radar Event Reports must be collected for the AU to initiate the DFS.

The range is 1 to 30 minutes.

The default is 30.

4.2.6.2.2.5.10 Clear Radar Detected Channels after Reset

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

The default is Disable.

4.2.6.2.2.5.11 Show DFS Settings And Data

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

4.2.6.2.2.6 Show Frequency definitions

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

4.2.6.2.3 Transmit Power

The Transmit Power submenu includes the following options:

4.2.6.2.3.1 Transmit Power

The Transmit Power parameter defines the transmit power level of the AU.

The minimum value for the Transmit Power Parameter is 10 dBm. The maximum value of the Transmit Power Parameter depends on antenna gain applicable regulations and several unit properties and parameters:

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

For information on how to view the Sub-Band supported by the unit and the supported parameters' values and options, refer to [Section 4.2.2.4](#).

Typically the maximum supported transmit power is used to provide 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, or for compliance with local regulatory requirements.

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

For each modulation level, the unit will use as transmit power the minimum between this parameter and the maximum Tx power allowed by the HW and the Country Code for the specific modulation level.

The default Transmit Power is the highest allowed value.

4.2.6.2.3.2 Show Transmit Power Parameters

This option displays the Transmit Power parameter and the current transmit power for the different modulation levels. Different power levels may be used for different modulation levels by taking into account possible HW limitations or regulatory restrictions.

4.2.6.2.4 ATPC 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 each SU according to the actual level at which it is received by the AU. To support proper operation of the system with optimal performance

and minimum interference between neighboring sectors, the ATPC algorithm should be enabled in all units.

4.2.6.2.4.0.1 ATPC Option for EZ

The ATPC Option for EZ enables or disables the Automatic Transmit Power Control (ATPC) algorithm for SU-EZ units. The ATPC feature requires Layer 3 connectivity.

The default is Disable.

4.2.6.2.4.0.2 ATPC Minimum SNR Level

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

Available values: 4 to 60 (dB).

Default value: 28 (dB).

4.2.6.2.4.0.3 ATPC Delta from Minimum SNR Level

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

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

Available values: 4 to 20 (dB).

Default value: 5 (dB) for units operating in the 5.4 and 5.8 GHz bands. 8 (dB) for units operating in the 5.2 and 5.3 GHz bands.

4.2.6.2.4.0.4 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 SU. Setting a low value for this parameter may lead to higher overhead and to an excessive rate of power level changes at the SUs. High values for this parameter increase the time it will take the SUs to reach optimal transmit power level.

Available values: 1 to 3600 seconds.

Default value: 30 seconds.

4.2.6.2.4.0.5 Show ATPC Parameters

Lists values for all the parameters in the ATPC Parameters menu.

4.2.6.2.5 Tx Control

The Tx Control option enables turning Off/On the AU's transmitter, or having the AU Tx status controlled by the status of the Ethernet port/link.

If the selected option is Ethernet Status Control, then:

- If the Ethernet link is down, the AU transmitter will be switched to Off
- If the Ethernet link is up, the AU transmitter will be switched to On.

This feature can be used during maintenance or testing to avoid transmissions using undesired parameters.

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

The default is On.

4.2.6.2.6 Antenna Gain

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

The lower limit for the Antenna Gain parameter is 0 (dBi). The upper limit for the Antenna Gain is Regulation Max EIRP + 10 in dBi (since the minimum Tx Power is -10dBm), up to a maximum of 50 (dBi). If Regulation Max EIRP is No Limit, the upper limit is 50 (dBi). A value of "Don't Care" means that the actual value is not important. A value of "Not Set Yet" means that the unit will not transmit until the actual value is configured. The unit can be configured to "Don't Care" or "Not Set Yet" only in factory. Once a value is configured, it is not possible to reconfigure the unit to either "Don't Care" or "Not Set Yet".

The default value depends on unit type. The default value for AUs that are supplied with a detached antenna is in accordance with the antenna's gain. In units supplied without an antenna the default is typically "Not Set Yet".

4.2.6.2.7 Cell Distance Parameters

The higher the distance of an SU from the AU that is serving it, the higher the time it takes for messages sent by one of them to reach the other. To ensure appropriate services to all SUs regardless of their distance from the AU while maintaining a high overall performance level, two parameters should be adapted to the distances of SUs from the serving AU:

- The time that a unit waits for a response message before retransmission (ACK timeout) should take into account the round trip propagation delay between the AU and the SU (The one-way propagation delay at 5 GHz is 3.3 microseconds per km/5 microseconds per mile.). The higher the distance from the AU of the SU served by it, the higher the ACK timeout should be.

The ACK timeout in microseconds is: $20 + \text{Distance (km)} * 2 * 3.3$ or $20 + \text{Distance (miles)} * 2 * 5$.

- To ensure fairness in the contention back-off algorithm between SUs located at different distances from the AU, the size of the time slot should also take into account the one-way propagation delay. The size of the time slot of all units in the cell should be proportional to the distance from the AU of the farthest SU served by it.

4.2.6.2.7.1 Maximum Distance

The Maximum Cell Distance parameter should be configured with the estimated distance of the farthest SU served by the AU.

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

The default is 0 (No Compensation).

4.2.6.2.7.2 Show Cell Distance Parameters

Select Show Cell Distance Parameters to view the Maximum Cell Distance parameter. It also displays the Measured Distance (the measured distance to the farthest SU, applicable only for VL SUs in Mixed Mode, Not Measured for SU-EZ units) the MAC address of the Unit with Maximum Distance (applicable only for VL SUs in Mixed Mode, 00-00-00-00-00-00 in EZ Mode or if there are only SU-EZ units in Mixed Mode).

4.2.6.2.8 Arbitration Inter-Frame Spacing (AIFS)

The time interval between two consecutive transmissions of frames is called Inter-Frame Spacing (IFS). This is the time during which the unit determines whether the medium is idle using the carrier sense mechanism. The IFS depends on the type of the next frame to be transmitted, as follows:

- SIFS (Short Inter-Frame Spacing) is used for certain frames that should be transmitted immediately, such as ACK and CTS frames. The value of SIFS is 16 microseconds.
- DIFS (Distributed coordination function Inter-Frame Spacing) is typically used for other frame types when the medium is free. If the unit decides that the medium is not free, it will defer transmission by DIFS plus a number of time slots as determined by the Contention Window back-off algorithm (see [Section 4.2.6.5.2](#)) after reaching a decision that the medium has become free.

DIFS equal SIFS plus AIFS, where AIFS can be configured to a value from 1 to 50 time slots. A unit with a lower AIFS has an advantage over units with a higher AIFS, since it has a better chance to gain access to limited wireless link resources. Typically, AIFS should be configured to two time slots. A value of 1 should only be used in one of the two units in a point-to-point link, where in the other unit the AIFS remains configured to two time slots. This ensures that the unit with AIFS configured to one has an advantage over the other unit, provided that the [Minimum Contention Window](#) (Section 4.2.6.5.2) parameter in both units is configured to 0 to disable the contention window back-off algorithm.

The available options are 1 to 50 (time slots).

The default is 2 time slots.

CAUTION



An AIFS value of 1 should only be used in point-to-point applications. Otherwise the default value of 2 must always be used. In a point-to-point link, only one unit should be configured to an AIFS value of 1. When both units need to transmit, the unit with an AIFS value of 1 will have an advantage over the unit with AIFS of 2.

4.2.6.2.9 Maximum Number of Associations

The Maximum Number of Associations parameter defines the maximum number of Subscriber Units that can be associated with the selected AU, while still guaranteeing the required quality of service to customers.

Available values range from 0 to 512.

Default value is 48.

NOTE



The Maximum Number of Associations must be set to a value of 124 or lower to enable Data Encryption. As long as Data Encryption is enabled, the Maximum Number of Associations cannot be set to a value higher than 124.

The Maximum Number of Associations Limit (512 when Data Encryption is disabled, 124 when Data Encryption is enabled) is indicated in the Show Air Interface Parameters display.

NOTE



There is no aging time for SUs. An SU is only removed from the list of associated SUs under the following condition:

- The SU failed to respond to a certain number of consecutive frames transmitted by the AU and is considered to have "aged out".

Therefore, the database of associated SUs may include units no longer associated with the AU. If the number of associated SUs has reached the value of the Maximum Number of Associations parameter, the selected AU cannot serve additional SUs. To view the current number of associated SUs, use the Display Association Info option in the MAC Address Database menu. To delete inactive SUs from the database you must either disassociate them or reset the AU.

4.2.6.2.10 Wireless Link Trap Threshold

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

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

The default is 30 (%).

4.2.6.2.11 Spectrum Analysis

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

Upon activating the spectrum analysis the unit will automatically reset. During the information-gathering period the unit will not receive nor transmit data. It also will not be able to synchronize/associate, meaning that it cannot be managed via the wireless link. At the end of the period the unit will reset automatically regaining normal operability upon start up.

The Spectrum Analysis submenu includes the following options:

4.2.6.2.11.1 Spectrum Analysis Channel Scan Period

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

Range: 2-30 seconds.

Default value: 5 seconds.

4.2.6.2.11.2 Spectrum Analysis Scan Cycles

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

Range: 1-100 cycles.

Default value: 2 cycles.

4.2.6.2.11.3 Automatic Channel Selection

The Automatic Channel selection option defines whether the AU will choose the best noise free channel upon startup after completion of the spectrum analysis

process. The selection is per analysis: when the analysis is completed it will be disabled automatically.

The default is Disable.

4.2.6.2.11.4 Spectrum Analysis Activation

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

4.2.6.2.11.5 Reset Spectrum Analysis Information

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

4.2.6.2.11.6 Spectrum Analysis Information Display

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

- **Frequency in MHz**

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

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

- **Signal Max SNR:** The maximum SNR of signals (excluding OFDM frames with the correct bandwidth) in the channel.

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

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

- **OFDM SNR:** The average SNR (in dB) of OFDM frames received in the channel.

- **OFDM Max SNR:** The maximum SNR (in dB) of OFDM frames received in the channel.

- **Noise Floor Avg:** The average Noise Floor (in dBm) calculated for the channel.

- **Noise Floor Max:** The maximum Noise Floor (in dBm) calculated for the channel.

4.2.6.2.11.7 Spectrum Analysis Information Display - Continuous

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

4.2.6.2.11.8 Show Spectrum analysis Parameters & Data

The Show Spectrum analysis Parameters & Data option enables viewing the Spectrum analysis test parameters and the last test results.

4.2.6.2.12 Lost Beacons Watchdog Threshold

When it is unable to send beacon frames for a predetermined period of time, such as in the case of interferences, the AU resets itself. The Lost Beacons Transmission Threshold parameter represents the number of consecutive lost beacons after which the unit will reset itself.

The range for this parameter is 100 - 1000 or 0. When the parameter is set to 0, this feature is disabled, i.e. internal refresh will never be performed.

The default value is 218.

4.2.6.2.13 Disassociate

The Disassociate feature enables disassociating all SUs associated with the AU or a selected SU. This feature is useful during configuration changes, enabling to force the SU(s) to re-initiate the association process, without performing a full reset.

The Disassociate submenu includes two options:

- **Disassociate All SUs**
- **Disassociate SU By MAC Address:** to disassociate a selected SU

4.2.6.2.14 Noise Immunity Control

The Adaptive Noise Immunity (ANI) mechanism, active by default, is designed to reduce the wireless physical layer errors and by that enhance the processing power of the unit, delivering higher packet processing efficiency.

This ANI mechanism is triggered by the rate of detected Physical Errors and it is modifying different thresholds affecting the immunity to specific interference types.

Due to the high processing power of the AU, enabling it to process a relatively large number of packets per second, the ANI mechanism (triggered by the number of received error packets) may not function properly in certain scenarios, resulting in link performances that are far below the expectations. The option of manually controlling the various parameters used by the ANI mechanism enables to achieve optimal performance in certain deployments where the automatic ANI mechanism may not function properly.

