



BreezeACCESS[®] 4900

System Manual

PRELIMINARY

**S/W Version 3.2
July 2005
P/N 214151**

Legal Rights

© Copyright 2005 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®, BreezeMANAGE™, BreezeLINK®, BreezeCONFIG™, BreezeMAX™, AlvariSTAR™, MGW™, eMGW™, WAVEXpress™, MicroXpress™, WAVEXchange™, WAVEView™, GSM Network in a Box and TurboWAVE™ 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

BreezeACCESS 4900 (the “Product”) is intended as a non-critical public safety communication channels and is provided subject to and on condition of this Disclaimer. If the communication channel is CRITICAL, customer shall provide for backup. Alvarion is neither an insurer nor guarantor and does not guarantee that the Product will reduce the time it takes for emergency personnel to respond to or locate the source of any emergency call. Nor does Alvarion guarantee that the Product will be error-free or work all of the time or, in all cases, provide access to emergency services. The Product may be subject to compromise, error or failure due to a variety of reasons, including, but not limited to:

- Signals sent by wireless transmitters may be blocked or reflected before reaching their destination.
- The equipment, like any other electrical device, is subject to component failure.
- Although the Product works on radio frequencies and telephone lines, there may be interference on the radio frequency.

ACCORDINGLY, THE PRODUCT IS PROVIDED “AS IS” WITHOUT WARRANTIES OF ANY KIND, AND ALVARION EXPRESSLY DISCLAIMS ALL WARRANTIES WITH RESPECT TO THE PRODUCT, AND TO ALL COMPONENTS THEREOF, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE, NON-INFRINGEMENT OF THIRD PARTY RIGHTS, OR BASED ON COURSE OF CONDUCT OR TRADE CUSTOM OR USAGE. Alvarion shall not be liable for any damages arising from or related to the use of the Product, including, but not limited to, any emergency calls placed via the Product, or any

other cause related to the use or inability to use the Product. Alvarion shall not have any liability for any personal injury, property damage or other loss based on any claim arising from or related to the Product, the use of or inability to use such Product or any other cause related to the Product. Alvarion shall have no liability whatsoever for any direct, indirect, punitive, special, incidental or other consequential damages arising directly or indirectly from the use of or inability to use the Product, including, but not limited to, any damages or injury caused by any error, omission, deletion, defect, interruption, failure of performance, delay in operation or transmission, computer virus, communication line failure, theft or destruction or unauthorized access to, alteration of whether for breach of contract, negligence, tortious behavior, or under any other cause of action.

YOUR SOLE REMEDY AND ALVARION'S SOLE LIABILITY IS, IN ALVARION'S DISCRETION, EITHER (i) THE REPLACEMENT OR REPAIR OF THE PRODUCT; OR (ii) THE REFUND OF THE PURCHASE PRICE FOR THE PRODUCT.

All use the Product is at your sole risk. You assume all risks of use of this Product and hereby waive and release, to the full extent permitted by law, Alvarion and its subsidiaries and affiliated companies, and their respective employees, officers, directors and agents, from any and all claims, damages, demands, and any other liability relating to or arising from the use of the Product and agree to defend, indemnify and hold harmless Alvarion and its subsidiaries and affiliated companies, and their respective employees, officers, directors and agents against any and all claims resulting from or arising out of any use of or inability to use the Product.

Limitation of Liability

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

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

Electronic Emission Notices

This device complies with Part 15 of the FCC rules.

Operation is subject to the following two conditions:

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

FCC Radio Frequency Interference Statement

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

The Base Station equipment 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, and must not be co-located or operating in conjunction with any other antenna or transmitter.

R&TTE Compliance Statement

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

Safety Considerations

For the following safety considerations, "Instrument" means the BreezeACCESS 4900 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, Alvarion is not liable for any injury, damage or regulation violations associated with or caused by installation, grounding or lightning protection.

Important Notice

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

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

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



About This Manual

This manual describes the BreezeACCESS 4900 Broadband Wireless Access System Release 3.2 and how to install, operate and manage the system components.

This manual is intended for technicians responsible for installing, setting up and operating the BreezeACCESS 4900 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 4900 system and its components.
- **Chapter 2** – Installation: Describes how to install the system components.
- **Chapter 3** – Commissioning: Describes how to configure basic parameters, align the Subscriber Unit antenna and validate unit operation.
- **Chapter 4** – Operation and Administration: Describes how to use the BreezeACCESS 4900 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 Restore Link Parameters Utility: Describes how to use the special Restore Link Parameters utility to enable management access to units where wrong or unknown configuration disables regular access to the unit for management purposes.
- **Appendix D** – Preparing the indoor to outdoor cable: Provides details on preparation of the indoor to outdoor Ethernet cable.

- **Appendix E** – Supported MIBs and Traps: Provides a brief description of the parameters contained in the private MIB agent incorporated into the BreezeACCESS 4900 devices. In addition, a description of all traps relevant to the BreezeACCESS 4900 devices is provided.

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

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

- **Appendix H** – Troubleshooting.



Contents

Chapter 1 - System Description	1
1.1 Introducing BreezeACCESS 4900	2
1.2 Base Station Equipment.....	3
1.2.1 Modular Base Station Equipment	3
1.2.2 Standalone “Micro-cell” Access Unit.....	4
1.3 Subscriber Unit	6
1.4 Networking Equipment.....	7
1.5 Management Systems	8
1.5.1 BreezeCONFIG™	8
1.5.2 AlvariSTAR™	8
1.6 Specifications	10
1.6.1 Radio	10
1.6.2 Data Communication	11
1.6.3 Configuration and Management	12
1.6.4 Standards Compliance, General.....	13
1.6.5 Physical and Electrical.....	14
Chapter 2 - Installation	21
2.1 Installation Requirements	22
2.1.1 Packing List	22
2.1.2 Indoor-to-Outdoor Cables	24
2.2 Equipment Positioning Guidelines	26

2.3 Installing the Outdoor Unit.....	27
2.3.1 Pole Mounting the Outdoor Unit.....	27
2.3.2 Connecting the Grounding and Antenna Cables	29
2.3.3 Connecting the Indoor-to-Outdoor Cable.....	30
2.4 Installing the Universal IDU Indoor Unit	32
2.4.1 RESET Button Functionality	33
2.5 Installing the Modular Base Station Equipment.....	34
2.5.1 BS-SH Slot Assignment.....	34
2.5.2 BS-PS-AC Power Supply Module	35
2.5.3 BS-PS-DC Power Supply Module.....	36
2.5.4 BS-AU Network Interface Module	37
2.5.5 Installing the BS-SH Chassis and Modules.....	38
Chapter 3 - Commissioning	41
3.1 Configuring Basic Parameters.....	42
3.2 Aligning the Subscriber Unit Antenna	45
3.3 Configuring the Subscriber Unit’s Maximum Modulation Level.....	46
3.4 Operation Verification.....	48
3.4.1 Outdoor Unit Verification.....	48
3.4.2 Indoor Unit Verification.....	51
3.4.3 Verifying the Ethernet Connection (Modular Base station)	52
3.4.4 Verifying the Indoor-to-Outdoor Connection (Modular Base Station).....	52
3.4.5 Verifying Data Connectivity.....	52
Chapter 4 - Operation and Administration.....	53
4.1 Working with the Monitor Program	54
4.1.1 Accessing the Monitor Program Using Telnet.....	54
4.1.2 Common Operations.....	55

4.2 Menus and Parameters	57
4.2.1 Main Menu	57
4.2.2 Info Screens Menu.....	57
4.2.3 Unit Control Menu.....	62
4.2.4 Basic Configuration Menu.....	74
4.2.5 Site Survey Menu	77
4.2.6 Advanced Configuration Menu	90
 Appendix A - Software Version Loading Using TFTP.....	 145
 Appendix B - File Download and Upload Using TFTP.....	 149
 Appendix C - Using the Set Factory Defaults Utility	 153
 Appendix D - Preparing the Indoor to Outdoor SU Cable.....	 155
 Appendix E - Supported MIBS and Traps	 159
E.1 System Object Identifiers.....	160
E.2 breezeAccessVLMib	162
E.2.1 System Information Parameters	162
E.2.2 Unit Control Parameters	165
E.2.3 Network Management Parameters	168
E.2.4 IP Parameters.....	170
E.2.5 Bridge Parameters.....	171
E.2.6 Air Interface Parameters.....	174
E.2.7 Service Parameters	188
E.2.8 User Filtering Parameters.....	193
E.2.9 Security Parameters	195
E.2.10 Performance Parameters.....	196
E.2.11 Site Survey Parameters.....	198

E.3 Supported Traps	209
E.3.1 Trap Variables.....	209
E.3.2 Private Traps.....	210
Appendix F - Parameters Summary	213
F.1 Unit Control Parameters.....	214
F.2 IP Parameters	216
F.3 Air Interface Parameters.....	217
F.4 Network Management Parameters	219
F.5 Bridge Parameters	220
F.6 Performance Parameters.....	222
F.7 Service Parameters.....	223
F.8 Security Parameters	225
Appendix G - Using the Feature License Web Application	227
G.1 The Feature License Web Application	228
G.1.1 Loading License Strings to Devices.....	230
Appendix H - Troubleshooting	233
H.1 Ethernet Port Connection Problems	234
H.2 SU Association Problems	235
H.3 Low Throughput Problems	236



Figures

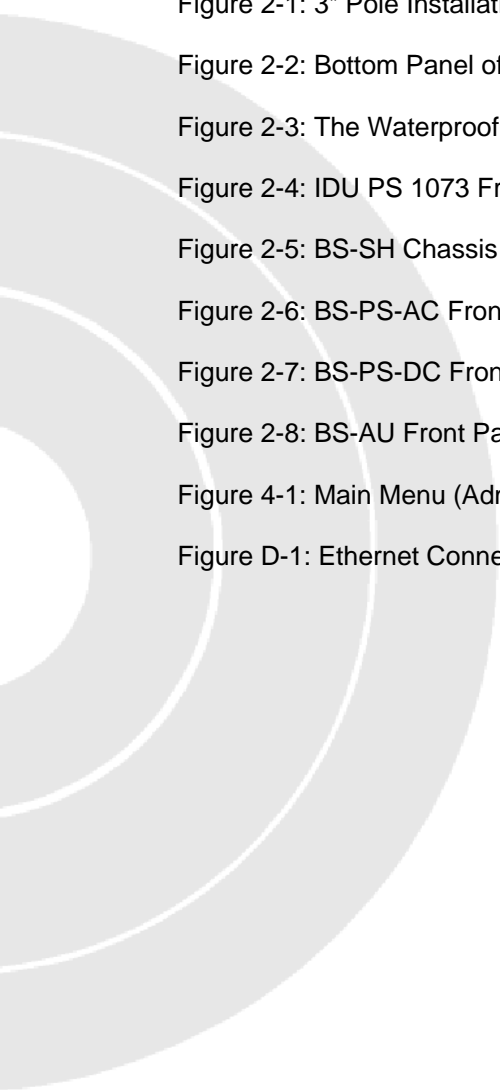


Figure 2-1: 3" Pole Installation Using Special Brackets.....	28
Figure 2-2: Bottom Panel of the Outdoor Unit (without the seal assembly).....	29
Figure 2-3: The Waterproof Seal	30
Figure 2-4: IDU PS 1073 Front Panel.....	32
Figure 2-5: BS-SH Chassis Slot Assignment.....	34
Figure 2-6: BS-PS-AC Front Panel.....	35
Figure 2-7: BS-PS-DC Front Panel.....	36
Figure 2-8: BS-AU Front Panel	37
Figure 4-1: Main Menu (Administrator Level)	55
Figure D-1: Ethernet Connector Pin Assignments.....	156