It is strongly recommended to consult with Alvarion experts before switching to manual mode and modifying any of the parameters.

Try switching to Manual mode if overall throughput is too low or if SUs are lost although communication conditions are sufficient for good connectivity.

In many deployments the transition to Manual mode is sufficient. If not, you may try changing the Noise Immunity Level and/or Spur Immunity Level parameters. The target is to reduce the amount of Phy Error rate reported by the unit (see **Total Rx** events on page 61). To ensure that sensitivity is not reduced too much and SUs are not lost, verify that the Age (see Display Association Info on page 64) of all SUs is below 20 seconds.

Do not activate the OFDM Weak Signal parameter if the SNR is below 26 dB without fading margin. Under normal conditions, the OFDM Weak Signal should never be activated in the AU, since the SNR of all SUs will be below 36 dB when ATPC is enabled.

The Noise Immunity Control submenu includes the following options:

4.2.6.2.14.1 Noise Immunity State Control

The Noise Immunity State Control defines the activation mode of the Adaptive Noise Immunity mechanism: Automatic or Manual. The following parameters of the Noise Immunity Control mechanism are applicable only for Manual mode.

The default is Automatic.

4.2.6.2.14.2 Noise Immunity Level

The Noise Immunity Level parameter sets the threshold for immunity against broadband interfering signals. A higher value may reduce the number of errors at the expense of reduced sensitivity.

The range is from 0 to 4. In the current version only 0 and 4 should be used.

The default is 0.

4.2.6.2.14.3 Spur Immunity Level

The Spur Immunity Level parameter sets the threshold for immunity against narrow band interfering signals such as spurious from signals at other

frequencies. A higher value may reduce the number of errors at the expense of reduced sensitivity.

The range is from 0 to 7.

The default is 0.

4.2.6.2.14.4 OFDM Weak Signal

The OFDM Weak Signal parameter sets the threshold for immunity against interfering OFDM signals.

The available options are 0 or 1. A value of 1 means that the unit will immediately reject OFDM packets with a relatively low SNR.

The default is 0.

4.2.6.2.14.5 Pulse Detection Sensitivity

The Pulse Detection Sensitivity parameter affects the Phy error count: If it is set to Low, than all Phy errors will be reported as regular Phy errors, regardless of the signal level. If it is set to High, all Phy errors with levels below a certain threshold (not accessible to the user) will be reported as regular Phy errors, while those with levels higher than the threshold will be reported as detected radar pulses.

When DFS (radar detection) is used or during a Spectrum Analysis test, the Pulse Detection Sensitivity is set internally to High (regardless of the configured value).

The default is Low.

4.2.6.2.14.6 Show Noise Immunity

Select this option to view the current values of the Noise Immunity Control parameters, and some additional parameters of the ANI mechanism.

4.2.6.2.15 Noise Floor Calculation Parameters

The Noise Floor calculation mechanism incorporated in the units is used for estimating the level of the noise floor. This value is used for estimating SNR values and for decisions on existence of signals in the channel. In some cases, especially when a very strong signal exists in neighboring channels, the noise floor calculated by the built-in mechanism may be significantly below the actual noise floor level.

Typically, the expected noise floor level (for a 20 MHz bandwidth) is -96 (dBm).

The default calculation mode is Fully Automatic, using only the built-in mechanism. If you experience problems in the wireless link such as excessively long association process or very low throughput, it may be caused by errors in noise floor calculation. In this case, it is recommended to perform a Spectrum Analysis (see [Section 4.2.6.2.11](#)) and view the Average Noise Floor values. If the

calculated Noise Floor is lower by more than 5 dB from the expected value, it is recommended to change the calculation mode to Automatic with Minimum Value, using the expected value as the minimum (Forced Value).

Note that if the SNR of received signals is very low (typically below 10 dB), it is recommended to maintain the default calculation mode (Fully Automatic). Changing the calculation mode to Automatic with Minimum Value may result in loss of connectivity with units for which the calculated SNR before the change was relatively low.

The Noise Floor Calculation Parameters submenu includes the following options:

4.2.6.2.15.1 Calculation Mode

The Calculation Mode defines the method used for calculation the Noise Floor value to be used by the device for estimating the quality of received signals. The available options are:

- **Fully Automatic:** According to the built-in noise floor calculation mechanism.
- **Forced:** The Noise Floor value is set manually to the value configured for the Forced Value parameter (see below). Typically this mode should be used only for special testing purposes.
- **Automatic with Minimum Value:** If the calculated Noise Floor using the built-in mechanism is higher than the value configured for the Forced Value parameter, the calculated value will be used. Otherwise, the Forced Value will be used.

The default option is Fully Automatic.

4.2.6.2.15.2 Forced Value

The Forced Value parameter enables configuring the Noise Floor to be used if the selected Calculation Mode is Forced. This is also the minimum value to be used if the selected Calculation Mode is Automatic with Minimum Value.

If you decided to change the calculation mode to Automatic with Minimum Value and you still experience problems in the link (long association time, exceptionally low throughput), try to improve it by increasing the configured Forced Value.

The available range is from -107 to -55 (dBm)

The default value is -96 (dBm)

4.2.6.2.15.3 Show Noise Floor Calculation

Select this option to view the current values of the Noise Floor Calculation parameters and the Noise Floor Current Value (the actual current value used by the device).

4.2.6.2.16 Calibration of Noise Floor Indication

The Calibration of Noise Floor Indication feature has been introduced to overcome possible inaccuracies in the Noise Floor Calculation mechanism. The calibrated Noise Floor Indication is used for correcting the displayed Noise Floor values versus the values that are calculated/used by the internal noise floor calculation mechanism.

The Calibration of Noise Floor Indication submenu includes the following options:

4.2.6.2.16.1 Run Calibration

Select the Run Calibration option to perform a new calibration process. Typically this should be performed for a new unit when Factory calibration is not available, whenever the bandwidth (sub-band) is being changed (not applicable for current release), or if the previous calibration process has failed.

Calibration can be performed only under the following conditions:

- The Spectrum Analyzer is not in progress
- There is no active TFTP or FTP session

If the calibration has started the unit will reset itself, will perform the calibration and after that it will reset again and return to normal mode of operation.

The calibration process may take several minutes: 6 seconds for each of the channels available in the tested sub-band, plus two resets.

If the calibration is running the user will not be able to start a spectrum analysis or a TFTP/FTP session.

If the calibration failed the results of the previous successful calibration will be kept. If the calibration passed, the new results will be used for Noise Floor Indication.

4.2.6.2.16.2 Select Calibration Option to Use

This option enables selection of the calibration option to be used by the device. The available options are None, Field and Factory.

If Factory option is available, indicating that the unit was calibrated in the factory (in the current version Factory calibration is not available), this is the option that should be used.

If Factory option is not available, a Field calibration should be performed (using the Run Calibration option), and the Field option should be selected.

The None option should be used only if the Field Calibration is repeatedly failing (see Show Noise Floor Calibration below), or if the RSSI displayed when using the Field option (following a "successful" Field calibration) is clearly inaccurate, indicating erroneous results.

The default is None.

4.2.6.2.16.3 Show Noise Floor Calibration

Select this option to view the current status and parameters of Calibration of Noise Floor Indication. The displayed parameters are:

- **Field Calibration Status:** Indicating whether a Field Calibration is being performed currently (Active or Inactive).
- **Last Field Calibration Result:** Indicating the result of the last Field calibration process (Passed, Failed or None if no Field calibration has been done).
- **Bandwidth Used for Last Field Calibration:** The bandwidth used by the device during the last Field Calibration. A new Field Calibration should be performed after changing the bandwidth (sub-band) used by the device (not applicable for current release that supports a single bandwidth).
- **Available Calibration Options:** Indicating whether Field, Factory or both Field and Factory Calibration options are available for selection.
- **Selected Calibration Option:** The currently selected Calibration Option to Use.

4.2.6.3 Network Management Parameters

The Network Management Parameters menu enables protecting the Unit from unauthorized access by defining a set of discrete IP addresses as well as IP address ranges 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. The direction from which management access is permitted can also be configured, which means that management access may be permitted from the wireless medium only, from the wired Ethernet only, or from both.

The Network Management Menu also enables managing transmission of traps, including definition of up to 10 traps destination IP addresses and the associated community strings.

The Network Management Parameters menu includes the following options:

- Access to Network Management
- Network Management Filtering
- Set Network Management IP address
- Delete a Network Management IP Address
- Delete All Network Management IP Addresses
- Set/Change Network Management IP Address Ranges
- SNMP Traps

4.2.6.3.1 Access to Network Management

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

- From Wireless Link Only
- From Ethernet Only
- From Both Ethernet and Wireless Link

The default selection is From Both Ethernet and Wireless Link.

CAUTION



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

4.2.6.3.2 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 either the Network Management IP Addresses list or in the Network Management IP

Address Ranges list, described below, and that are connected to the unit via the defined port(s). The following options are available:

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

The default selection is Disable.

4.2.6.3.3 Set Network Management IP Address

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

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

4.2.6.3.4 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.

4.2.6.3.5 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.

4.2.6.3.6 Set/Change Network Management IP Address Ranges

The Set/Change Network Management IP address Ranges menu enables defining, updating or deleting IP address ranges from which the unit can be managed if the Network Management Filtering option is enabled. This is in addition to the previous options in the Network Management menu that enable defining, updating and deleting discrete IP addresses.

The menu includes the following options:

4.2.6.3.6.1 Set/Change Network Management IP Address Range

The Set/Change Network Management IP Address Range option enables defining/updating up to 10 IP address ranges from which the unit can be managed if the Network Management Filtering option is enabled.

The default Network Management IP Address Range is 0.0.0.0 TO 0.0.0.0 (all 10 ranges).

A range can be defined using a string that includes either a start and end address, in the format "<start address> to <end address>" (example: 192.168.1.1 to 192.168.1.255), or a base address and a mask, in the format "<base address> mask <mask>" (example: 192.168.1.1 mask 255.255.255.0).

4.2.6.3.6.2 Delete Network Management IP Address Range

The Delete Network Management IP Address Range option enables deleting IP address range entries from the Network Management IP Address Ranges list.

4.2.6.3.6.3 Delete All Network Management IP Address Ranges

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

4.2.6.3.6.4 Show Network Management IP Address Ranges

Displays all the 10 available IP address ranges from which the unit can be managed when Network Management Filtering is enabled.

4.2.6.3.7 SNMP Traps

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

4.2.6.3.7.1 Send SNMP Traps

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

The default selection is Disable.

4.2.6.3.7.2 **SNMP Traps Destination IP Addresses**

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

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

4.2.6.3.7.3 **SNMP Traps Community**

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

Valid strings: Up to 8 ASCII characters.

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

4.2.6.3.7.4 **Delete One Trap Address**

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

4.2.6.3.7.5 **Delete All Trap Addresses**

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

4.2.6.3.7.6 **Show Traps Parameters**

The Show Traps Parameters displays all the 10 available IP addresses to which the SNMP Traps are to be sent and their corresponding communities.

4.2.6.3.8 **Show Network Management Parameters**

Aggregates information regarding: type of access to Network Management, Network Management IP filtering, Network Management IP addresses, activation/deactivation of SNMP traps sending, SNMP traps destination IP addresses and communities and Network Management IP address ranges.

4.2.6.4 **Bridge Parameters**

The Bridge Parameters menu provides a series of parameter sets that enables configuring parameters such as control and filtering options for certain types of transmissions, VLAN support, and denying/allowing services to specific SUs.

The Bridge Parameters menu includes the following options:

- VLAN Support
- Ethernet Broadcast/Multicast Limiter
- Bridge Aging Time

- Broadcast/Multicast Relaying
- Unicast Relaying
- MAC Address List
- Show Bridge Parameters

4.2.6.4.1 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 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 AU-EZ units supports frame routing by port information, whereby each port is connected to only one VLAN.

The VLAN Support menu includes the following parameters:

- VLAN Link Type
- VLAN ID - Management
- VLAN Forwarding
- VLAN Relaying
- VLAN Traffic Priority
- Show VLAN Parameters

4.2.6.4.1.1 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 options for some restrictions when configuring this parameter.

Table 4-7: VLAN Management Port Functionality

Action	Management Port - Internal
Receive from Ethernet I	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

4.2.6.4.1.2 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 and Trunk Link.

The default selection is Hybrid Link.

4.2.6.4.1.2.1 Trunk Link

Trunk Link transfers only tagged frames, as 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.

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

NOTE



If the **VLAN Relaying** option is enabled and you manage your devices from behind an SU unit, be sure to include the **VLAN ID-Management** value of all units to be managed when relaying via the wireless port of the AU unit, in the Relaying List. If the VLAN Forwarding option is also enabled in the AU, these VLAN IDs should also be included in the Forwarding List.

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

Table 4-8: VLAN Data Port Functionality - Trunk Link

Action	Data Port - AU and SU
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

4.2.6.4.1.2.2 Hybrid Link

Hybrid Link transfers both tagged and untagged frames, as 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 4-9 summarizes the functionality of the data port for a Hybrid link.

Table 4-9: VLAN Data Port Functionality - Hybrid Link

Action	Data Port - AU and SU
Accept from Ethernet	All
Accept from Wireless	All
Tag Insert	No
Tag Remove	No

4.2.6.4.1.3 VLAN Forwarding

The VLAN Forwarding feature is applicable only for Trunk Links. 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:

4.2.6.4.1.3.1 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.

4.2.6.4.1.3.2 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.

4.2.6.4.1.3.3 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.

4.2.6.4.1.3.4 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.

4.2.6.4.1.4 VLAN Relaying

The VLAN Relaying feature is applicable only for Trunk Links. It enables defining the VLAN ID values to be included in the VLAN Relaying List.

If the Link Type is defined as either a Trunk Link and the VLAN Relaying Support option is enabled, a frame relayed from the wireless link, which is a frame received from the wireless link that should be transmitted back through the wireless link, with a VLAN ID that is not a member of the unit's VLAN Relaying List, is discarded. If VLAN Forwarding Support is also enabled, it is necessary to configure all the VLAN IDs in the Relaying List also in the Forwarding List to enable the relaying operation.

The VLAN Relaying menu provides the following options:

4.2.6.4.1.4.1 VLAN Relaying Support

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

Available selections are Disable and Enable.

The default selection is Disable.

4.2.6.4.1.4.2 Add Relaying VLAN ID

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

Valid values are 1 to 4094.

4.2.6.4.1.4.3 Remove Relaying VLAN ID

The Remove Relaying VLAN ID option enables removing a VLAN ID from the VLAN ID Relaying List. Valid values are VID values (from 1 to 4094) that are included in the VLAN Relaying List.

4.2.6.4.1.4.4 Show VLAN ID Relaying List

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

NOTE



If the VLAN ID Relaying List is empty and the VLAN Relaying Support is Enabled, then all data frames relayed from the wireless link 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.

4.2.6.4.1.5 VLAN Traffic Priority

The VLAN Traffic Priority menu enables configuring the VLAN Priority field in applicable frames. These parameters only impact the way in which other VLAN aware devices in the network will handle the packet. All parameters that affect prioritization within the system, including VLAN-based prioritization, are located in the Traffic Prioritization menu.

The VLAN Traffic Priority menu includes the VLAN Priority - Management parameter:

4.2.6.4.1.5.1 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 0.

4.2.6.4.1.6 Show VLAN Parameters

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

4.2.6.4.2 Ethernet Broadcast/Multicast Limiter

The Ethernet Broadcast/Multicast Limiter parameters enable to limit the number of broadcast and/or multicast packets that can be transmitted per second, in order to prevent the potential flooding of the wireless medium by certain ARP attacks.

When the Ethernet Broadcast/Multicast Limiter is enabled and the specified limit is reached, the unit will send a trap. The trap will be sent periodically till the number of broadcast/multicast packets will be less than the maximum. The trap will inform the user how many packets were discarded in the last period.

The Ethernet Broadcast/Multicast Limiter menu allows viewing and setting the following parameters:

4.2.6.4.2.1 Ethernet Broadcast/Multicast Limiter Option

The Ethernet Broadcast/Multicast Limiter Option defines the limiter's functionality. The available options are:

- Disable: No limiter
- Limit only Broadcast Packets
- Limit Multicast Packets that are not Broadcasts
- Limit All Multicast Packets (including broadcast)

The default selection is Disable.

4.2.6.4.2.2 Ethernet Broadcast/Multicast Limiter Threshold (packets/sec)

The Ethernet Broadcast/Multicast Limiter Threshold defines the maximum number of packets per second that will pass the limiter when it is enabled.

The range is from 0 to 204800 (packets/second).

The default is 50 packets.

4.2.6.4.2.3 Ethernet Broadcast/Multicast Limiter Send Trap Interval (min)

The Ethernet Broadcast/Multicast Limiter Send Trap Interval defines the minimum time in minutes between two consecutive transmissions of the trap indicating the number of packets that were dropped by the limiter since the previous trap (or since the time that the limit has been exceeded).

The range is from 1 to 60 minutes.

The default is 5 minutes.

4.2.6.4.2.4 Show Ethernet Broadcast/Multicast Limiter

The Show Ethernet Broadcast/Multicast Limiter displays aggregated information regarding Ethernet Broadcast/Multicast Limiter activation, threshold and send trap interval.

4.2.6.4.3 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 BreezeACCESS units.

The available range is 20 to 2000 seconds.

The default value is 300 seconds.

4.2.6.4.4 Broadcast/Multicast Relaying

The Broadcast/Multicast Relaying option enables selecting whether the unit performs relaying of broadcasts and/or multicasts.

The available options are:

- Disable
- Broadcast/Multicast Enable
- Broadcast Enable
- Multicast Enable

If broadcast/multicast relaying is disabled, these packets are sent only to the local wired LAN and are not sent back to the wireless link. When broadcast and or multicast relaying is enabled, the relevant packets (broadcasts only, multicasts only or both broadcasts and multicasts) originating from devices on the wireless link are transmitted by the AU back to the wireless link devices, as well as to the wired LAN.

The default selection is Broadcast/Multicast Enable.

4.2.6.4.5 Unicast Relaying

The Unicast Relaying option enables selecting whether the unit performs unicast relaying. When the Unicast Relaying parameter is enabled, unicast packets originating from devices on the wireless link can be transmitted back to the wireless link devices. If disabled, these packets are not sent to the wireless link even if they are intended for devices on the wireless link. Disable the Unicast Relaying parameter only if all unicast messages from the wireless link are certain to be directed to the local wired LAN.

The default selection is Enable.

4.2.6.4.6 MAC Address List

The MAC Address List submenu enables to define a list of up to 100 MAC addresses as belonging to devices that are either granted or denied service. When the list is defined as a Deny List, the AU will not provide services to a unit whose MAC address is included in the list, enabling to disconnect units in cases such as when the user had fraudulently succeeded to configure the unit to values different from the subscription plan. When the list is defined as an Allow List, the AU will provide services only to units with a MAC address that is included in the list.

In addition, the Station Allowed Option enables defining whether an SU with any MAC address can try to associate with the AU, or only SUs with a MAC address starting with 00-10-E7 (the supplier's MAC addresses range).

The MAC Address List submenu includes the following:

4.2.6.4.6.1 Add MAC Address to List

Select Add MAC Address to List to add a MAC Address to the List.

4.2.6.4.6.2 Remove MAC Address from List

Select Remove MAC Address from List to remove a MAC Address from the List.

4.2.6.4.6.3 MAC Address List Action

This parameter defines the working mode of the MAC list:

- In the case of an Allowed list, if the MAC address is included in the list, the SU will be able to associate itself with the AU and receive permission for generating traffic; if it is not found in the list, it will still be associated but without the permission to generate traffic.

- In the case of a Deny list, if the MAC address is included in the list, the SU will be able to associate itself with the AU but will not be able to generate traffic; otherwise (if the address is not found in the list) the SU will be associated and will be able to generate traffic.

Possible options for this parameter are Deny and Allow.

The default is Deny.

4.2.6.4.6.4 Station Allowed Option

Set this parameter to Enable to allow any SU (regardless of its' MAC address) to try associating with the AU. Set it to Disable to allow only SUs whose MAC address starts with 00-10-E7 to try associating with the AU.

The default is Enabled.

4.2.6.4.6.5 Show MAC Address List

Select Show MAC Address List to display the current list of MAC Addresses included in the List and the selected List Action.

4.2.6.4.7 Show Bridge Parameters

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

4.2.6.5 Performance Parameters

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

The Performance Parameters menu includes the following parameters:

- RTS Threshold
- Min. Contention Window
- Max. Contention Window
- Multicast Modulation Level
- Maximum Modulation Level
- Average SNR Memory Factor
- Number of HW Retries
- Burst Mode
- Adaptive Modulation
- Show Performance Parameters

4.2.6.5.1 RTS Threshold

The RTS Threshold parameter defines the minimum frame size that requires an RTS/CTS (Request To Send/Clear To Send) handshake. Frames whose size is smaller than the RTS Threshold value are transmitted directly to the wireless link without being preceded with RTS frames. Setting this parameter to a value larger than the maximum frame size eliminates the RTS/CTS handshake for frames transmitted by this unit.

The available values range from 20 to 4092 bytes.

The default value is 4092. It is recommended that this value be used to ensure that RTS/CTS is never used in the AU.

4.2.6.5.2 Minimum Contention Window

The Minimum Contention Window parameter determines the time that a unit waits from the time it has concluded that there are no detectable transmissions by

other units until it attempts to transmit. The system uses a special mechanism based on detecting the presence of a carrier signal and analyzing the information contained in the transmissions of the AU to estimate the activity of other SUs served by the AU. The target is to minimize collisions in the wireless medium resulting from attempts of more than one unit to transmit at the same time.

The system uses an exponential Back-off algorithm to resolve contention between several units that want to access the wireless medium. The method requires each station to choose a random number N between 0 and a given number C each time it wants to access the medium. The unit will attempt to access the medium only after a time equal to DIFS (for more details refer to [Section 4.2.6.2.8](#)) plus N time slots, always checking if a different unit has accessed the medium before. Each time the unit tries to transmit and a collision occurs; the maximum number C used for the random number selection will be increased to the next available value. The available values are 7, 15, 31, 63, 127, 255, 511 and 1023.

The Minimum Contention Window parameter is the first maximum number C used in the back-off algorithm. The higher the number of SUs served by the same AU, the higher the Minimum Contention Window for each SU should be.

The available values are 0, 7, 15, 31, 63, 127, 255, 511 and 1023. A value of 0 means that the contention window algorithm is not used and that the unit will attempt to access the medium immediately after a time equal to DIFS.

The default value is 15.

4.2.6.5.3 Maximum Contention Window

The Maximum Contention Window parameter defines the upper limit for the maximum number C used in the back-off algorithm as described in Minimum Contention Window above.

The available values are 7, 15, 31, 63, 127, 255, 511 and 1023.

The default value is 1023.

4.2.6.5.4 Multicast Modulation Level

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

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

The minimum and maximum values for the Multicast Modulation Level are defined by the Sub-Band in use. For information on how to view the Sub-Bands supported by the unit and the supported parameters' values and options, refer to [Section 4.2.2.4](#). Currently, all Sub Bands support the entire range of modulation levels, from 1 to 8.

The default value is the lowest supported modulation level.