Tables

Table 1-1: AU Detached Antennas	4
Table 1-2: Subscriber Unit ODU Types	6
Table 1-3: Radio Specifications	10
Table 1-4: Data Communication	11
Table 1-5: Configuration and Management	12
Table 1-6: Standards Compliance, General.....	13
Table 1-7: Mechanical Specifications, Subscriber Unit.....	14
Table 1-8: Connectors, Subscriber Unit.....	14
Table 1-9: Electrical Specifications, Subscriber Unit	15
Table 1-10: Mechanical Specifications, Modular Base Station Equipment	16
Table 1-11: Connectors, Modular Base Station Equipment.....	17
Table 1-12: Electrical Specifications, Modular Base Station Equipment.....	17
Table 1-13: Mechanical Specifications, Stand Alone Access Unit	18
Table 1-14: Connectors, Stand Alone Access Unit.....	18
Table 1-15: Electrical Specifications, Stand Alone Access Unit	19
Table 1-16: Environmental Specifications.....	19
Table 2-1: Approved Category 5E Ethernet Cables	25
Table 2-2: BS-PS LED Functionality.....	36
Table 3-1: Basic Parameters	42
Table 3-2: Recommended Maximum Modulation Level	47
Table 3-3: AU-ODU LEDs.....	48
Table 3-4: SU-ODU LEDs.....	49
Table 3-5: SU-ODU SNR Bar LED Functionality	50
Table 3-6: BS-AU LEDs	51

Table 3-7: PS1073 SU IDU / AU-SA IDU LEDs	52
Table 4-1: Default Passwords	54
Table 4-2: Sub-Band Dependent Parameters	61
Table 4-3: Parameters not reset after Set Complete Factory/Operator Defaults	64
Table 4-4: Parameters that are not reset after Set Partial Factory/Operator Defaults	65
Table 4-5: Authentication and Association Process	85
Table 4-6: VLAN Management Port Functionality	114
Table 4-7: VLAN Data Port Functionality - Access Link	115
Table 4-8: VLAN Data Port Functionality - Trunk Link	116
Table 4-9: VLAN Data Port Functionality - Hybrid Link	116
Table 4-10: Recommended Maximum Modulation Level	128

Chapter 1 - System Description

In This Chapter:

- [Introducing BreezeACCESS 4900](#), page 2
- [Base Station Equipment](#), page 3
- [Subscriber Unit](#), page 6
- [Networking Equipment](#), page 7
- [Management Systems](#), page 8
- [Specifications](#), page 10

1.1 Introducing BreezeACCESS 4900

BreezeACCESS 4900 is a high capacity, IP services oriented Broadband Wireless Access system operating in the 4.9 GHz licensed spectrum band allocated for public safety. The system employs wireless packet switched data technology to support high-speed IP services with a network connection that is always on. The system is designed for both Point-to-Point and Point-to-Multipoint configurations, supporting data, VoIP and video applications.

The system supports Virtual LANs based on IEEE 802.1Q, enabling secure operation and Virtual Private Network (VPN) services. The system supports layer-2 traffic prioritization based on IEEE 802.1p and layer-3 traffic prioritization based on either IP ToS Precedence (RFC791) or DSCP (RFC2474). It also supports traffic prioritization based on UDP and/or TCP port ranges. BreezeACCESS 4900 uses advanced security mechanisms, including WEP128, AES128 and FIPS compliance.

Using OFDM modem technology and high power radios, BreezeACCESS 4900 offers an unmatched combination of wide coverage, high capacity and value-added features to provide wireless connectivity that works also in near and non-line-of-site (NLOS) conditions.

Alvarion's Complete Spectrum solution enables the BreezeACCESS 4900 to integrate seamlessly into other BreezeACCESS networks. Supporting both fixed and mobile platforms at multiple frequency bands, the Complete Spectrum enables simultaneous deployment of systems at 900 MHz, 2.4 GHz, 3.5 GHz, 4.9 GHz, and the entire 5 GHz band.

A BreezeACCESS 4900 system comprises the following:

- **Customer Premise Equipment (CPE):** BreezeACCESS 4900 Subscriber Units (SUs).
- **Base Station Equipment (BS):** BreezeACCESS 4900 Access Units and supporting equipment.
- **Networking Equipment:** Standard Switches/Routers supporting connections to the backbone and/or Internet.
- **Management Systems:** SNMP-based Management, Billing and Customer Care, and other Operation Support Systems.

1.2 Base Station Equipment

The Access Units, installed at the Base Station site, provide all the functionality necessary to communicate with the Subscriber Units and to connect to the backbone of the network.

There are 2 lines of Access Units with different architectures:

- Modular Base Station Equipment
- Standalone “Micro-Cell” Access Unit

1.2.1 Modular Base Station Equipment

The Base Station Equipment is based on the BS-SH 3U chassis, which is suitable for installation in 19-inch racks. The chassis contains one or two Power Supply modules and has 8 slots that can accommodate BS-AU Network Interface modules. These slots can also

accommodate various combinations of other modules, including Network Interface (BS-AU) modules for Access Units operating in any of the bands supported by BreezeACCESS VL



equipment or BreezeACCESS equipment using GFSK modulation, including BreezeACCESS 900, BreezeACCESS II, BreezeACCESS XL and BreezeACCESS V. It can also accommodate a BS-GU GPS and Alarms module to support GPS-based synchronization of BreezeACCESS systems using Frequency Hopping radios.

Two different types of power supply modules are available for the BreezeACCESS 4900 chassis: The BS-PS-DC that is powered from a -48 VDC power source, and the BS-PS-AC, powered from the 110/220 VAC mains. The optional use of two power supply modules ensures fail-safe operation through power supply redundancy. When the same chassis is used also for Access Unit modules belonging to other BreezeACCESS families using GFSK modulation, then one BS-PS power supply (AC or DC) should be used to provide power to the BreezeACCESS 4900 Access Units, and a different power supply module, suitable for GFSK equipment, is required for powering the BreezeACCESS GFSK Access Units.

Each BS-AU module, together with its outdoor AU-D/E-BS-ODU radio unit and an antenna comprise an AU-D/E-BS Access Unit that serves a single sector/cell.

One AU-BS Access Unit can serve up to 512 Subscriber Units (124 when Data Encryption is used).

The AU-D/E-BS-ODU outdoor unit contains the processing and radio modules and connects to an external antenna using a short RF cable.

E model units, such as the AU-E-BS-4900, are supplied without an antenna and are primarily intended for Point-to-Point applications.

D model units, namely AU-D-BS-4900-360 and AU-D-BS-4900-120, are supplied with a detached antenna, as listed in Table 1-1:



Unit	Antenna	Band (GHz)	Horizontal Beam Width	Gain (dBi)
AU-D-BS-4900-120	AU-Ant-4.9G-15-120	4.900-5.100	120°	15
AU-D-BS-4900-360	AU-Ant-4.9G-9-Omni	4.900-5.100	360°	9

The BS-AU indoor module connects to the network through a standard IEEE 802.3 Ethernet 10/100BaseT (RJ 45) interface. The indoor module is connected to the outdoor unit via a Category 5E Ethernet cable. This cable carries Ethernet traffic between the indoor module and the outdoor unit, and also transfers power (54 VDC) and control from the indoor module to the outdoor unit.

1.2.2 Standalone “Micro-cell” Access Unit

The standalone AU-D/E-SA Access Unit is very similar to the AU-D/E-BS unit. The AU-D/E-SA-ODU outdoor unit is very similar to the AU-D/E-BS-ODU outdoor unit (identical functionality, but the units are not interchangeable). Units are differentiated based on the availability of an antenna: E model units are supplied without an antenna, while D model units are supplied with a detached antenna.



Available units are:

- AU-D-SA-4900-360 (Standalone AU with a 9 dBi omni antenna)
- AU-D-SA-4900-120 (Standalone AU with a 15 dBi, 120° sector antenna)
- AU-E-SA-4900 (Standalone AU)

The available antennas for D model units are the same as those of the AU-D-BS Access Unit. The main difference is in the structure of the indoor part; in the AU-D/E-SA Access Unit the indoor unit is a standalone desktop or wall-mountable

unit (the same Universal IDU that is also used in the SU) rather than a 19" module.

The AU-SA Access Unit can serve up to 512 Subscriber Units (124 when Data Encryption is used).

The IDU connects to the network through a standard IEEE 802.3 Ethernet 10/100BaseT (RJ 45) interfaces and is powered from the 110/220 VAC mains. The indoor unit is connected to the outdoor unit via a Category 5E 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.

NOTE

The AU-D/E-SA-ODU and the AU-D/E-BS-ODU are not interchangeable:
The AU-D/E-SA-ODU cannot be used with the BS-AU; the AU-D/E-BS-ODU cannot be used with the standalone IDU.

1.3 Subscriber Unit

The Subscriber Unit (SU) installed at locations that require service, enables the customer data connection to the Access Unit. The Subscriber Unit provides an efficient platform for high speed Internet and Intranet services, supporting single or multiple end users. The use of packet switching technology provides the user with a connection to the network that is always on, enabling immediate access to services.



The Subscriber Unit comprise a desktop or wall-mountable Indoor Unit (IDU) and an outdoor unit that contains the processing and radio modules. Several ODU types are available to support different requirements, as detailed in Table 1-2:

Table 1-2: Subscriber Unit ODU Types	
SU Type	Antenna Description
SU-A-ODU	Vertically polarized high-gain flat antenna integrated on the front panel
SU-E-ODU	A connection to an external antenna

The Subscriber Unit supports a gross rate of up to 27 Mbps and can bridge a full LAN.

The IDU provides the interface to the user’s equipment and is powered from the 110/220 VAC mains. The customer’s data equipment is connected via a standard IEEE 802.3 Ethernet 10/100BaseT (RJ 45) interface. The indoor unit is connected to the outdoor unit via a Category 5E 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.

1.4 Networking Equipment

The Base Station equipment is connected to the backbone through standard data communication and telecommunication equipment. The 10/100BaseT ports of the AU modules can be connected directly to a multi-port router or to an Ethernet switch connected to a router.

The point-to-point link from the Base Station to the backbone can be either wired or wireless. Data to the Internet is routed to the backbone through standard routers.