4.2.6.5.5 Maximum Modulation Level

When the Adaptive Modulation Algorithm (see [Section 4.2.6.5.9](#)) is enabled, it changes the modulation level dynamically according to link conditions. The purpose is to increase the probability of using the maximum possible modulation level at any given moment. Although the algorithm will avoid using modulation levels that are too high for the prevailing link conditions, it might be better 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, as higher modulation levels increase the error rate. In such conditions, a higher Maximum Modulation Level increases the number of retransmissions before the modulation level is being reduced by the Adaptive Modulation Algorithm. A high number of retransmissions reduces the overall throughput of the applicable SU as well as all other SUs associated with the same AU.

The link quality can be estimated based on the SNR measurement of the SUs at the AU, which can be viewed in the MAC Address Database option in the Site Survey menu. If the measured SNR of all Sus is less than a certain threshold, it is recommended that the maximum modulation level be decreased in accordance with Table 4 8, 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 AU is accurate only when receiving transmissions from the applicable SU.

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

The minimum and maximum values for the Maximum Modulation Level are defined by the Sub-Band in use. For information on how to view the Sub-Bands supported by the unit and the supported parameters' values and options, refer to

[Section 4.2.2.4](#). Currently, all Sub Bands support the entire range of modulation levels, from 1 to 8.

The default is the highest supported Modulation Level.

Table 4-10: Recommended Maximum Modulation Level

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

4.2.6.5.6 Average SNR Memory Factor

This parameter is not supported in the current release. The Average SNR Memory Factor defines the weight of history (value of last calculated average SNR) in the formula used for calculating the current average SNR for data frames received from SUs. This average SNR is used by the ATPC algorithm in the AU and is also included in the Adaptive Modulation Algorithm information messages transmitted by the AU and the SU. 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.

4.2.6.5.7 Number of HW Retries

The Number of HW Retries parameter defines the maximum number of times that an unacknowledged packet is retransmitted. When the Adaptive Modulation Algorithm is disabled, a frame will be dropped when the number of unsuccessful retransmissions reaches this value. For details on the effect of this parameter when the Adaptive Modulation Algorithm is enabled, refer to [Section 4.2.6.5.9](#).

The available values range is from 1 to 14.

The default value is 10.

4.2.6.5.8 Burst Mode

Burst mode provides an increased throughput by reducing the overhead associated with transmissions in the wireless medium. In a burst transmission the inter-frame spacing is reduced and unicast data frames are transmitted without any contention period (burst mode is not activated on broadcasts/multicasts).

The Burst Mode is available only if Burst Mode is supported by the Sub-Band in use. For information on how to view the Sub-Bands supported by the unit and the supported parameters' values and options, refer to [Section 4.2.2.4](#).

4.2.6.5.8.1 Burst Mode Option

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

The default is Enable.

4.2.6.5.8.2 Burst Mode Time Interval

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

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

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

4.2.6.5.9 Adaptive Modulation

The Adaptive Modulation Algorithm enables adapting the modulation level of transmitted data to the prevailing conditions of the applicable radio link. The algorithm provides Access Units with simultaneous, adaptive support for multiple Subscriber Units at different modulation levels, as transmission's modulation level decisions are made separately for each associated SU.

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

The decisions made by the Adaptive Modulation Algorithm for the modulation level to be used are based on multiple parameters, including the SNR of received signals, time that has passed since last transmission to the relevant unit, and the recent history of successful and unsuccessful transmissions and retransmissions. The decision algorithm is performed separately for each SU.

The transmission/retransmission mechanism operates as follows:

- 1 Each new frame (first transmission attempt) will be transmitted at a modulation level selected by the Adaptive Modulation algorithm.
- 2 If first transmission trial has failed, the frame will be retransmitted at the same modulation level up to the maximum number of retransmission attempts defined by the Number of HW Retries parameter.

The Adaptive Modulation Parameters menu includes the following parameters:

4.2.6.5.9.1 Adaptive Modulation Option

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

The default selection is Enable.

4.2.6.5.9.2 Adaptive Modulation Decision Thresholds

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

The default is Normal.

4.2.6.5.9.3 Show Adaptive Modulation Parameters

The Show Adaptive Modulation Parameters option displays aggregated information regarding: Adaptive Modulation activation and decision thresholds and the minimum interval between Adaptive Modulation messages.

4.2.6.5.10 Show Performance Parameters

The Show Performance Parameters option displays aggregated information regarding: RTS threshold, min/max contention window, maximum modulation level, multicast modulation level, number of HW retries, average SNR memory factor, burst mode activation, minimum interval between adaptive modulation messages, adaptive modulation decision thresholds.

4.2.6.6 Service Parameters

The Service Parameters menu enables defining user filtering, MIR/CIR parameters, traffic prioritization parameters and DRAP parameters.

The Service Parameters menu includes the following options:

- User Filtering Parameters
- MIR and CIR Parameters
- Traffic Prioritization
- DRAP Parameters
- Show Service Parameters

4.2.6.6.1 User Filtering Parameters

The User Filtering Parameters submenu enables defining the IP addresses of user devices authorized to access the wireless medium 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:

4.2.6.6.1.1 User Filtering Option

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

- **Disable** - no filtering.
- **IP Protocol Only** - only IP Protocol packets pass.
- **User Defined Addresses Only** - only IP frames from/to IP addresses included in the User Filter Addresses list pass.

The default selection is Disable.

4.2.6.6.1.2 Set/Change Filter IP Address Range

The Set/Change Filter IP Address Ranges option enables defining/updating up to 8 IP address ranges to/from which IP frames are to pass if the User Defined Addresses Only option is selected in the User Filtering Option parameter.

The default Filter IP Address Range is 0.0.0.0 TO 0.0.0.0 (all 8 ranges).

A range can be defined using a string that includes either a start and end address, in the format "<start address> to <end address>" (example: 192.168.1.1 to

192.168.1.255), or a base address and a mask, in the format "<base address> mask <mask>" (example: 192.168.1.1 mask 255.255.255.0).

4.2.6.6.1.3 Delete Filter IP Address Range

The Delete Filter IP Address Range option enables deleting IP address range entries from the Filter IP Address Ranges list.

4.2.6.6.1.4 Delete All User Filtering Entries

The Delete All User Filtering Entries option enables deleting all entries from the Filter IP Address Ranges list.

4.2.6.6.1.5 DHCP Unicast Override Filter

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

The default is Disable DHCP Unicast.

4.2.6.6.1.6 PPPoE Override Filter

When user filtering is activated, PPPoE packets are filtered out. The PPPoE Override Filter option enables to overcome this problem. When enabled, PPPoE packets pass, overriding the user filtering mechanism.

The default is Disable.

4.2.6.6.1.7 Show User Filtering Parameters

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

4.2.6.6.2 MIR and CIR Parameters

The MIR (Maximum Information Rate) value specifies the maximum data rate available for burst transmissions, provided such bandwidth is available.

Under normal conditions, the actual Information Rate (IR) is between the 0 to the MIR values, based on the formula $IR = K * MIR$.

In this formula K is between 0 and 1 and is determined dynamically by the AU according to overall demand in the cell and the prevailing conditions that influence the performance of the wireless link.

The MIR/CIR algorithm uses buffers to control the flow of data. To balance the performance over time, a special Burst Duration algorithm is employed to enable higher transmission rates after a period of inactivity. If no data intended for a certain SU is received from the Ethernet port during the last N seconds, the unit is allowed to transmit to this destination N times its allowed IR value without any

delay. For example, if the Burst Duration is set to 0.5 second (or more), then after a period of inactivity of 0.5 seconds up to $128 \text{ Kbits} \times 0.5 = 64 \text{ Kbits}$ may be transmitted to a unit whose IR is 128 Kbps, without any delay (provided overall conditions in the wireless link allow this burst).

The MIR and CIR parameters are

4.2.6.6.2.1 **MIR: Downlink for SU-EZ**

Sets the Maximum Information Rate of the downlink from the AU to each of the SUs.

Available values range is from 128 to 12032 (Kbps)

The default value is 12032 (Kbps).

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

4.2.6.6.2.2 **Maximum Burst Duration**

Sets the maximum time for accumulating burst transmission rights according to the Burst Duration algorithm.

Available values range from 0 to 2000 (milliseconds).

The default value is 5 (milliseconds), enabling a maximum burst of $(0.005 \times \text{CIR})$ Kbps after a period of inactivity of 5 milliseconds or more.

4.2.6.6.2.3 **Graceful Degradation Limit**

Sets the limit on using the graceful degradation algorithm. In cases of over demand, the performance of all SUs is degraded proportionally to their CIR ($\text{IR} = (100\% - k\%) \times \text{CIR}$). The graceful degradation algorithm is used as long as $k \geq K$, where K is the Graceful Degradation Limit. Beyond this point, the simple "brute force" algorithm is used. The Graceful Degradation Limit should be raised in proportion to the demand in the cell. The higher the expected demand in a cell, the higher the value of the Graceful Degradation Limit. Higher demand can be expected in cases of significant over subscription and/or in deployments where a high number of subscribers are in locations without proper communication with the AU at the highest data rate.

The available values range from 0 to 70 (%).

The default value is 70 (%).

4.2.6.6.2.4 **MIR Only Option**

When the MIR Only Option is enabled, it forces the MIR/CIR algorithm to use MIR values only. The MIR/CIR algorithm determines the actual information rate for each of the supported SUs under changing conditions of demand, based on the

configured CIR and MIR values. When the MIR Only Option is enabled, the MIR/CIR algorithm is overridden and forced to operate with MIR values only. For example, the AU attempts to enable all SUs to transmit/receive information at the specified MIR value. When enabled, the graceful degradation algorithm, which is a part of the CIR/MIR algorithm, is also disabled.

The default is Enable.

4.2.6.6.2.5 **MIR Threshold Percent**

Sets the threshold of wireless link utilization above which the MIR/CIR algorithm is activated.

The range is from 0 to 100 (%).

The default is 50%.

4.2.6.6.2.6 **Show MIR/CIR Parameters**

Displays the current values of the MIR and CIR parameters.

4.2.6.6.3 **Traffic Prioritization**

Each packet that is received from the Ethernet port is placed in either the High or Low queue, according to the Traffic Prioritization parameters. When the MIR/CIR mechanism decides that a packet must be sent, the High priority queue will be checked first. If the High priority queue is not empty, the first element in the queue is forwarded to the MIR/CIR mechanism. Packets from the Low priority queue will be forwarded only if the High queue is empty.

The prioritization of the packets is done using different classifiers:

- VLAN Priority
- ToS Priority: IP Precedence or DSCP
- UDP and/or TCP ports

Each one of these classifiers can be activated/deactivated. If more than one classifier is activated, the priority of each packet will be determined by the highest priority given to it by the active classifiers.

The Traffic Prioritization menu enables activating/deactivating each of these classifiers, and configuring the applicable parameters for each classifier.

The Low Priority Traffic Minimum Percent parameter can be used to prevent starvation of low priority traffic by ensuring that a certain number of low priority packets are transmitted even at the expense of high priority traffic.

NOTE

Note that in BreezeACCESS-EZ traffic prioritization is available only for downlink transmissions. As a result, in most applications there is no meaningful benefit to this feature.

4.2.6.6.3.1 VLAN Traffic Prioritization

This menu accesses the VLAN Priority Threshold. The VLAN Priority Threshold is applicable for Trunk and Hybrid Links. It enables defining the value of the VLAN Priority Threshold. If the VLAN Priority field in a tagged frame is higher than the value of the VLAN Priority Threshold parameter, the packet will be routed to the High queue. If the VLAN Priority field is lower than or equal to this value, the packet will be transferred to the Low queue (unless it is assigned a High priority by another classifier).

Valid values range from 0 to 7.

The default value is 7, which means that all packets get a low priority (equivalent to disabling the VLAN-based classifier).