1.5 Management Systems

The end-to-end IP-based architecture of the system enables full management of all components, from any point in the system. BreezeACCESS 4900 components can be managed using standard management tools through SNMP agents that implement standard and proprietary MIBs for remote setting of operational modes and parameters. The same SNMP management tools can also be used to manage other system components including switches, routers and transmission equipment. Security features incorporated in BreezeACCESS 4900 units restrict access for management purposes to specific IP addresses and/or directions, that is, from the Ethernet and/or wireless link.

In addition, the Ethernet WAN can be used to connect to other Operation Support Systems including servers, Customer Care systems and AAA (Authentication, Authorization and Admission) tools.

1.5.1 BreezeCONFIG™

The BreezeCONFIG for BreezeACCESS 4900 utility is an SNMP-based application designed to manage BreezeACCESS 4900 system components and upgrade unit software versions. The system administrator can use the BreezeCONFIG utility to control a large number of units from a single location. In addition, BreezeCONFIG enables you to load an updated configuration file to multiple units simultaneously, thus radically reducing the time spent on unit configuration maintenance.

1.5.2 AlvariSTAR™

AlvariSTAR is a comprehensive Carrier-Class network management system for Alvarion's Broadband Wireless Access products-based Networks. AlvariSTAR is designed for today's most advanced Network Operation Centers (NOCs), providing the network Operation, Administration and Maintenance (OA&M) staff and managers with all the network surveillance, monitoring and configuration capabilities that they require in order to effectively manage the BWA network while keeping the resources and expenses at a minimum.

AlvariSTAR is designed to offer the network's OA&M staff with a unified, scalable and distributable network management system. The AlvariSTAR system uses a distributed client-server architecture, which provides a robust, scalable and fully redundant network management system in which all single points of failure can be avoided.

AlvariSTAR provides the following BWA network management functionality:

- Device Discovery
- Device Inventory
- Topology
- Fault Management
- Configuration Management
- Performance Monitoring
- Device embedded software upgrade
- Security Management
- Northbound interface to other Network Management Systems or OSS.

1.6 Specifications

1.6.1 Radio

Table 1-3: Radio Specifications	
Item	Description
Frequency	4.940 – 4.990 GHz
Operation Mode	Time Division Duplex (TDD)
Channel Bandwidth	10 MHz / 5 MHz
Central Frequency Resolution	5 MHz
Antenna Port (AU-D-BS/SA-ODU)	N-Type, 50 ohm
Max. Input Power (at antenna port)	-40 dBm typical
Maximum Output Power	TBD
SU-A-ODU Integral Antenna	20 dBi, 10.5° horizontal x 10.5° vertical, vertical or horizontal polarization, compliant with EN 302 085 V1.1.1 Range 1, Class TS 1, 2, 3, 4, 5
AU-D Detached Antennas	<ul style="list-style-type: none"> ■ AU-Ant-4.9G-15-120: 15 dBi, 4.900-5.100 GHz, 124° horizontal x 6.5° vertical sector antenna, vertical polarization, compliant with EN 302 085 V1.1.2 CS3. ■ AU-Ant-4.9G-9-Omni: 9 dBi, 4.900-5.100 GHz, 360° horizontal x 8° vertical, vertical polarization.

Item	Description			
Sensitivity, typical (dBm at antenna port, PER<10%)	Modulation Level ¹	Sensitivity 5 MHz bandwidth	Sensitivity 10 MHz bandwidth	Min. SNR
	1	-93 dBm	-92 dBm	6 dB
	2	-92 dBm	-91 dBm	7 dB
	3	-91 dBm	-89 dBm	9 dB
	4	-89 dBm	-87 dBm	11 dB
	5	-86 dBm	-84 dBm	14 dB
	6	-82 dBm	-80 dBm	18 dB
	7	-77 dBm	-76 dBm	22 dB
	8	-75 dBm	-74 dBm	23 dB
Modulation	OFDM modulation, 64 FFT points; BPSK, QPSK, QAM16, QAM64			

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

1.6.2 Data Communication

Item	Description
Standard compliance	IEEE 802.3 CSMA/CD
VLAN Support	Based on IEEE 802.1Q
Layer-2 Traffic Prioritization	Based on IEEE 802.1p
Layer-3 Traffic Prioritization	IP Precedence ToS (RFC791) DSCP (RFC2474)
Layer 4 Traffic Prioritization	UDP/TCP destination ports

1.6.3 Configuration and Management

Table 1-5: Configuration and Management	
Type	Standard
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 ■ Selection between WEP, AES/OCB and AES/CCM 128-bit encryption standards ■ ESSID
SNMP Agents	SNMP ver 1 client MIB II, Bridge MIB, Private BreezeACCESS 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

1.6.4 Standards Compliance, General

Type	Standard
EMC	FCC Part 15 class B
Safety	UL 60950-1
Radio	FCC Part 90 FCC Part 15

1.6.5 Physical and Electrical

1.6.5.1 Subscriber Unit

1.6.5.1.1 Mechanical

Unit	Structure	Dimensions (cm)	Weight (kg)
General	An IDU indoor unit and an SU-A-ODU outdoor unit with an integral antenna		
IDU PS1073	Plastic box (black), desktop or wall mountable	14 x 6.6 x 3.5	0.3
SU-A-ODU	Metal box plus an integral antenna in a cut diamond shape in a plastic enclosure, poll or wall mountable	43.2 x 30.2 x 5.9	1.85

1.6.5.1.2 Connectors

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) 2 embedded LEDs in PS1036
	AC IN	3 pin AC power plug
SU-A-ODU	INDOOR	10/100BaseT Ethernet (RJ-45), protected by a waterproof sealing assembly

1.6.5.1.3 Electrical

Table 1-9: Electrical Specifications, Subscriber Unit	
Unit	Details
General	Power consumption: 25W
IDU	AC power input: 85-265 VAC, 50-60 Hz
SU-A-ODU	54 VDC from the IDU over the indoor-outdoor Ethernet cable

1.6.5.2 Modular Base Station Equipment

1.6.5.2.1 Mechanical

Unit	Structure	Dimensions (cm)	Weight (kg)
BS-SH	19" rack (3U) or desktop	13 x 48.2 x 25.6	4.76
BS-PS-DC	DC power supply module	12.9 x 7.0 x 25.3	1.2
BS-PS-AC	AC power supply module	12.9 x 7.0 x 25.3	1.2
BS-AU	Indoor module of the AU-D-BS access unit	12.9 x 3.5 x 25.5	0.15
AU-D-BS-ODU	pole or wall mountable	30.6 x 12.0 x 4.7	1.85
AU-Ant-4.9G-15-120	2"-4" pole mountable	55 x 25 x 1.7	1.5

1.6.5.2.2 Connectors

Table 1-11: Connectors, Modular Base Station Equipment		
Unit	Connector	Description
BS-AU	10/100 BaseT	10/100BaseT Ethernet (RJ-45) with 2 embedded LEDs. Cable connection to a PC: crossed Cable connection to a hub: straight
	RADIO	10/100BaseT Ethernet (RJ-45) with 2 embedded LEDs
AU-D-BS-ODU	INDOOR	10/100BaseT Ethernet (RJ-45), protected by a waterproof sealing assembly
	ANT	N-Type jack, 50 ohm, lightning protected
BS-PS-AC	AC-IN	3-PIN AC power plug
BS-PS-DC	-48 VDC	3 pin DC D-Type 3 power pins plug Amphenol 717TWA3W3PHP2V4RRM6
Antenna	RF	N-Type jack (on a 1.5m cable in the Omni-8-5.8)

1.6.5.2.3 Electrical

Table 1-12: Electrical Specifications, Modular Base Station Equipment	
Unit	Details
General	240W max. for a fully equipped chassis (1 PS, 6 AU)
BS-PS-AC	AC power input: 85-265 VAC, 47-65 Hz DC power output: 54 V; 3.3 V
BS-PS-DC	DC power input: -48 VDC nominal (-34 to -72), 10 A max DC power output: 54 V; 3.3 V
BS-AU	3.3 VDC, 54 VDC from the power supply module(s) via the back plane
AU-D-BS-ODU	54 VDC from the BS-AU over the indoor-outdoor Ethernet cable
AU-D-BS (IDU+ODU)	Power consumption: 30W

1.6.5.3 Standalone Access Unit

1.6.5.3.1 Mechanical

Unit	Structure	Dimensions (cm)	Weight (kg)
General	An IDU indoor unit and an AU-D-BS-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
AU-D-SA-ODU	Pole or wall mountable	30.6 x 12 x 4.7	1.85
AU-Ant-4.9G-15-120	2"-4" pole mountable	55 x 25 x 1.7	1.5
AU-Ant-4.9G-9-Omni	1.5"-3" pole mountable	46 cm high, 5.5 cm base diameter	0.6

1.6.5.3.2 Connectors

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). 2 embedded LEDs in the PS1036
	AC IN	3-PIN AC power plug
AU-D-SA-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

1.6.5.3.3 Electrical

Table 1-15: Electrical Specifications, Stand Alone Access Unit	
Unit	Details
General	Power consumption: 25W
IDU	AC power input: 85-265 VAC, 50-60 Hz
AU-D-SA-ODU	54 VDC from the IDU over the indoor-outdoor Ethernet cable

1.6.5.4 Environmental

Table 1-16: Environmental Specifications		
Type	Unit	Details
Operating temperature	Outdoor units	-40 °C to 55 °C
	Indoor equipment	0 °C to 40 °C
Operating humidity	Outdoor units	5%-95% non condensing, weather protected
	Indoor equipment	5%-95% non condensing

Chapter 2 - Installation

In This Chapter:

- [Installation Requirements](#), page 22
- [Equipment Positioning Guidelines](#), page 26
- [Installing the Outdoor Unit](#), page 27
- [Installing the Universal IDU Indoor Unit](#), page 32
- [Installing the Modular Base Station Equipment](#), page 34

2.1 Installation Requirements

This section describes all the supplies required to install the BreezeACCESS 4900 system components and the items included in each installation package.

2.1.1 Packing List

2.1.1.1 Subscriber Unit

The SU installation kit includes the following components:

- IDU indoor unit with a wall mounting kit
- Mains power cord
- Outdoor Unit:
 - ◇ SU-A-ODU outdoor unit with an integrated vertically polarized antenna
- OR
- ◇ SU-E-ODU outdoor unit with a connection to an external antenna
- Pole mounting kit for the ODU
- 20m Category 5E indoor-to-outdoor Ethernet cable with shielded RJ-45 connectors

2.1.1.2 Modular Base Station Equipment

This section describes the items included in the installation packages for each Modular Base Station system component.

2.1.1.2.1 BS-SH Base Station Chassis

The BS-SH installation kit includes the following components:

- BS-SH chassis with blank panels
- Rubber legs for optional desktop installation

2.1.1.2.2 AU-D/E-BS Access Unit

The AU-D/E-BS and installation kit includes the following components:

- BS-AU Network Interface module

- AU-D/E-BS-ODU outdoor unit
- Pole mounting kit for the AU-D/E-BS-ODU
- In AU-D-BS kits: Antenna, including pole mounting hardware
- RF cable

2.1.1.2.3 BS-PS-AC Power Supply

Up to two BS-PS-AC power supply modules can be included in each Base Station chassis. The BS-PS-AC installation kit includes the following components:

- BS-PS-AC power supply module
- Mains power cord

2.1.1.2.4 BS-PS-DC Power Supply

Up to two BS-PS-DC power supply modules can be included in each Base Station chassis. The BS-PS-DC installation kit includes the following components:

- BS-PS-DC power supply module
- DC power cable

2.1.1.3 AU-D/E-SA Standalone Access Unit

The AU-D/E-SA installation kit includes the following components:

- IDU indoor unit with a wall mounting kit
- Mains power cord
- AU-D/E-SA-ODU outdoor unit with an integrated antenna
- Pole mounting kit for the AU-D/E-SA-ODU
- In AU-D-SA kits: Antenna, including pole mounting hardware
- RF cable

2.1.1.4 Additional Installation Requirements

The following items are also required to install the BreezeACCESS 4900 system components:

- Indoor-to-outdoor Category 5E Ethernet cable with shielded RJ-45 connectors * (available in different lengths. For more details refer to section [2.1.2](#))
- Ethernet cable (straight for connecting to a hub/switch etc., crossed for connecting directly to a PC's NIC)
- Crimping tool for RJ-45 connectors
- Antenna, for E model units supplied without an antenna
- 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 or BreezeCONFIG for BreezeACCESS 4900* application and a crossed Ethernet cable
- Installation tools and materials, including appropriate means (e.g. a pole) for installing the outdoor unit.

NOTE

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



2.1.2 Indoor-to-Outdoor Cables

NOTE

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

Use only Category 5E 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
Superior Cables Ltd. www.cvalim.co.il	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

2.2 Equipment Positioning Guidelines

This section provides key guidelines for selecting the optimal installation locations for the various BreezeACCESS 4900 system 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 BreezeACCESS 4900 product warranty and may expose the end user or Service Provider to legal and financial liabilities. Alvarion and its resellers or distributors are not liable for injury, damage or regulation violations associated with the installation of Outdoor Units or antennas.

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

- The outdoor unit can be either pole or wall mounted. Its location should enable easy access to the unit for installation and testing.
- The higher the placement of the antenna, the better the achievable link quality.
- AU-ODU units should be installed as close as possible to the antenna.
- The antenna connected to the AU-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 antenna of the SU (integrated on the front side of SU-A-ODU and SU-A-H-ODU unit) should be installed to provide a direct, or near line of sight with the Base Station antenna. The antenna should be aligned to face the Base Station.
- The indoor equipment should be installed as close as possible to the location where the indoor-to-outdoor cable enters the building. The location of the indoor equipment should take into account its connection to a power outlet and the CPE.

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 brackets and open-ended bolts are supplied with each unit. There are two pairs of threaded holes on the back of the unit, enabling the special brackets to be mounted on diverse pole 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 illustrates the method of mounting an outdoor unit on a pole, using the brackets and open-ended bolts.

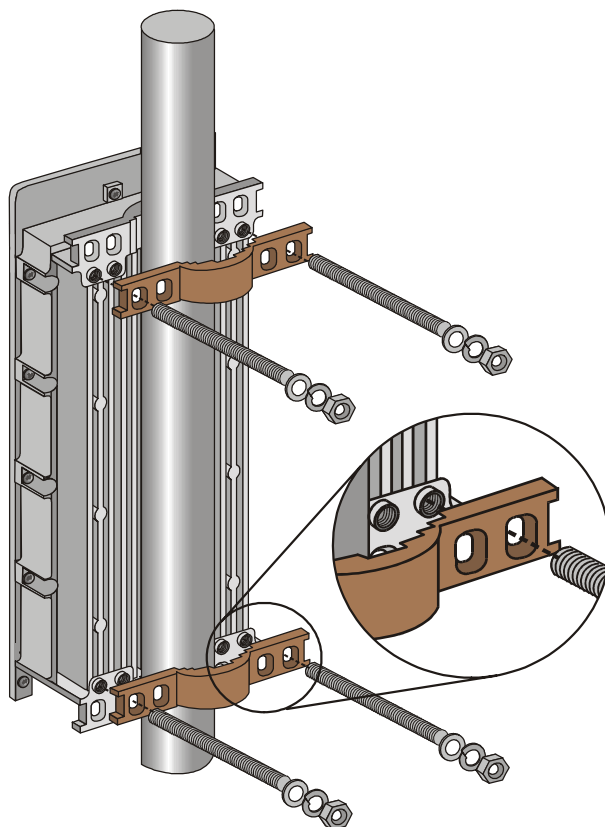


Figure 2-1: 3" Pole Installation Using Special Brackets

NOTE



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

2.3.2 Connecting the Grounding and Antenna Cables

The Grounding screw (marked \equiv) is located on the bottom panel of the outdoor unit. The Antenna RF connector (marked ∇) is located on the top panel of the AU-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 (units with external antenna):

- 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.

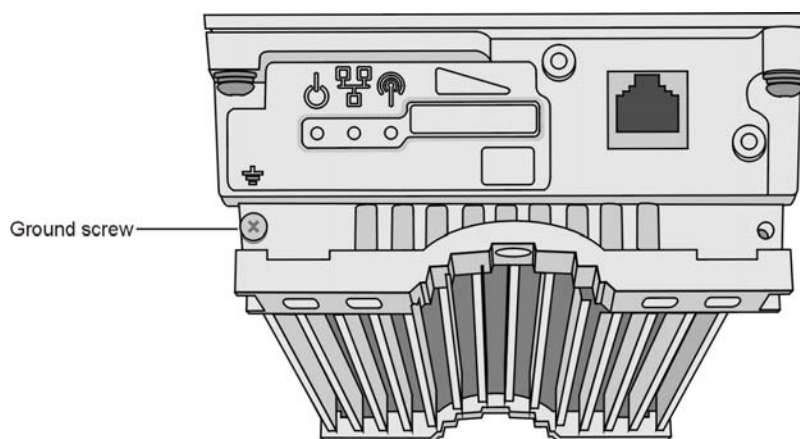


Figure 2-2: Bottom Panel of the Outdoor Unit (without the seal assembly)



NOTE

The MAC Address of the unit is marked on both the ODU and the indoor unit (on the print side of the BS-AU module or 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.

2.3.3 Connecting the Indoor-to-Outdoor Cable

2.3.3.1 Units with an Installed Waterproof Seal



To connect the indoor-to-outdoor cable:

- 1 Remove the two screws holding the waterproof seal to the outdoor unit and remove the waterproof seal.
- 2 Unscrew the top nut from the waterproof seal.

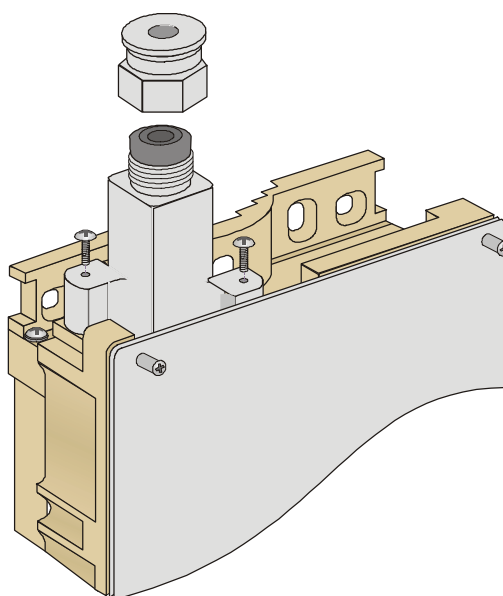


Figure 2-3: The Waterproof Seal

- 3 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](#).

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



2.3.3.2 Units with a Waterproof Seal Supplied with the Ethernet Cable



To connect the indoor-to-outdoor cable:

- 1 Verify that the o-ring supplied with the cable kit is in place.
- 2 Connect the RJ-45 connector of the Ethernet cable to the outdoor unit.
- 3 Attach the waterproof seal to the unit. Tighten the top nut.
- 4 Route the cable to the location selected for the indoor equipment.
- 5 Assemble an RJ-45 connector with a protective cover on the indoor end of the indoor-to-outdoor cable.

See [Appendix C](#) for instructions on preparing the 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. The drilling template included with the unit can be used to facilitate the wall installation process.

The equipment is shipped with a PS1073 IDU, shown in the following figure:

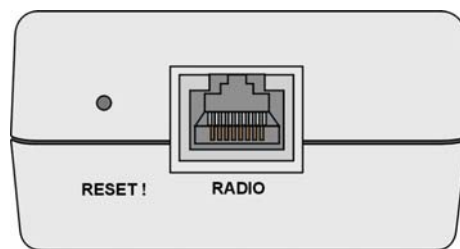


Figure 2-4: IDU PS 1073 Front Panel

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

**NOTE**

Reset the ODU using the RESET button on the IDU after connecting or reconnecting the indoor and outdoor units with the indoor-to-outdoor cable.

2.5 Installing the Modular Base Station Equipment

The following sections describe the slot assignment for the Base Station chassis, provide illustrated descriptions of the power supply modules and Access Unit network interface modules, and describe how to install the Base Station equipment.

2.5.1 BS-SH Slot Assignment

The Base Station chassis comprises ten slots, as shown in Figure 2-5.

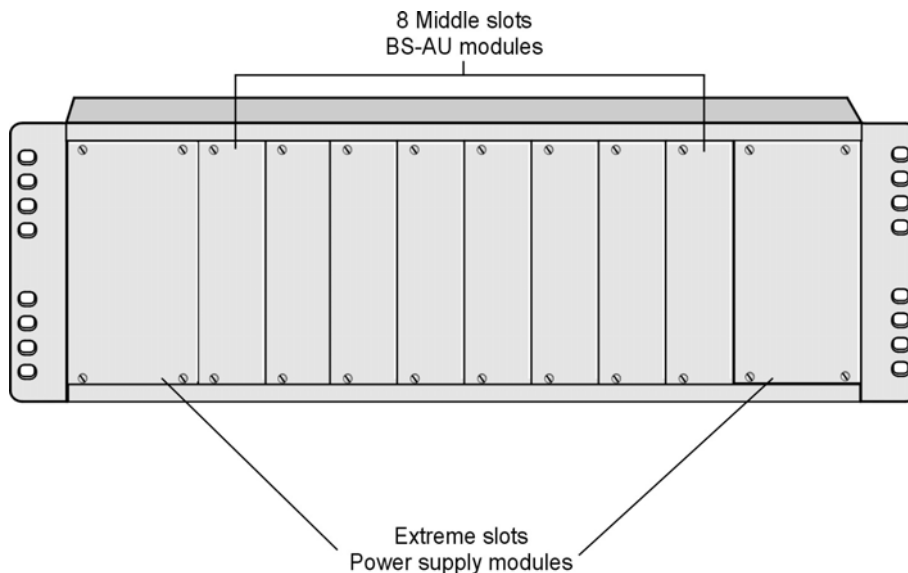


Figure 2-5: BS-SH Chassis Slot Assignment

To enable power supply redundancy, two BS-PS power supply modules can be installed in the wider side slots. If a single power supply module is used, it can be inserted into either one of the two available slots.