4.2.6.6.3.2 ToS Prioritization

The ToS Prioritization parameters enable defining prioritization in accordance with either the 3 IP Precedence bits in the IP header in accordance with RFC 791, or the 6 DSCP (Differentiated Services Code Point) bits in accordance with RFC 2474. The ToS Prioritization menu includes the following parameters:

4.2.6.6.3.2.1 ToS Prioritization Option

The ToS Prioritization Option defines whether ToS-based prioritization is enabled or disabled. The following options are available:

- Disable
- Enable IP Precedence (RFC791) Prioritization
- Enable DSCP (RFC2474) Prioritization

The default is Disable.

4.2.6.6.3.2.2 IP Precedence Threshold

The IP Precedence Threshold parameter is applicable when the ToS Prioritization Option is set to Enable IP Precedence (RFC791) Prioritization. If the value of the 3 IP Precedence bits in the IP header is higher than this threshold, the packet is

routed to the High queue. If the value is lower than or equal to this threshold, the packet will be transferred to the Low queue (unless it is assigned a High priority by another classifier).

Valid values range from 0 to 7.

The default value is 4.

4.2.6.6.3.2.3 DSCP Threshold

The DSCP Threshold parameter is applicable when the ToS Prioritization Option is set to Enable DSCP (RFC2474) Prioritization. If the value of the 6 DSCP bits in the IP header is higher than this threshold, the packet is routed to the High queue. If the value is lower than or equal to this threshold, the packet will be routed to the Low queue (unless it is assigned a High priority by another classifier).

Valid values range from 0 to 63.

The default value is 32.

4.2.6.6.3.3 UDP/TCP Port Ranges Traffic Prioritization

The UDP/TCP Port Ranges Traffic Prioritization parameters enable defining prioritization in accordance with the UDP and/or TCP destination port ranges. The UDP/TCP Port Ranges Traffic Prioritization menu includes the following parameters:

4.2.6.6.3.3.1 UDP/TCP Port Ranges Prioritization Option

The UDP/TCP Port Ranges Prioritization Option defines whether port ranges based prioritization is enabled or disabled. The following options are available:

- Disable
- Enable Only for UDP
- Enable Only for TCP
- Enable for both UDP and TCP

The default is Disable.

4.2.6.6.3.3.2 UDP Port Ranges

The UDP Port Ranges menu enables defining port ranges to be used as priority classifiers when the UDP/TCP Port Ranges Prioritization Option is set to either Enable Only for UDP or Enable for both UDP and TCP. All packets whose destination is included in the list will be routed to the High queue. All other packets will be routed to the Low queue (unless they were assigned a High priority by another classifier).

The UDP Port Ranges menu includes the following options:

- **UDP RTP/RTCP Prioritization:** Voice over IP is transported using Real Time Protocol (RTP). The Real Time Control Protocol (RTCP) is used to control the RTP. When an application uses RTP/RTCP, it chooses for destination ports consecutive numbers: RTP port is always an even number, and the port with the odd number following it will be assigned to RTCP.

If the administrator selects to prioritize only the RTP packets, then all the packets with an odd numbered destination port will always have Low priority. The packets with an even number for destination port will receive High priority, if the port number is included in the specified ranges.

If the administrator selects to prioritize both RTP and RTCP packets, then all packets whose destination port number is included is in the specified ranges will receive High priority.

The available options are:

- » RTP & RTCP
- » RTP Only

The default is RTP & RTCP

- **Add UDP Port Ranges:** This option enables adding UDP port ranges to the list of priority port numbers. The list can include up to 64 ranges. It is possible to add discrete port numbers and/or ranges. In ranges, a hyphen is used to separate between start and end port numbers. A comma is used to separate between entries.

For example: 8900,9000-9005,9010,9016-9017.

- **Delete UDP Port Ranges:** This option enables deleting UDP port ranges from the list of priority port numbers. It is possible to delete discrete port numbers and/or ranges. In ranges, a hyphen is used to separate between start and end port numbers. A comma is used to separate between entries.

For example: 8900,9000-9005,9010,9016-9017.

- **Delete All UDP Port Ranges:** This option enables deleting all UDP port ranges from the list of priority port numbers.

- **Show UDP Port Ranges:** Select this option to view the current UDP RTP/RTCP Prioritization option and the list of UDP Port Ranges.

4.2.6.6.3.3.3 TCP Port Ranges

The TCP Port Ranges menu enables defining port ranges to be used as priority classifiers when the UDP/TCP Port Ranges Prioritization Option is set to either Enable Only for TCP or Enable for both UDP and TCP. All packets whose destination is included in the list will be routed to the High queue. All other packets will be routed to the Low queue (unless they were assigned a High priority by another classifier).

The TCP Port Ranges menu includes the following options:

- **TCP RTP/RTCP Prioritization:** Voice over IP is transported using Real Time Protocol (RTP). The Real Time Control Protocol (RTCP) is used to control the RTP. When an application uses RTP/RTCP, it chooses for destination ports consecutive numbers: RTP port is always an even number, and the port with the odd number following it will be assigned to RTCP.

If the administrator selects to prioritize only the RTP packets, then all the packets with an odd numbered destination port will always have Low priority. The packets with an even number for destination port will receive High priority, if the port number is included in the specified ranges.

If the administrator selects to prioritize both RTP and RTCP packets, then all packets whose destination port number is included in the specified ranges will receive High priority.

The available options are:

- » RTP & RTCP
- » RTP Only

The default is RTP & RTCP

- **Add TCP Port Ranges:** This option enables adding TCP port ranges to the list of priority port numbers. The list can include up to 64 ranges. It is possible to add discrete port numbers and/or ranges. In ranges, a hyphen is used to separate between start and end port numbers. A comma is used to separate between entries. For example: 8900,9000-9005,9010,9016-9017.

- **Delete TCP Port Ranges:** This option enables deleting TCP port ranges from the list of priority port numbers. It is possible to delete discrete port numbers and/or ranges. In ranges, a hyphen is used to separate between start and end port numbers. A comma is used to separate between entries.

For example: 8900,9000-9005,9010,9016-9017.

- **Delete All TCP Port Ranges:** This option enables deleting all TCP port ranges from the list of priority port numbers.
- **Show TCP Port Ranges:** Select this option to view the current TCP RTP/RTCP Prioritization option and the list of TCP Port Ranges.

4.2.6.6.3.4 Low Priority Traffic Minimum Percent

This feature ensures that a certain amount of low priority packets, specified by the Low Priority Traffic Minimum Percent (LPTMP) parameter, is transmitted even at the expense of high priority traffic.

The mechanism guarantees a low priority traffic with a rate of $LPTMP * RT / 100$, where RT symbolizes the allowed traffic rate. The high priority traffic will thus not be able to exceed $(100-LPTMP) * RT / 100$. If the system receives high priority traffic at a rate higher than this figure, some high priority packets will be discarded.

The range is between 0 and 100 (%).

The default value is 0 (%).

4.2.6.6.3.5 Show Traffic Prioritization

The Show Traffic Prioritization option displays aggregated information regarding current values of the parameters that affect the traffic prioritization.

4.2.6.6.4 DRAP Parameters

DRAP (Dynamic Resources Allocation Protocol) is a protocol that can be used by the AU to communicate with Voice and Networking Gateways connected to SUs served by it, enabling identification of these Gateways. It also enables managing voice calls made by Voice Gateways (VG).

The AU keeps track of all current voice calls and, upon receiving from a VG a request for a new call, compares the current number of calls to the maximum allowed number. If the maximum allowed number has been reached, the AU will not confirm the request.

The DRAP feature is applicable only for gateways that support DRAP.

The following is a description of DRAP-related parameters:

4.2.6.6.4.1 DRAP Support

The DRAP Support option enables or disables the DRAP feature that offers the possibility of identifying the connected Gateways and limiting the maximum number of voice calls made by Voice Gateways in a cell.

The default option is Enable.

4.2.6.6.4.2 UDP Port

The UDP Port parameter defines the UDP port used by the DRAP protocol.

The range is from 8000 to 8200.

The default value is 8171.

4.2.6.6.4.3 Maximum Number of Voice Calls

The Maximum Number of Voice Calls parameter sets the maximum number of active calls in the cell.

The range is between 0 and 255.

The default value is 40.

4.2.6.6.4.4 DRAP TTL (seconds)

The DRAP TTL parameter sets the time between two consecutive Allocation Requests from the Gateways. The Allocation requests are used to identify the existence of an active Gateway. In Voice Gateways they also include information about the current number of voice calls and requests for new calls.

The range is between 1 and 255 (seconds).

The default value is 10 (seconds).

4.2.6.6.4.5 Number of Active Voice Calls

This option shows the current number of active voice calls in the cell.

4.2.6.6.4.6 Show Drap Parameters

The Show Drap Parameters option displays current and runtime values of the DRAP parameters.

4.2.6.6.5 Show Service Parameters

Displays the current values of the Service Parameters.

4.2.6.7 Security Parameters

BreezeACCESS-EZ systems can support encryption of authentication messages and/or data frames using one of the following encryption standards:

- WEP Wired Equivalent Privacy algorithm. WEP is defined in the IEEE 802.11 Wireless LAN standard and is based on the RSA's RC4 encryption algorithm.
- FIPS 197 is certified for compliance with Federal Information Processing Standards. It provides encryption and message integrity in one solution and implements the Advanced Encryption Standard using Rijndael block cipher.

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

- Authentication Algorithm
- Data Encryption Option
- Security Mode
- Default Multicast Key
- Key # 1 to Key # 4
- Show Security Parameters

4.2.6.7.1 Authentication Algorithm

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

- **Open System:** An SU configured to Open System can only associate with an AU also configured to Open System. In this case, the authentication encryption algorithm is not used.
- **Shared Key:** The authentication messages are encrypted. An SU configured to use a Shared Key can only be authenticated by an AU configured to use a Shared Key, provided the applicable Key (which means both the key number and its content) in the AU is identical to the key selected as the Default Key in the SU.

The default is Open System.

NOTE



The AU and all the SUs it serves should be configured to the same Authentication Algorithm option. Mixed operation is not supported.

An AU with Data Encryption Option enabled can accept non-encrypted data frames.

4.2.6.7.2 Data Encryption Option

The Data Encryption Option allows enabling or disabling data encryption. When enabled, all data frames, including frames using management protocols such as Telnet, FTP, TFTP, SNMP, DHCP and ICMP, are encrypted.

The default is Disable.

NOTE



- The AU and all the SUs it serves should be configured to the same Data Encryption Option. Mixed operation is not supported.
- The Maximum Number of Associations must be set to a value of 124 or lower to enable Data Encryption. As long as Data Encryption is enabled, the Maximum Number of Associations cannot be set to a value higher than 124. The Maximum Number of Associations Limit (512 when Data Encryption is disabled, 124 when Data Encryption is enabled) is indicated in the Show Air Interface Parameters display.

4.2.6.7.3 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 FIPS 197.

The default is WEP.

4.2.6.7.4 Default Multicast Key

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

Available values range from 1 to 4.

The default is KEY # 1.

4.2.6.7.5 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 part of the encryption/decryption process. The Keys must be set before the Shared Key authentication algorithm or Data Encryption can be used. To support proper operation, both the Key # and the content must be identical at both sides of a wireless link.

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

The default for all 4 Keys is 000...0 (a string of 32 zeros), which means it is a key used by the unit.

4.2.6.7.6 Show Security Parameters

The Show Security Parameters option displays aggregated information regarding: authentication algorithm, data encryption activation, security mode and the default multicast key.

4.2.6.8 Country Code Parameters

4.2.6.8.1 Select Country Code

The Select Country code option enables changing the Country Code used by the unit. In the current release this option is applicable only to units in the 5.4 and 5.8 GHz bands.

The default Country Code is set in factory according to the destination country.

CAUTION



The selected Country Code must comply with applicable local radio regulations.