The remaining eight slots can hold up to six BS-AU modules. Unused slots should remain covered until required.

The design of the BS-SH supports collocation of BreezeACCESS 4900 Access Units with Access Units belonging to BreezeACCESS VL family or other BreezeACCESS families using GFSK modulation. It supports any mixture of BS-AU 4900 modules with BreezeACCESS VL or BreezeACCESS GFSK BS-AU modules, including an optional BS-GU-GPS module. If Access Units belonging to BreezeACCESS GFSK families are used, then it is necessary to use two power supply modules: one BS-PS (AC or DC) power supply for the BreezeACCESS 4900 Access Units and one BS-PS GFSK (AC or DC) for the BreezeACCESS GFSK

Access Units. The same BS-PS power supply modules can be used to power also BreezeACCESS VL BS-AU modules.

2.5.2 BS-PS-AC Power Supply Module

The BS-PS-AC is an AC to DC converter that provides power to all the BS-AU modules installed in the BS-SH chassis. Figure 2-6 shows the BS-PS-AC front panel.

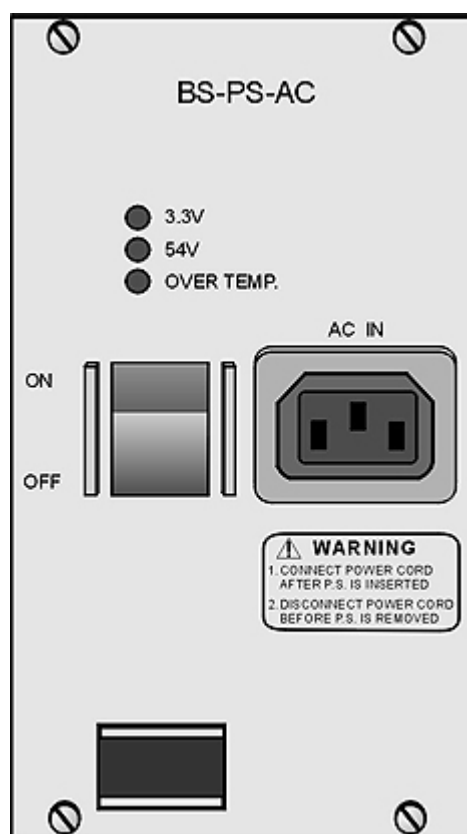


Figure 2-6: BS-PS-AC Front Panel

The BS-PS-AC includes a power input connector, marked AC IN, for connecting the AC power cord to the mains.

The ON/OFF Power Switch controls the flow of mains power to the power supply module.

Table 2-2: BS-PS LED Functionality	
Name	Description
54V	Green LED. Indicates that the 54V power supply module is OK
3.3V	Green LED. Indicates that the 3.3V power supply module is OK
OVER TEMP	Red LED. Indicates an over temperature condition in the power supply module

2.5.3 BS-PS-DC Power Supply Module

The BS-PS-DC is a DC-to-DC converter that provides power to all the BS-AU modules installed in the BS-SH chassis. Figure 2-7 shows the BS-PS-DC front panel.

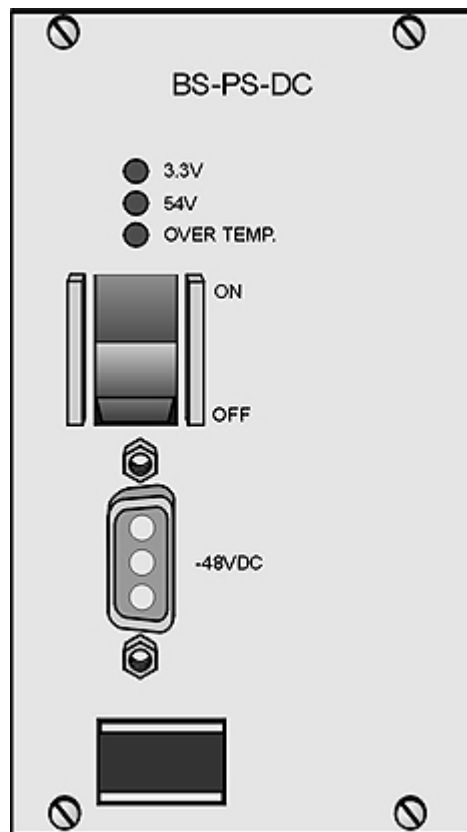


Figure 2-7: BS-PS-DC Front Panel

The BS-PS-DC provides a power input connector, marked -48VDC, for connecting the -48 VDC power source to the module.

The color codes of the cable wires are as follows:

- Black (pin 2): 48 VDC

- Red (pin 1): + (Return)
- Shield (pin 3)

The ON/OFF Power Switch controls the flow of mains power to the power supply module.

The functionality of the LEDs is described in Table 2-2.

2.5.4 BS-AU Network Interface Module

Figure 2-8 shows the front panel of the BS-AU Access Unit Network Interface module.

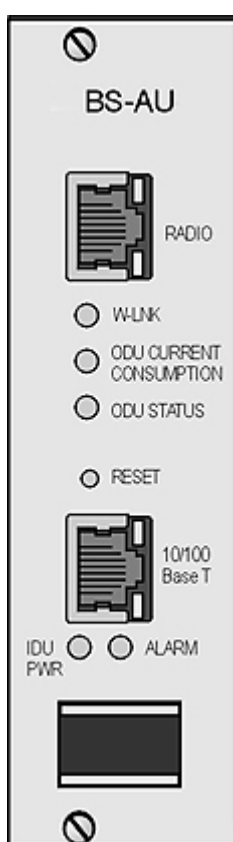


Figure 2-8: BS-AU Front Panel

The BS-AU provides the following interfaces:

- **10/100 BaseT:** A 10/100BaseT Ethernet connector for connecting the BS-AU to the network. A straight Ethernet cable should be used to connect the module to a hub, router or switch.
- **RADIO:** A 10/100BaseT Ethernet connector for connecting the BS-AU to an AU-ODU outdoor unit.



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.

The recessed **RESET** switch on the front panel is for resetting the outdoor unit.

2.5.5 Installing the BS-SH Chassis and Modules

This section describes how to install the power supply and Access Unit network interface modules in the Base Station chassis.



To install the BS SH chassis and modules:

- 1 Install the BS-SH chassis in a 19" cabinet. To prevent over-heating, leave a free space of at least 1U between the upper/lower covers of the BS-SH chassis and other units in the cabinet.

OR

Place the BS-SH chassis on an appropriate shelf or table. When mounting the BS-SH on a shelf or table, attach the rubber legs supplied with the unit.

- 2 Connect one end of a grounding cable to the ground terminal located on the rear panel of the BS-SH chassis and firmly tighten the grounding screw.
- 3 Connect the opposite end of the grounding cable to a ground connection or to the cabinet, if applicable.
- 4 Carefully insert the BS-PS power supply and the BS-AU modules into the relevant slots and push firmly until they are securely locked. Before insertion, verify that the switches of all BS-PS modules are in the OFF position. Refer to section [2.5.1](#) for a description of the slot assignment.
- 5 Close the captive screws attached to each module.
- 6 Place blank covers over all of the unused slots.
- 7 Connect the indoor-to outdoor cable(s) to the RADIO connector(s) of the BS-AU module(s).
- 8 If a BS-PS-DC power supply is used, connect the DC power cord to the -48 VDC IN jack of the BS-PS-DC power supply. If a redundant power supply module is installed, connect a DC power cord also to the second DC power module. Connect the power cord(s) to the -48 VDC power source, as follows:
 - a Connect the black wire to the 48 VDC contact of the power source.
 - b Connect the red wire to the + (Return) contact.
 - c Connect the shield to the ground.

- 9 If a BS-PS-AC power supply is used, connect the AC power cord to the AC IN jack of the BS-PS-AC power supply. If a redundant power supply module is installed, connect an AC power cord also to the second AC power module. Connect the power cord(s) to the mains outlet.
- 10 Switch the BS-PS-AC/DC power supplies to ON. Verify that all power indicator LEDs on the BS-PS-AC/DC front panel are ON and that the OVERTEMP alarm indicator is off. Refer to Table 2-2 for a description of these LEDs.
- 11 Configure the basic parameters in all BS-AU modules as described in section [3.1](#).
- 12 Connect the 10/100 BaseT LAN connector(s) to the network. The cable connection should be 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 each of the Ethernet cables (the cable connecting the indoor unit to the user's equipment and the Indoor-to-Outdoor cable) should not exceed 100 meters.
- Reset the unit using the RESET button after connecting or reconnecting the indoor and outdoor units with the indoor-to-outdoor cable.

Chapter 3 - Commissioning

About This Chapter:

- [Configuring Basic Parameters](#), page 42
- [Aligning the Subscriber Unit Antenna](#), page 45
- [Configuring the Subscriber Unit's Maximum Modulation Level](#), page 46
- [Operation Verification](#), page 48

3.1 Configuring Basic Parameters

After completing the installation process, as described in the preceding chapter, the basic parameters must be configured to ensure that the unit operates correctly. 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 Subscriber and 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.

Parameter	Default Value	Comment
Ethernet Port Negotiation Mode (in Unit Control Parameters)	Auto Negotiation	
IP Address	10.0.0.1	
Subnet Mask	255.0.0.0	
Default Gateway Address	0.0.0.0	
DHCP Options	Disable	
Access to DHCP	AU: From Ethernet Only SU: From Wireless Only	
ESSID	ESSID1	
Sub-Band Select	1	
Frequency Subset Definition (SU)	A (All)	The list of frequencies is in accordance with the Sub-Band.

Table 3-1: Basic Parameters		
Parameter	Default Value	Comment
Tx Power for Modulation Levels 1 to 5, Tx Power for Modulation Level 6, Tx Power for Modulation Level 7, Tx Power for Modulation Level 8	Dependent on Sub-Band	Tx Power cannot be higher than the applicable Maximum Tx Power parameter.
Maximum Tx Power for Modulation Levels 1 to 5 (SU), Maximum Tx Power for Modulation Level 6 (SU), Maximum Tx Power for Modulation Level 7 (SU) Maximum Tx Power for Modulation Level 8 (SU)	Dependent on Sub-Band	Max Tx Power cannot be higher than the upper limit according to the Sub-Band in use.
Tx Power (AU)	On	
Antenna Gain (units with external antenna)	According to the antenna supplied with the unit and the Sub-Band.	If set to "Not Set Yet", must be configured according to actual value, taking into account cable's attenuation.
ATPC Option	Enable	
Best AU Support (SU)	Disable	
Preferred AU MAC Address (SU)	00-00-00-00-00-00 (none)	Applicable only when Best AU Support is enabled.
Cell Distance Mode (AU)	Automatic	
Maximum Cell Distance (AU)	0 (No Compensation)	
Maximum Modulation Level (SU)	8	Refer to section 3.3 .
VLAN ID-Management	65535	
Authentication Algorithm	Open System	

Parameter	Default Value	Comment
Data Encryption Option	Disable	
Security Mode	WEP	
Default Multicast Key (AU)	Key 1	
Promiscuous Authentication (AU)	Disable	
Default Key (SU)	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.

3.2 Aligning the Subscriber Unit Antenna

The SNR bar display is located on the bottom panel of the outdoor unit. The ten LEDs indicate the quality of the received signal. The higher the number of green LEDs indicating On, the higher the quality of the received signal. This section describes how to align the Subscriber Unit antenna using the SNR bar display.



NOTE

Antenna alignment using the SNR bar display is possible only after the Subscriber Unit is associated with an Access Unit. The associated Access Unit must be operational and the basic Subscriber Unit parameters must be correctly configured. Otherwise, the unit will not be able to synchronize with the Access Unit. As the SNR measurement is performed on received frames, its results are meaningless unless the Subscriber Unit is associated with an Access Unit.



To align the Subscriber Unit antenna:

- 1 Align the antenna by pointing it in the general direction of the Base Station.
- 2 Verify that the power indication of the unit is **On**.
- 3 Verify that the W-LINK LED of the ODU is **On**, indicating that the unit is associated with an Access Unit. If the W-LINK LED is **Off**, check that the **ESSID** and **Frequency** parameters are correctly configured. If the SU is still not associated with the AU, increase the transmit power level to its maximum value. If the unit is still not associated with the AU, improve the quality of the link by changing the direction of the antenna or by placing the antenna at a higher or alternate location.
- 4 Rotate the antenna until the maximum SNR reading is achieved, where at least 1 green LED is on. If you encounter prolonged difficulty in illuminating the minimum required number of green LEDs, try to improve the reception quality by placing the antenna at a higher point or in an alternate location.
- 5 Ensure that the front of the antenna is always facing the Base Station. However, in certain conditions, such as when the line of site to the Base Station is hampered, better reception may be achieved using a reflected signal. In this case, the antenna is not always directed toward the Base Station.
- 6 Secure the unit firmly to the pole.



NOTE

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

3.3 Configuring the Subscriber Unit's Maximum Modulation Level

This section describes how to configure the maximum modulation level for Subscriber Units.



NOTE

If the unit is associated with the AU, then the final configuration of the Maximum Modulation Level parameter may be performed remotely, for example, from the site of the AU or from another site.



To configure the Maximum Modulation Level:

- 1 If the SNR of the SU at the AU is too low, it is recommended that you configure the *Maximum Modulation Level* parameter to a value that is lower than the maximum supported by the unit. This can decrease the number of retransmissions due to attempts to transmit at modulation levels that are too high for the actual quality of the link.
- 2 Check the SNR of the SU at the AU. You can use Telnet to view the SNR values in the *MAC Address Database*, which can be accessed from the *Site Survey* menu. If the ATPC algorithm is not enabled in both AU and SU, the test should be done with the *Initial Power Level* at the SU configured to its maximum value. If the SNR is lower than the values required for the maximum modulation level according to Table 3-2, it is recommended that you decrease the value of the Maximum Modulation Level.



NOTE

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

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

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

3.4 Operation Verification

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

3.4.1 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 and alignment processes are completed.

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.

Name		Description	Functionality
W-LINK		Wireless Link Indicator	<ul style="list-style-type: none"> ■ Green – Unit is associated with an AU, no wireless link activity ■ Blinking Green – Data received or transmitted on the wireless link. Blinking rate is proportional to wireless traffic rate ■ Off – Wireless link 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 between the indoor and outdoor units is detected, no activity ■ Blinking Green – Ethernet connectivity is OK, with traffic on the port. Blinking rate proportional to traffic rate. ■ Red – No Ethernet connectivity between the indoor and outdoor units.
SNR BAR (SU-RA)		Received signal strength Indication	<ul style="list-style-type: none"> ■ Red LED: Signal is too low (SNR < 4 dB) ■ 8 green LEDs: Quality of the received signal ■ Orange LED: Signal is too high (SNR > 50 dB)

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

3.4.2 Indoor Unit Verification

To verify the correct operation of the indoor equipment, examine the LED indicators located on the top panel of the SU IDU and AU IDU units, or on the front panel of the BS-AU module.

[Table 3-6](#) provides information for the BS-AU IDU LEDs. [Table 3-7](#) lists the LEDs of the PS1073 IDU and their associated indications.

Name	Description	Functionality
W-LINK	Wireless link activity	<ul style="list-style-type: none"> ■ Green - At least one SU is associated. ■ Blinking Red - No SU is associated. ■ Off - Wireless link is disabled.
ODU CURRENT CONSUMPTION	Current Consumption of the Outdoor Unit	<ul style="list-style-type: none"> ■ Red - over current. ■ Blinking Red - open circuit or below anticipated current consumption. ■ Green - within tolerance.
ODU STATUS	Outdoor Unit Self-test	<ul style="list-style-type: none"> ■ Green - Self test passed and ODU ready for operation. ■ Blinking Amber - Testing (not ready for operation) ■ Red - fatal failure.
IDU PWR	Power indication for the Indoor Unit	<ul style="list-style-type: none"> ■ Green - IDU power is OK. ■ Off - no power is supplied to the IDU.
ALARM	Indoor Unit Alarm Indication	<ul style="list-style-type: none"> ■ Red - a fatal failure indication. ■ Off - IDU is functioning properly.

Name	Description	Functionality
POWER	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).

3.4.3 Verifying the Ethernet Connection (Modular Base station)

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

3.4.4 Verifying the Indoor-to-Outdoor Connection (Modular Base Station)

After connecting the unit to an Ethernet outlet, verify that the Ethernet Integrity Indicator, which is the yellow LED embedded in the **RADIO** connector, is on. This indicates that the unit has detected an Ethernet link connection. The Ethernet Activity Indicator, which is the green embedded LED, should blink whenever the unit receives or transmits traffic on the **RADIO** port.

3.4.5 Verifying Data Connectivity

To verify data connectivity, from the end-user's PC or from a portable PC connected to the unit, ping the Access Unit, or try to connect to the Internet.

Chapter 4 - Operation and Administration

In This Chapter:

- [Working with the Monitor Program](#), page 54
- [Menus and Parameters](#), page 57

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.

Access Rights	Password
Read-Only	public
Installer	user
Administrator	private



NOTE

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

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


```

BreezeACCESS 4900/AU-SA-4900
Official Release Version - 3.2.3
Release Date: June 14 2005, 17:10:21
Main Menu
=====
1 - Info Screens
2 - Unit Control
3 - Basic Configuration
4 - Site Survey
5 - Advanced Configuration
x - Exit
>>>

```

Figure 4-1: Main Menu (Administrator Level)



NOTE

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

The 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 click **Enter**.
- Click Esc to exit a menu or option.



NOTE

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

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

4.2 Menus and Parameters

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 including the encryption Keys, ESSID and Operator ESSID are only displayed to users with Administrator access rights.

The Info Screens menu includes the following options:

- Show Unit Status
- Show Basic Configuration

- Show Advanced Configuration
- Show Country Dependent Parameters
- Show All Parameters

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:** Identifies the unit's function: AU-BS (a modular access unit), AU-SA (a stand-alone access unit), or SU-BD (a subscriber unit that supports a gross CPE rate of 27 Mbps and a full LAN).
- **Unit MAC Address:** The unit's unique IEEE MAC address.
- **Current Number of Associations (AU only):** 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 conditions:

- A SNAP frame is received from another AU indicating that the SU is now associated with the other AU.
- 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:** For SUs - displays the total number of associations with any AU since the last reset, including duplicate associations with the same AU. For AUs - displays the number of SUs that have associated with the AU since the last reset, including duplicate associations with the same SU.
- **Unit Status (SU only):** The current status of the SU. There are two status options:
 - ◇ **SCANNING:** The SU is searching for an AU with which to associate.
 - ◇ **ASSOCIATED:** The SU is associated with an AU.



- **AU MAC Address (SU only):** The MAC address of the AU with which the unit is currently associated. If the unit is not associated with any AU, the address defaults to the IEEE broadcast address, which is FF-FF-FF-FF-FF-FF.
- **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.
- **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 Client IP Address
- ◇ FTP Client IP Mask
- ◇ FTP Server IP Address
- ◇ FTP Gateway IP Address
- ◇ FTP User Name
- ◇ FTP Password

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

- ◇ FTP Source Directory
- ◇ FTP SW Version File Name

- **Configuration File Download/Upload Parameters:** The parameters for Configuration file upload/download using FTP, as defined in 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 Policy**

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

The Country Dependent Parameters displays the parameters that are affected by applicable regulations. BreezeACCESS 4900 supports two sets of frequencies (Sub-Bands). For each of these Sub-Bands, there is a set of parameters that reflects the applicable radio regulations. In addition, there are several general parameters that reflect availability of various security options. The Country Dependent Parameters include the following:

- **Country Code:** 1022 – FCC 4.9 GHz.
- **Data Encryption Support:** Supported.
- **AES Encryption Support:** Supported.
- **Authentication Encryption Support:** Supported.
- **Sub-Band Dependent Parameters:**

Parameter	Sub-Band 1	Sub-Band 2
Sub-Band ID	1	2
Frequencies	4947.5 - 4982.5 MHz, 5 MHz steps	4947.5 - 4982.5 MHz, 5 MHz steps
Allowed Bandwidth	10 MHz	5 MHz
Regulation Max Tx Power at Antenna Port	20 dBm	17 dBm
Regulation Max EIRP	AU: 46 dBm SU: No Limit	AU: 43 dBm SU: No Limit
Min Modulation Level	1	1
Max Modulation Level	8	8
Burst Mode	Enabled	Enabled

Parameter	Sub-Band 1	Sub-Band 2
Maximum Burst Duration	10 milliseconds	10 milliseconds
DFS Option	Not Supported	Not Supported
Minimum HW Revision Support	D	D

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, including the encryption Keys, ESSID and Operator 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:

- Reset Unit
- Default Settings
- Change Unit Name
- Change Password
- Flash Memory Control
- SW Version Download
- Configuration File Upload/Download
- Log Out Timer
- Ethernet Port Negotiation Mode
- Change System Location

- Event Log Menu

- Feature Upgrade

4.2.3.1 Reset Unit

The Reset Unit 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 [4.2.3.7](#) 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 4-3.

Parameters Group	Parameter
Unit Control Parameters	All Passwords
	FTP Server IP address* (see note below)
	FTP Gateway IP address* (see note below)
	FTP Client IP address* (see note below)
	FTP Client IP Mask* (see note below)
	FTP User Name* (see note below)
	FTP Password* (see note below)
	Ethernet Port Negotiation Mode
Air Interface Parameters	Selected Sub-Band
	Frequency (AU)
	Frequency Subset (AU)
	Antenna Gain (AU)

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 4-4.