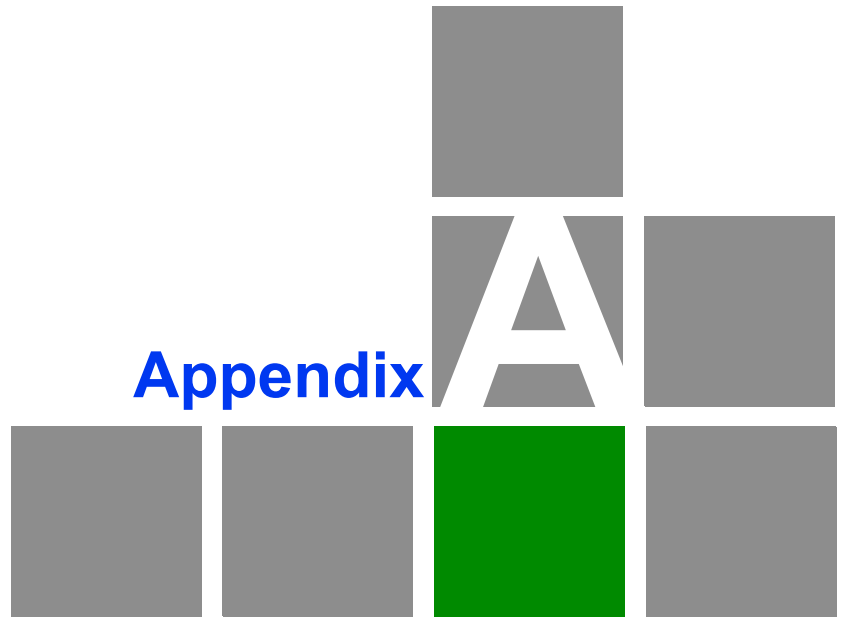
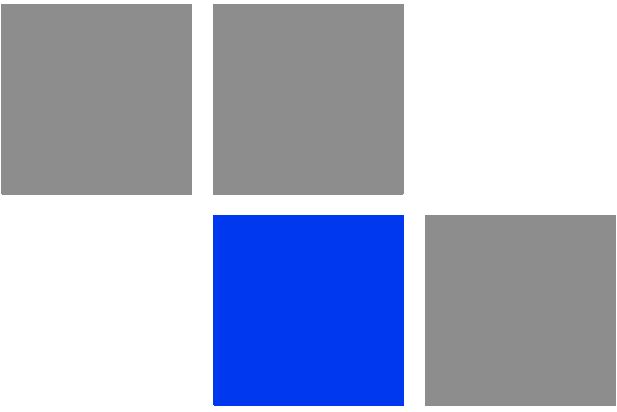
4.2.6.8.2 Re-apply Country Code Values

After loading a new SW version with any changes in the relevant Country Code, the Re-apply Country Code Values option must be activated for the changes to take effect. Following activation of this feature, the unit must be reset to fully apply the changes.

NOTE



Following activation of the Re-apply Country Code Values option, all parameters that are affected by the Country Code (frequency parameters, transmit power parameters, DFS operation, modulation level parameters, burst mode parameters) revert to their factory default values and must be re-configured.



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 is in the structure *aX_Y_Z.bz*, where *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 *a5_0_15.bz* to an AU whose IP address is *206.25.63.65*: *tftp -i 206.25.63.65 put a5_0_15.bz private.bz*
- 9 When the loading is complete, the following message is displayed, indicating completion of the TFTP process:

```
SW download 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 the current Main versions. The unit will also reject a file designated for a different unit type.
- 11 The FLASH memory can store two software versions. One version is called *Main* 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
=====
```

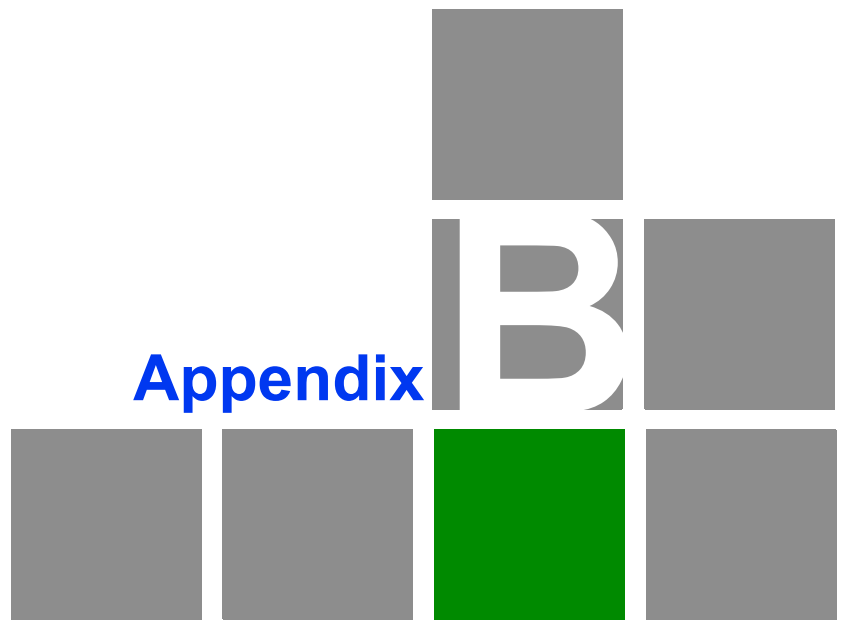
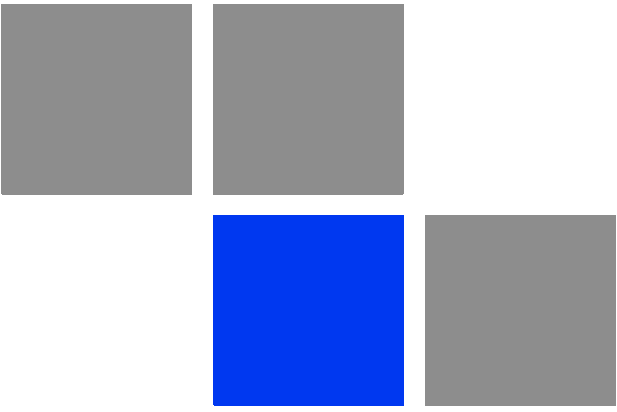
```
Running from                :main version
Main Version File Name      :A4_5_16.bz
Main Version Number         :4.5.16
Shadow Version File Name    :A5_0_15.bz
```

Shadow Version Number: :5.0.15

NOTE



After loading a new SW version with any changes in the relevant Country Code, these changes must be applied by activation the Re-apply Country Code Values option in the Unit Control Menu. Note that following activation of the Re-apply Country Code Values option, all parameters that are affected by the Country Code (frequency parameters, transmit power parameters, DFS operation, modulation level parameters, burst mode parameters) revert to their factory default values and must be re-configured.



File Download and Upload Using TFTP

The File Download/Upload feature simplifies the task of remotely configuring a large number of units using TFTP protocol. By downloading the configuration file to a PC it is possible to view all the parameters configured for the unit, as a plain ASCII text file. It is necessary to edit the file using a simple editor (that does not insert special characters) and remove certain parameters or change their values prior to uploading the configuration to another unit. The file loading procedure can also be used for uploading a feature license file or an updated country code file to multiple units.

When multiple configurations are being done simultaneously, that is, the file is being uploaded to several units, it is recommended that the file will include only the required parameters.

In the configuration file, the following three fields represent each parameter:

- 1 A symbolic string similar to the name of the parameter in the Monitor program, followed by "=".
- 2 The value of the parameters, which uses the same values as the Monitor program.
- 3 An optional comment. If used, the comment should start with a ";" character.

An unknown parameter or a known parameter with a value that is invalid or out of range will be ignored.

Use the SNMP write community string (the default is "private") to define both the uploaded file (put) and the downloaded file (get). The file should be transferred in ASCII mode.

Use the extension `cfg` for a configuration file.

Use the extension `cmr` for the Operator Defaults file.

Use the extension `fln` for a Feature License file.

Use the extension `ccf` for a Country Code file.

Feature license and country code files include multiple strings, where each string is applicable only for a certain unit identified by its MAC address. When uploading a feature license or a country code file to multiple units, each unit will accept only the parts that are applicable for itself.

Examples:

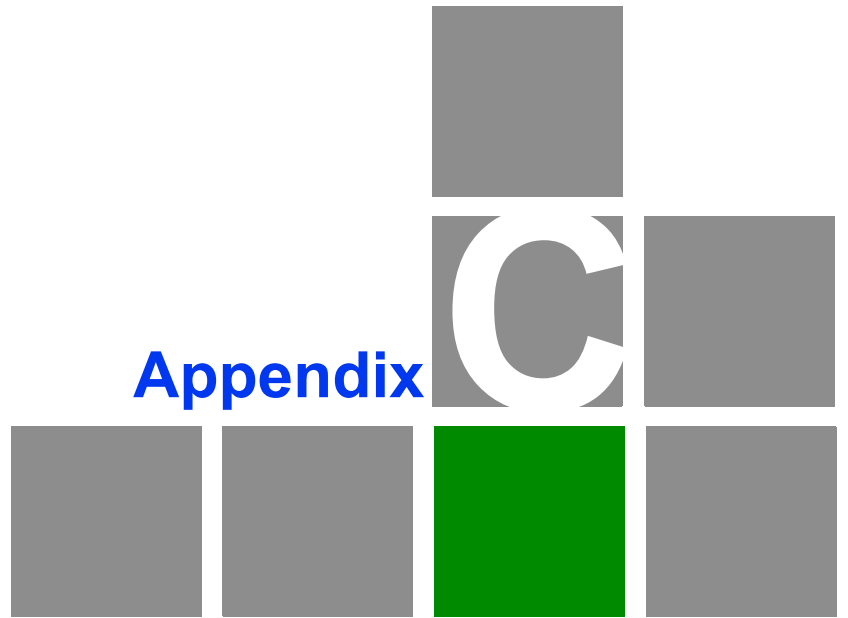
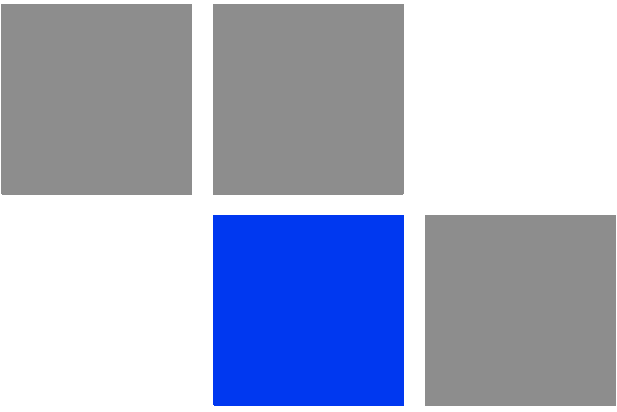
- 1 To upload the configuration file using a DOS based TFTP Client to an AU whose IP address is 206.25.63.65, enter:
`tftp 206.25.63.65 put Auconf private.cfg`

- 2 To download the Operator Defaults file from the same unit, enter:
tftp 206.25.63.65 get private.cmr Auconf
- 3 To upload the Feature Upgrade file to the same unit, enter:
tftp 206.25.63.65 put Auconf private.fln
- 4 To upload the Country Code file from to same unit, enter:
tftp 206.25.63.65 put Auconf private.ccf

NOTE



The Configuration File mechanism is common to multiple product lines. The Configuration File may includes parameters that are not applicable for AU-EZ. Do not attempt to change the default values of these parameters.



Appendix

Using the Set Factory Defaults Utility

The Set Factory Defaults utility is intended to enable management access to a unit in cases where such access is not possible due to wrong or unknown configuration of certain parameters. This includes cases such as unknown Management VLAN ID and wrong management access filtering.