Parameters Group	Parameter
Unit Control parameters	Passwords
	Ethernet Port Negotiation Mode
	FTP Server IP address
	FTP Gateway IP Address
	FTP Client IP address
	FTP Client IP Mask
	FTP User Name
	FTP Password
IP Parameters	IP Address
	Subnet Mask
	Default Gateway Address
	DHCP Option
	Access to DHCP
Security Parameters	Authentication Algorithm
	Default Key (SU)
	Data Encryption Mode
	Default Multicast Key (AU)
	Security Mode
	Key # 1 to Key # 4
Air Interface Parameters	ESSID
	Operator ESSID Option (AU)
	Operator ESSID (AU)
	Cell Distance Mode (AU)
	Maximum Cell Distance (AU)
	Selected Sub-Band

Parameters Group	Parameter
	Frequency (AU)
	Frequency Subset (SU)
	ATPC Option (AU)
	Transmit Power
	Tx Control (AU)
	Best AU Support (SU)
	Preferred AU MAC Address (SU)
Performance Parameters	Adaptive Modulation Decision Thresholds
Bridge Parameters	VLAN ID – Management
	MAC Address Deny List (AU)

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 4-3.

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 4-4.

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 you 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 SW Version Download

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

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

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

The default is an empty string.

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

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

The default is VxWorks.bz.

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

The default is: 1.1.1.3

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

The default is: 255.255.255.0

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

The default is: 1.1.1.4.

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

The default is: 0.0.0.0.

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

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

The default is: vx

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

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

The default is: vx

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



NOTE

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

4.2.3.7 Configuration File Upload/Download

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

- **Execute FTP GET/PUT Configuration File:** The Execute FTP GET/PUT Configuration File executes the upload/download of a Configuration file or an Operator Defaults file according to the parameters defined below. The following options are available:
 - ◇ Execute FTP Get Configuration File (cfg)
 - ◇ Execute FTP Put Configuration File (cfg)
 - ◇ Execute FTP Get Operator Defaults File (cmr)
 - ◇ Execute FTP Put Operator Defaults File (cmr)

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

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

The default is an empty string.

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

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

The default is config.cfg.

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

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

The default is operator.cmr.

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

The default is: 1.1.1.3

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

The default is: 255.255.255.0

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

The default is: 1.1.1.4

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

The default is: 0.0.0.0.

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

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

The default is: vx

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

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

The default is: vx

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



NOTE

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

4.2.3.8 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.

4.2.3.9 Ethernet Port Negotiation Mode

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

- Force 10 Mbps and Half-Duplex
- Force 10 Mbps and Full-Duplex
- Force 100 Mbps and Half-Duplex
- Force 100 Mbps and Full-Duplex

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

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

4.2.3.10 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.

4.2.3.11 Event Log Menu

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

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

The Event Log Menu includes the following options:

- Event Log Policy
- Display Event Log
- Erase Event Log
- Event Load Upload

4.2.3.11.1 Event Log Policy

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

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

The default selection is Warning Level severity.

4.2.3.11.2 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 in descending order, with the most recent event displayed first.

4.2.3.11.3 Erase Event Log

The Erase Event Log option enables clearing the event log.

4.2.3.11.4 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: 1.1.1.4

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

The default is: 0.0.0.0.

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

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

The default is: vx

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

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

The default is: vx

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



NOTE

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

4.2.3.12 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](#)).

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:

4.2.4.1.1 IP Parameters

- IP Address
- Subnet Mask
- Default Gateway Address
- DHCP Client
 - ◇ DHCP Option
 - ◇ Access to DHCP

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

4.2.4.1.2 Air Interface Parameters

- ESSID
 - Operator ESSID Parameters (AU)
 - ◇ Operator ESSID Option
 - ◇ Operator ESSID
- Frequency Definition
 - ◇ Select Sub-Band (if more than one is available)
 - ◇ Frequency (AU)
 - ◇ Sub-Band Definition
- Best AU Parameters (SU)
 - ◇ Best AU Support
 - ◇ Preferred AU MAC Address
- Cell Distance Parameters
 - ◇ Cell Distance Mode (AU)
 - ◇ Maximum Cell Distance (AU)

- ATPC
 - ◇ ATPC Option
- Transmit Power parameters
- Maximum Transmit Power parameters (SU)
- Tx Control (AU)
- Antenna Gain (AU)

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

4.2.4.1.3 Performance Parameters

- Maximum Modulation Level (SU)

Refer to section [4.2.6.5](#) for a description of these parameters.

4.2.4.1.4 Bridge Parameters

- VLAN ID – Management
- MAC Address Deny List

Refer to section [4.2.6.4](#) for a description of these parameters.

4.2.4.1.5 Security Parameters

- Authentication Algorithm
- Data Encryption Option
- Security Mode
- Default Multicast Key (AU)
- Default Key (SU)
- Key 1 to Key 4
- Promiscuous Authentication (AU)

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.

4.2.5 Site Survey Menu

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

The Site Survey menu includes the following options:

- Traffic Statistics
- Ping Test
- Continuous Link Quality display (SU only)
- MAC Address Database
- 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 a regular

IEEE 802.1 Ethernet frame that can be accepted from the Ethernet port is 1518 bytes. For tagged IEEE 802.1Q frames the maximum size is 1522 bytes.

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/CIR mechanism (for more information see section [4.2.6.6.3](#)).

Broadcasts/multicasts are routed to the Medium queue (applicable only for AU).

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 4900 unit via the wireless port (as opposed to messages intended

for stations behind other BreezeACCESS 4900 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 (AU only)
 - ◇ Management and Other Data frames, including successfully transmitted unicast frames and multicast/broadcast data frames (excluding retransmissions, excluding Beacons in AU)
- **Total Transmitted Unicasts (AU only):** 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:** 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 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.
 - **Total received concatenated frames:** The total number of concatenated frames received from the wireless medium, including duplicate frames. 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 pinging from the unit and includes the following options:

- **Destination IP Address:** The destination IP address of the device being pinged. The default IP address is 192.0.0.1.
- **Number of Pings to Send:** The number of ping attempts per session. The available range is from 0 to 9999. The default value is **1**. Select 0 for continuous pinging.
- **Ping Frame Length:** The ping packet size. The available range is from 60 to 1472 bytes. The default value is 64 bytes.
- **Ping Frame Timeout:** The ping frame timeout, which is the amount of time (in ms) between ping attempts. The available range is from 100 to 60,000 ms. The default value is 200 ms.
- **Start Sending:** Starts the transmission of ping frames.
- **Stop Sending:** Stops the transmission of ping frames. The test is automatically ended 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 pinging is selected.
- **Show Ping Test Values:** Displays the current values of the ping test parameters, the transmission status, which means whether it is currently

sending or not sending pings, the number of pings sent, and the number of pings received, which means the number of acknowledged frames.

4.2.5.3 Link Quality (SU only)

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

4.2.5.3.1 Continuous Average SNR Display

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

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

4.2.5.3.2 Continuous UpLink Quality Indicator Display

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

$$\text{LQI} = (0.9 \times \text{"Previous LQI"}) + (0.1 \times \text{"Last Successful Modulation Level"})$$

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

In order to receive quick and reliable LQI measurements, there should be sufficient traffic between the SU and the AU. It is recommended to have traffic of at least 100 packets per second. The traffic can be generated either by an external utility (FTP session, ping generator, etc.) or by the Ping Test option in the Site Survey menu with the appropriate settings (see section [4.2.5.2](#)).



NOTE

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

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

4.2.5.4 MAC Address Database

The MAC Address Database submenu includes the following options:

- MAC Address Database in AU
- MAC Address Database in SU

4.2.5.4.1 MAC Address Database in AU

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

- **Display Bridging and Association Info:** The Display Bridging and Association Info option displays a list 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 are also displayed: SU Unit Name, SU SW version, SU Unit Type and SU's Distance from the AU.
- ◇ **X:** An SU that is included in the Deny List.
- ◇ **Sp (Special):** 7 addresses that are always present, including:
 - The MAC address of the AU, which appears twice as it is learned from both the Ethernet and wireless ports.
 - The MAC address of the internal Operating System stack, which also appears twice.
 - Alvarion's Multicast address (01-20-D6-00-00-01, which also appears twice. The system treats this address as a Broadcast address.
 - The Ethernet Broadcast address (FF-FF-FF-FF-FF-FF).

In addition, a summary table displays information about the Forwarding Database (Bridging Info) and the Associated 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.



NOTE

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

- A SNAP frame is received from another AU indicating that the SU is now associated with the other AU.
 - The SU failed to respond to 50 consecutive frames transmitted by the AU and is considered to have "aged out".
-
- ◇ The aging time specified for entries in these tables. The aging time for Bridging Info is as specified by the **Bridge Aging Time** parameter. The default is 300 seconds. There is no aging time for Association Info entries.
 - ◇ The maximum number of entries permitted for these tables, which are 1017 (1024 minus the number of special Sp addresses as defined above) for Bridging Info and as specified by the **Maximum Number of Associations** parameter for Association Info. The default value of the Maximum Number of Associations parameter is 512.

**NOTE**

When Data Encryption is enabled, the actual maximum number of associations is limited to 124. The displayed number is the value configured for the Maximum Number of Associations parameter, which might be higher than the actual limit.

■ **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
- ◇ 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 4-5: Authentication and Association Process		
Message	Direction	Status in AU
SU Status: Scanning		
A Beacon with correct ESSID	AU → SU	-
SU Status: Synchronized		
Authentication Request	SU → AU	Not authenticated
Authentication Successful	AU → SU	Authenticated
SU Status: Authenticated		
Association Request	SU → AU	Authenticated

Table 4-5: Authentication and Association Process		
Message	Direction	Status in AU
Association Successful	AU → SU	Associated
SU Status: Associated		
ACK	SU → AU	Associated
Data Traffic	SU ↔ AU	Associated

- ◇ The SNR measured at the SU
- ◇ The Unit Name of the SU.
- ◇ The SW version of the SU.
- ◇ The Unit Type of the SU.
- ◇ Distance.

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.

NOTE



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

- A SNAP frame is received from another AU indicating that the SU is now associated with the other AU.
 - The SU failed to respond to 50 consecutive frames transmitted by the AU and is considered to have "aged out".
- ◇ The aging time specified for entries in these table. There is no aging time for Association Info entries.
 - ◇ The maximum number of entries permitted for this table, which is specified by the **Maximum Number of Associations** parameter. The default value of the **Maximum Number of Associations** parameter is 512.

- **Show MIR/CIR Database:** Displays information on the MIR/CIR support for associated Subscriber Units.

Each entry includes the following information:

- ◇ The MAC address of the associated Subscriber Unit
 - ◇ The values of the MIR and CIR parameters configured in the applicable SU for the downlink (AU to SU) and for the uplink (SU to AU).
 - ◇ The value configured in the applicable SU for the Maximum Delay parameter.
 - ◇ The maximum data rate of the Subscriber Unit
- **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.

4.2.5.4.2 MAC Address Database in SU

The **MAC Address Database** option in the SU displays information regarding the Subscriber Units bridging (forwarding) information. The following option is available:

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

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

- ◇ **Et (Ethernet):** An address learned from the Ethernet port.
- ◇ **Wl (Wireless):** An address of a node behind the associated AU, learned via the wireless port.
- ◇ **Sp (Special):** 8 addresses that are always present, including:
 - The MAC address of the SU, which appears twice as it is learned from both the Ethernet and wireless ports.
 - The MAC address of the internal Operating System stack, which also appears twice.