The utility accesses the unit by sending a special packet. Access to the unit is based on its MAC address, which must be entered in the Unit MAC address field.

The set unit defaults feature is only available via the Ethernet port.



To set factory defaults:

- 1 Connect the PC with the Set Factory Defaults utility to the Ethernet port of the unit.

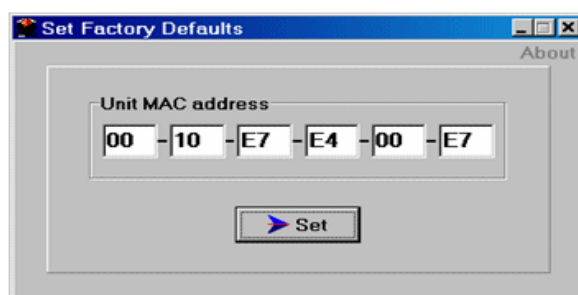
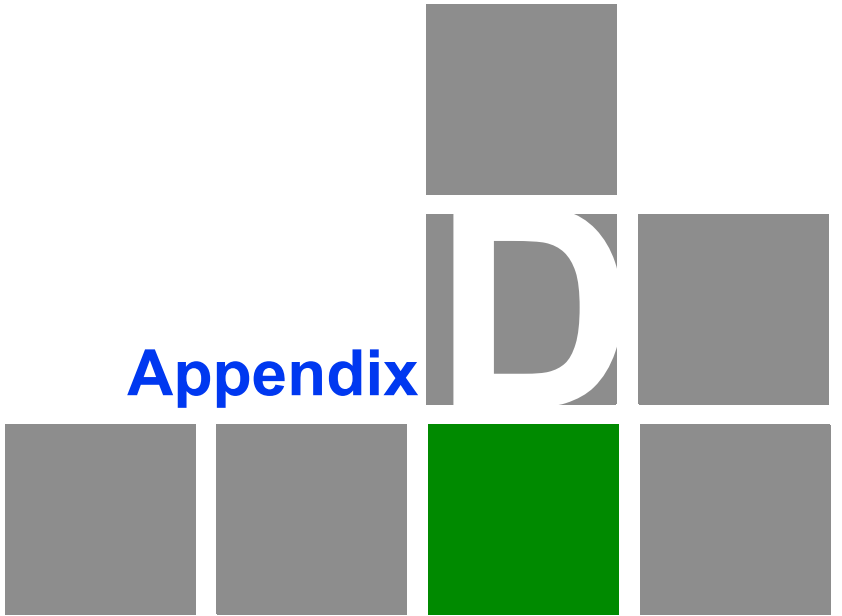
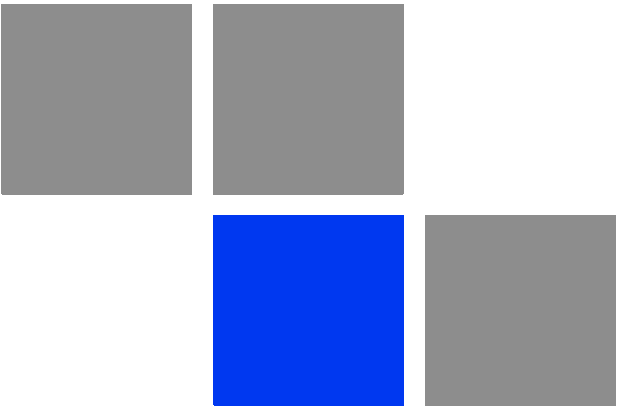


Figure C-1: Set Factory Defaults window

Enter the unit's MAC address.

- 2 Click on the **Set** button.

This utility performs the same operation as Set Complete Factory Defaults, restoring the default factory configuration of all parameters, except to Passwords, general FTP parameters and AU's Frequency.



Preparing the Indoor to Outdoor Cable

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

Figure 4 2 shows the wire pair connections required for the Indoor-to-Outdoor cable.

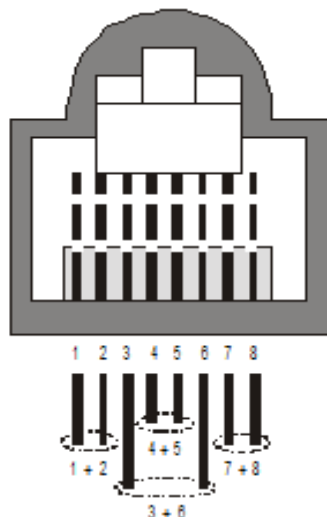


Figure D-1: Ethernet Connector Pin Assignments

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

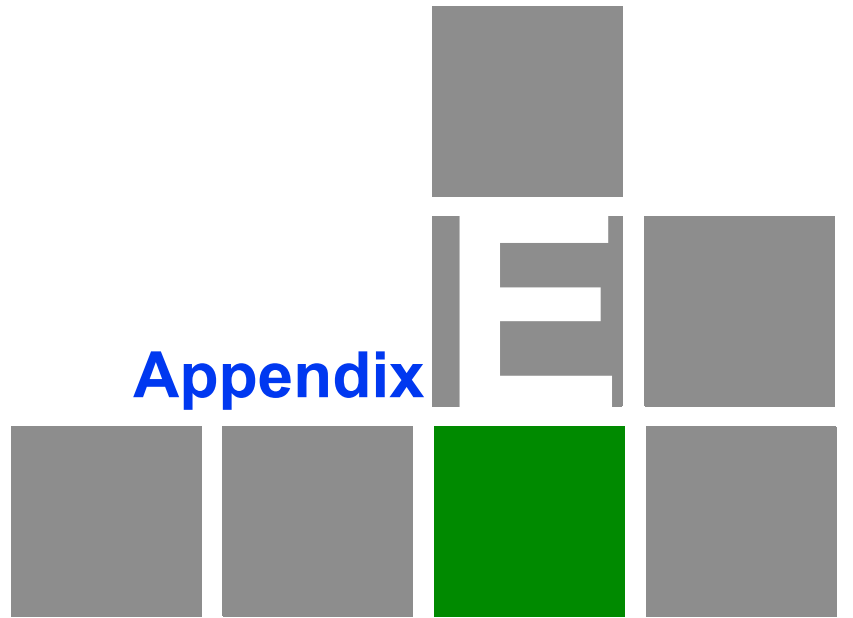
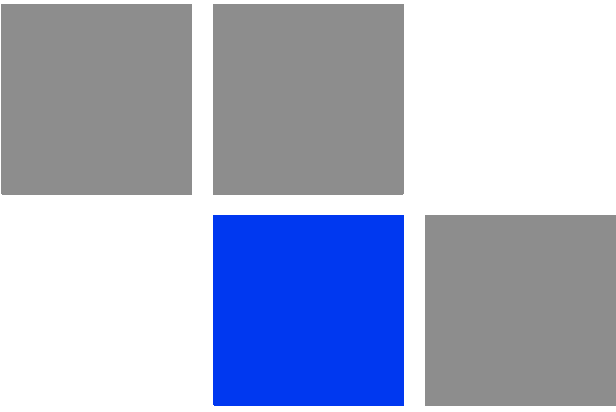
Table D-1: Cable Color Codes

Wire Color	Pin
Blue	1
Blue/white	2
Orange	3
Orange/white	4
Brown	5
Brown/white	6
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.



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 ("No" in the Run-Time column indicates that a change to the parameter will take effect only after reset).

E.1 Parameters Summary

E.1.1 Unit Control Parameters

Parameter	Range	Default	Run-Time
Change Unit Name	Up to 32 printable ASCII characters	None	Yes
Change Read Only Password	Up to 8 printable ASCII characters	public	No
Change Installer Password	Up to 8 printable ASCII characters	user	No
Change Administrator Password	Up to 8 printable ASCII characters	private	No
FTP SW Version File Name	Up to 20 printable ASCII characters. An empty string is not allowed.	VxWorks.bz	Yes
Configuration File Name	Up to 20 printable ASCII characters. An empty string is not allowed.	config.cfg	Yes
Operator Defaults File Name	Up to 20 printable ASCII characters. An empty string is not allowed.	operator.cmr	Yes
FTP Source Dir	Up to 80 printable ASCII characters. Use "." to clear.	None (empty)	Yes
FTP Server IP Address	IP address	10.0.0.253	Yes
FTP Gateway IP Address	IP address	0.0.0.0	Yes
FTP User Name	Up to 18 printable ASCII characters	vx	Yes
FTP Password	Up to 18 printable ASCII characters	vx	Yes
FTP Log File Name	Up to 20 printable ASCII characters	logfile.log	Yes
FTP Log File Destination Directory	Up to 80 printable ASCII characters. Use "." to clear.	None (empty)	Yes
Event Log Policy	<ul style="list-style-type: none"> <input type="checkbox"/> Message <input type="checkbox"/> Warning <input type="checkbox"/> Error <input type="checkbox"/> Fatal <input type="checkbox"/> Log None 	Warning	Yes
Log Out Timer	1 999 minutes	5	Yes

Parameter	Range	Default	Run-Time
Ethernet Port Negotiation Mode	<ul style="list-style-type: none">■ Force 10 Mbps and Half-Duplex■ Force 10 Mbps and Full-Duplex■ Force 100 Mbps and Half-Duplex■ Force 100 Mbps and Full-Duplex■ Auto Negotiation	Auto Negotiation	No
Change System Location	Up to 34 printable ASCII characters	None	Yes
Manual Feature Upgrade	License string: 32 to 64 hexadecimal digits	None	No
AP Working Mode	<ul style="list-style-type: none">■ EZ Mode■ Mixed Mode	EZ Mode	No

E.1.2 IP Parameters

Parameter	Range	Default	Run-Time
IP Address	IP address	10.0.0.1	No
Subnet Mask	IP address	255.0.0.0	No
Default Gateway Address	IP address	0.0.0.0	No
DHCP Option	<input type="checkbox"/> Disable <input type="checkbox"/> DHCP Only <input type="checkbox"/> Automatic	Disable	No
Access to DHCP	<input type="checkbox"/> From Wireless Only <input type="checkbox"/> From Ethernet Only <input type="checkbox"/> From Both Wireless and Ethernet	From Ethernet Only	No

E.1.3 Air Interface Parameters

Parameter	Range	Default	Run-Time
ESSID	Up to 31 printable ASCII characters	ESSID	No
Operator ESSID Option (Mixed Mode)	<input type="checkbox"/> Disable <input type="checkbox"/> Enable	Enable	No
Operator ESSID (Mixed Mode)	Up to 31 printable ASCII characters	ESSID1	No
Maximum Cell Distance	0-54 (Km) 0 means no compensation	0 (no compensation)	Yes
Arbitration Inter-Frame Spacing	1-50 (time slots)	2 time slots	No
Wireless Trap Threshold	1-100 (%)	30 (%)	No
Maximum Number of Associations	1-512 (1 124 if Data Encryption Option should be enabled).	48	Yes
Frequency	According to the Sub-Band	The lowest frequency in the Sub-Band	Yes
DFS Required by Regulations*	<input type="checkbox"/> No <input type="checkbox"/> Yes	Depends on Country Code	Yes

Parameter	Range	Default	Run-Time
Frequency Subset Definition (in AU)*	According to the Sub-Band. A list of frequency indexes or A for all frequencies supported by the Sub-Band	A	Yes
Channel Check Time* Assessment Period*	1 - 3600 (seconds)	60 (seconds)	Yes
Channel Avoidance Period*	1 - 60 (minutes)	30 (minutes)	Yes
SU Waiting Option (applicable only in Mixed Mode)	<input type="checkbox"/> Disable <input type="checkbox"/> Enable	Enable	Yes
Remote Radar Event Reports	0 - 512 detections	0 (disabled)	Yes
Remote Radar Events Monitoring Period	1 - 30 minutes	30	Yes
Minimum Pulses to Detect*	1-100	4 for FCC 8 for other (ETSI)	Yes
Clear radar Detected Channels After Reset*	<input type="checkbox"/> Disable <input type="checkbox"/> Enable	Disable	Yes
Channel Reuse Option*	<input type="checkbox"/> Disable <input type="checkbox"/> Enable	Disable	Yes
Radar Activity Assessment Period*	1 - 12 hours	5 hours	Yes
Maximum Number of Detections in	1 - 10 detections	5 detections	Yes
DFS Detection Algorithm	Applicable only for Universal Country Code in 5.4/5.8 GHz: <input type="checkbox"/> ETSI <input type="checkbox"/> FCC	ETSI	Yes
Country Code Learning By SU (Mixed Mode)	<input type="checkbox"/> Disable <input type="checkbox"/> Enable	Disable	Yes
Transmit Power	-10 dBm to a value that depends on Country Code / Antenna Gain	The highest allowed value	Yes

Parameter	Range	Default	Run-Time
ATPC Option (Mixed Mode)	<input type="checkbox"/> Disable <input type="checkbox"/> Enable	Enable	Yes
ATPC Option for EZ	<input type="checkbox"/> Disable <input type="checkbox"/> Enable	Disable	Yes
Delta from Minimum SNR Level	4-20 (dB)	<input type="checkbox"/> Units in 5.4, 5.8 GHz bands: 5 (dB) <input type="checkbox"/> Units in the 4.9, 5.2 and 5.3 GHz bands: 8 (dB)	Yes
Minimum SNR Level	4-60 (dB)	28 (dB)	Yes
Minimum Interval Between ATPC Messages (Mixed Mode)	1-3600 (seconds)	30 (seconds)	Yes
ATPC Power Level Steps (Mixed Mode)	1-20 (dB)	4	Yes
Tx Control	<input type="checkbox"/> Off <input type="checkbox"/> On <input type="checkbox"/> Ethernet Status Control	On	Yes
Antenna Gain	Minimum: 0 (dBi) Maximum: 50 or Regulation Max EIRP+10 (the lower of the two values).	According to the antenna supplied with the unit.	No
Spectrum Analysis Channel Scan Period	2 - 30 seconds	5 seconds	Yes (Configured per analysis)
Spectrum Analysis Scan Cycles	1 - 100 cycles	2 cycles	Yes (Configured per analysis)
Automatic Channel Selection	<input type="checkbox"/> Disable <input type="checkbox"/> Enable	Disable	Yes (Configured per analysis)
Lost Beacons Watchdog Threshold	100 - 1000, 0 means Not Used	218	Yes
Noise Immunity State Control	<input type="checkbox"/> Automatic <input type="checkbox"/> Manual	Automatic	Yes

Parameter	Range	Default	Run-Time
Noise Immunity Level	0 - 4 Use only 0 or 4	0	Yes
Spur Immunity Level	0 - 7	0	Yes
OFDM Weak Signal	0 (not active) or 1 (active)	Low	Yes
Pulse Detection Sensitivity	<input type="checkbox"/> Low <input type="checkbox"/> High	Low	Yes
Noise Floor Calculation Mode	<input type="checkbox"/> Fully Automatic <input type="checkbox"/> Forced <input type="checkbox"/> Automatic with Minimum Value	Fully Automatic	Yes
Noise Floor Forced Value	-107 to -55 (dBm)	-96	Yes
Select Calibration Option to Use	<input type="checkbox"/> None <input type="checkbox"/> Field <input type="checkbox"/> Factory (not available in current release)	None	Yes

* Applicable only if DFS is supported by the Sub-Band

E.1.4 Network Management Parameters

Parameter	Range	Default	Run-Time
Access to Network Management	<ul style="list-style-type: none"> <input type="checkbox"/> From Wireless Link Only <input type="checkbox"/> From Ethernet Only <input type="checkbox"/> From Both Ethernet and Wireless Link 	From Both Ethernet and Wireless Link	No
Network Management Filtering	<ul style="list-style-type: none"> <input type="checkbox"/> Disable <input type="checkbox"/> Activate Management IP Filter On Ethernet Port <input type="checkbox"/> Activate Management IP Filter On Wireless Port <input type="checkbox"/> Activate Management IP Filter On Both Ethernet and Wireless Ports 	Disable	No
Set Network Management IP Address	IP address	0.0.0.0 (all 10 entries)	No
Set/Change Network Management IP Address Ranges	<start address> to <end address> or, <base address> mask <mask>	0.0.0.0 TO 0.0.0.0 (all 10 entries)	No
Send SNMP Traps	<ul style="list-style-type: none"> <input type="checkbox"/> Disable <input type="checkbox"/> Enable 	Disable	Yes
SNMP Traps IP Destination	IP address	0.0.0.0 (all 10 entries)	No
SNMP Traps Community	Up to 14 printable ASCII characters	public (all 10 entries)	No

E.1.5 Bridge Parameters

Parameter	Range	Default	Run-Time
VLAN ID - Management	1 - 4094, 65535	65535 (no VLAN)	No
VLAN Link Type	<ul style="list-style-type: none"> <input type="checkbox"/> Hybrid Link <input type="checkbox"/> Trunk Link 	Hybrid Link	No

Parameter	Range	Default	Run-Time
VLAN Forwarding Support	Disable, Enable	Disable	No
VLAN Forwarding ID	1 - 4094 (up to 20 entries)	Empty list	No
VLAN Relaying Support	Disable, Enable	Disable	No
VLAN Relaying ID	1 - 4094 (up to 20 entries)	Empty list	No
VLAN Priority - Management	0 - 7	0	No
Ethernet Broadcast/Multicast Limiter Option	<ul style="list-style-type: none"> <input type="checkbox"/> Disable <input type="checkbox"/> Limit only Broadcast Packets <input type="checkbox"/> Limit Multicast Packets that are not Broadcasts <input type="checkbox"/> Limit All Multicast Packets (including broadcast) 	Disable	Yes
Ethernet Broadcast/Multicast Limiter Threshold	0 - 204800 (packets/second)	50	Yes
Ethernet Broadcast/Multicast Limiter Send Trap Interval	1 - 60 (minutes)	5 (minutes)	Yes
Bridge Aging Time	20 - 2000 seconds	300	No
Broadcast Relaying	<ul style="list-style-type: none"> <input type="checkbox"/> Disable <input type="checkbox"/> Broadcast/Multicast Enable <input type="checkbox"/> Broadcast Enable <input type="checkbox"/> Multicast Enable 	Broadcast/Multicast	No
Unicast Relaying	<ul style="list-style-type: none"> <input type="checkbox"/> Disable <input type="checkbox"/> Enable 	Enable	No
MAC Address List	Up to 100 MAC addresses	EnableNone (empty)	Yes

Parameter	Range	Default	Run-Time
MAC Address List Action	<input type="checkbox"/> Deny <input type="checkbox"/> Allow	Deny	Yes
Station Allowed Option	<input type="checkbox"/> Disable <input type="checkbox"/> Enable	Enable	Yes

E.1.6 Performance Parameters

Parameter	Range	Default	Run-Time
RTS Threshold	20 - 4092 (bytes)	4092	Yes
Minimum Contention Window	0, 7, 15, 31, 63, 127, 255, 511, 1023	15	No
Maximum Contention Window	7, 15, 31, 63, 127, 255, 511, 1023	1023	No
Maximum Modulation Level	1-8	8	Yes
Multicast Modulation Level	1-8	1	Yes
Number of HW Retries	1 - 14	10	Yes
Average SNR Memory Factor (Mixed Mode)	-1 to 32	5	Yes
Burst Mode Option*	<input type="checkbox"/> Disable <input type="checkbox"/> Enable	Enable	No
Burst Mode Time Interval*	1 to the value defined in the Sub-Band for Maximum Burst Duration (milliseconds)	5 milliseconds or the value of Maximum Burst Duration defined for the Sub-Band (the lower of the two values).	Yes
Adaptive Modulation Option	<input type="checkbox"/> Disable <input type="checkbox"/> Enable	Enable	No
Minimum Interval Between Adaptive Modulation Messages (Mixed Mode)	<input type="checkbox"/> 1-3600 (seconds)	4 (seconds)	Yes
Adaptive Modulation Decision Threshold	<input type="checkbox"/> Normal <input type="checkbox"/> High	Normal	No
Concatenation Option (Mixed Mode)	<input type="checkbox"/> Disable <input type="checkbox"/> Enable	Enable	No
Maximum Concatenated Frame Size (Mixed Mode)	<input type="checkbox"/> 256 to 4032 (bytes)	4032	Yes

* Applicable only if Burst Mode is supported by the Sub-Band.

E.1.7 Service Parameters

Parameter	Range	Default	Run-Time
User Filtering Option	<ul style="list-style-type: none"> <input type="checkbox"/> Disable <input type="checkbox"/> IP Protocol Only <input type="checkbox"/> User Defined Addresses Only <input type="checkbox"/> PPPoE Protocol Only 	Disable	Yes
Set/Change Filter IP Address Ranges	<start address> to <end address> or, <base address> mask <mask>	0.0.0.0 TO 0.0.0.0 (all 8 entries)	No
DHCP Unicast Override Filter	<ul style="list-style-type: none"> <input type="checkbox"/> Disable DHCP Unicast <input type="checkbox"/> Enable DHCP Unicast 	Disable DHCP Unicast	Yes
DHCP Unicast Override Filter	<ul style="list-style-type: none"> <input type="checkbox"/> Disable PPPoE Override Filter <input type="checkbox"/> Enable PPPoE Override Filter 	Disable PPPoE Override Filter	Yes
Maximum Burst Duration	0 - 2,000 (ms)	5 (ms)	No
MIR: Downlink for SU-EZ	128 to 12032 (Kbps)	12032	Yes
VLAN Priority Threshold	0 - 7	7	No
ToS Prioritization Option	<ul style="list-style-type: none"> <input type="checkbox"/> Disable <input type="checkbox"/> Enable IP Precedence (RFC791) Prioritization <input type="checkbox"/> Enable DSCP (RFC2474) Prioritization 	Disable	No
IP Precedence Threshold	0 - 7	4	No
DSCP Threshold	0 - 63	32	No
UDP/TCP Port Ranges Prioritization Option	<ul style="list-style-type: none"> <input type="checkbox"/> Disable <input type="checkbox"/> Enable Only for UDP <input type="checkbox"/> Enable Only for TCP <input type="checkbox"/> Enable for both UDP and TCP 	Disable	No

Parameter	Range	Default	Run-Time
UDP RTP/RTCP Prioritization	<input type="checkbox"/> RTP & RTCP <input type="checkbox"/> RTP Only	RTP & RTCP	No
TCP RTP/RTCP Prioritization	<input type="checkbox"/> RTP & RTCP <input type="checkbox"/> RTP Only	RTP & RTCP	No
Low Priority Traffic Minimum Percent	0 - 100 (%)	0 (%)	Yes
DRAP Support	<input type="checkbox"/> Disable <input type="checkbox"/> Enable	Enable	No
UDP Port	8000-8200	8171	No
Maximum Number Of Voice Calls	1-255	40	No
DRAP TTL	1-255 (seconds)	10 (seconds)	No

E.1.8 Security Parameters

Parameter	Range	Default	Run-Time
Authentication Algorithm	<input type="checkbox"/> Open system <input type="checkbox"/> Shared Key	Open system	No
Data Encryption Option	<input type="checkbox"/> Disable <input type="checkbox"/> Enable	Disable	No
Security Mode	<input type="checkbox"/> WEP <input type="checkbox"/> FIPS-197	WEP	No
Default Multicast Key	1-4	1	No
Key # 1 to Key # 4	32 hexadecimal digits	0...0 (all 0=no key)	No
Promiscuous Authentication (Mixed Mode)	<input type="checkbox"/> Disable <input type="checkbox"/> Enable	Disable	Yes (Disable after reset)