- Alvarion's Multicast address (01-20-D6-00-00-01), which also appears twice. The system treats this address as a Broadcast address.
- Alvarion's special Multicast address (01-20-D6-00-00-05), reserved for future use.
- The Ethernet Broadcast address (FF-FF-FF-FF-FF-FF).

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

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 Counters:** Select this option to display the current values of the Per Modulation Level Counters.
- **Reset Counters:** Select this option to reset the Per Modulation Level Counters.

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

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

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

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

For AUs, the **SUCCESS** and **FAILED** counts are provided for each of the associated SUs, which are identified by their MAC address.

4.2.5.6 Link Capability

The Link Capability option provides information on HW and SW capabilities of relevant units. In an AU, the information provided in the Link Capability reports

is for all associated SUs. In an SU, the Link Capability reports include information on all AUs in the neighboring AUs table (all AUs with whom the SU can communicate).

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

The Link Capability submenu 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. This parameter is available only in AUs, displaying the CPLD version in the relevant SU.
- **Country:** The 3 or 4 digits country code supported by the unit. Currently this value is 1022.
- **SwVer:** The SW version used by the unit. This parameter is available only in SUs, displaying the SW version in the relevant AU.
- **BootVer:** The Boot Version of the unit. This parameter is available only in AUs, displaying the Boot version in the relevant SU.

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.
- **Country Code Learning by SU:** Enable or Disable. This parameter is available only in SUs, displaying the current option in the relevant AU.

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, AES/OCB or AES/CCM.
- **Authentication Algorithm:** Shared Key or Open System.
- **Data Encryption Option:** Enable or Disable.

4.2.5.6.4 Show Link Capability by AU (SU only)

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

4.2.5.6.5 Show Link Capability by SU (AU only)

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

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

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 for Access Units is From Ethernet Only. The default for Subscriber Units is From Wireless Link 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 Parameters

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

4.2.6.2.1.1 ESSID

The ESSID parameter defines the ESSID of the unit.

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

The default value is ESSID1.

NOTE



The ESSID string is case sensitive.

4.2.6.2.1.2 Operator ESSID Parameters (AU only)

The Operator ESSID Parameters submenu includes the following parameters:

4.2.6.2.1.2.1 Operator ESSID Option

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

The default is Enable.

4.2.6.2.1.2.2 Operator ESSID

The Operator ESSID parameter defines the Operator ESSID.

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

The default value is ESSID1.

NOTE



The Operator ESSID string is case sensitive.

4.2.6.2.2 Frequency Definition Parameters

4.2.6.2.2.1 Sub-Bands and Frequency Selection

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.

To simplify the installation process the SU scans a definable frequencies subset after power-up. If the Best AU feature is enabled, the SU will scan the defined subset and the operating frequency 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.

Each unit is delivered with two 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 sub-band to be used can be selected in both the AU and the SU.

4.2.6.2.3 Frequency Definition Submenu in AU

The Frequency Definition submenu in AU includes the following parameters:

4.2.6.2.3.1 Sub-Band Select

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](#).

The available options are 1 and 2.

The default selection is Sub-Band 1.

4.2.6.2.3.2 Frequency

The Frequency parameter defines the transmit/receive frequency.

The range depends on the selected Sub-Band.

The default is the lowest frequency in the Sub-Band. In the current version, the default frequency for both Sub-Bands is 4947.5 MHz.

4.2.6.2.3.3 Country Code Learning by SU

This feature support simplified installation and updates processes by enabling the SU to adapt the Country Code used by the AU.

The AU advertises its country code in every beacon and association response message. Upon synchronization the SU will check if its country code and the country code received from the AU are the same. If they are not the same and the

Country Code Learning by SU is enabled, the SU will use the AU's country code: the country code derived limitations will be forced and the following parameters will be set according to new country definitions:

- Maximum TX Power (per modulation level) will be set to the maximum defined by the country code.
- TX Power (per modulation level) will be set to the maximum defined by the country code.
- The Modulation Level will be set to the maximum modulation level defined by the country code.
- The Multicast Modulation Level will be set to the minimum modulation level defined by the country code.
- The Burst Mode will be set to enable if the country code supports burst mode, and the burst duration will be set to default.

After country code learning (adaptation) the unit is automatically reset. Before this automatic reset, if the unit is running from the shadow version, the versions must be swapped and the running version must be set as main. This is done to avoid returning to the previous version, which occurs automatically after the reset.

The default is Enable.

NOTE

The Country Code Learning by SU feature does not function with the default ESSID (ESSID1).



4.2.6.2.3.4 Show Frequency definitions

Upon selecting Show Frequency Definitions, the selected Sub-Band and Frequency are displayed.

4.2.6.2.4 Frequency Definition Submenu in SU

4.2.6.2.4.1 Sub-Band Select

This parameter is available only if the country code supports two or more Sub-Bands. For information on how to view the Sub-Bands supported by the unit and the supported parameters' values and options, refer to section [4.2.2.4](#).

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

The default selection is Sub-Band 1.

4.2.6.2.4.2 Frequency Subset Definition

The Frequency Subset Definition parameter defines the frequencies that will be used by the SU when scanning for an AU. 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.

4.2.6.2.4.3 Show Frequency Definitions

Upon selecting the Show Frequency Definitions, the selected Sub-Band 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.

4.2.6.2.5 Best AU Parameters (SU)

An SU that can communicate with more than one AU using the same ESSID may become associated with the first AU it "finds", not necessarily the best choice in terms of quality of communication. The same limitation also exists if only one AU in the neighborhood has an ESSID identical to the one used by the SU, as it is not always necessarily the best choice.

The topology of a fixed access network is constantly changing. Changes in base station deployment and subscriber density can accumulate to create substantial changes in SU performance. The quest for load sharing together with the desire to create best throughput conditions for the SU created the need for the Best AU feature, to enable an SU to connect to the best AU in its neighborhood.

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

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

NOTE



Although the SU selects the Best AU based on long-term conditions prior to the decision time, it may not always be connected to the instantaneous Best AU at any given time. Note also that the decision is made only once during the scanning interval. The decision may not remain the optimal one for ever. If there are significant changes in deployment of neighboring AUs and the SUs served by them, overall performance may be improved if the applicable SUs are reset intentionally so as to re-initiate the Best AU decision process.

The Best AU Parameters menu includes the following options:

4.2.6.2.5.1 Best AU Support

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

The default is Disable.



NOTE

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

4.2.6.2.5.2 Number Of Scanning Attempts

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

Valid values: 1 - 255.

Default value: 4.

4.2.6.2.5.3 Preferred AU MAC Address

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

Valid values: A MAC address string.

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

4.2.6.2.5.4 Show Best AU Parameters and Data

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

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

■ MAC Address

- **SNR** of the received signal
- **Mark** - The computed quality mark for the AU.
- **Full** - The association load status of the AU. It is defined as full if the number of SUs associated with the AU has reached the maximum allowed according to the value of the **Maximum Number of Associations** parameter. An AU whose associations load status is full cannot be selected as the Best AU, even if its computed mark is the highest.
- **ESSID** - The ESSID of the AU.

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

- **Best AU Support**
- **Preferred AU MAC Address**
- **Number of Scanning Attempts**
- **Associated AU MAC Address** (the MAC address of the selected AU)

4.2.6.2.6 Scanning Mode (SU only)

The Scanning Mode parameter defines whether the SU will use Passive or Active scanning when searching for an AU.

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

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

The default selection is Passive.

4.2.6.2.7 Power Control Parameters

The Automatic Transmit Power Control (ATPC) algorithm simplifies the installation process and ensures optimal performance while minimizing interference to other units. This is achieved by automatically adjusting the power level transmitted by 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.

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

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

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

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

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

4.2.6.2.7.1 Transmit Power

The Transmit Power parameters are defined separately for different modulation levels.

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

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

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

- The modulation level
- The Maximum Allowed Tx Power as defined for the applicable Sub-Band.
- The Maximum EIRP as defined for the applicable Sub-Band, together with the value of the Antenna Gain. The Maximum EIRP of AUs (defined as Point-to-Multi-Point equipment) cannot exceed a certain value. In these cases the Transmit Power cannot exceed the value of (Maximum EIRP – Antenna Gain).
- Maximum Tx Power parameter (in SU only)

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](#).

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

The default Transmit Power is the highest allowed value.

4.2.6.2.7.2 Maximum Tx Power (SU only)

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

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

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

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](#).

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

The default Maximum Tx Power is the highest allowed value.

4.2.6.2.7.3 ATPC Parameters in AU

4.2.6.2.7.3.1 ATPC Option

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

The default is Enable.

4.2.6.2.7.3.2 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).

4.2.6.2.7.3.3 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: 11 (dB).

4.2.6.2.7.3.4 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.

4.2.6.2.7.3.5 ATPC Power Level Step

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

Valid range: 1-20 (dB)

Default value: 5 (dB)

4.2.6.2.7.4 ATPC Parameters in SU

4.2.6.2.7.4.1 ATPC Option

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

The default is Enable.



NOTE

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

4.2.6.2.7.5 Tx Control (AU only)

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

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

The default is On.



NOTE

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

4.2.6.2.8 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 cases when there is a limit on the EIRP allowed for the unit; the maximum allowed value for the Transmit Power parameters cannot exceed the value of (EIRP - Antenna Gain), where the EIRP is defined in the selected Sub-Band.

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

The range is 0–50 (dB). A value of "Don't Care" means that the actual value is not important. A value of "Not Set Yet" means that the unit will not transmit until the actual value (in the range 0 to 50) is configured. The unit can be configured to

“Don’t Care” or “Not Set Yet” only in factory. 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. In SUs with integral antenna it is set to 19 (read only). 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”.

4.2.6.2.9 Cell Distance Parameters (AU only)

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 (acknowledge time delay) should take into account the round trip propagation delay of the farthest SU. (The one-way propagation delay at 5 GHz is 3.3 microsecond/km.) The higher the distance from the AU of the farthest SU served by it, the higher the acknowledge time delay for all units in the cell should be.
- 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.

The distance from the AU of the farthest SU served by it can be determined either manually or automatically. In manual mode, this distance is configured manually. In automatic mode, the AU uses a special algorithm to estimate its distance from each of the SUs it serves, determine which SU is located the farthest and use the estimated distance of the farthest SU as the maximum distance.

It should be noted that if the size of the time slot used by all units is adapted to the distance of the farthest unit, then no unit will have an advantage when competing for services. However, this reduces the overall achievable throughput of the cell. In certain situations, the operator may decide to improve the overall throughput by reducing the slot size below the value required for full fairness. This means that when there is competition for bandwidth, the back-off algorithm will give an advantage to SUs that are located closer to the AU.

The Cell Distance Parameters menu includes the following parameters:

4.2.6.2.9.1 Cell Distance Mode

The Cell Distance Mode option defines whether the maximum distance of the AU from any of the SUs it serves will be determined manually (using the Maximum Cell Distance parameter) or automatically.

The Options are Automatic or Manual.

The default is Automatic.

4.2.6.2.9.2 Maximum Cell Distance

The Maximum Cell Distance parameter allows configuring the maximum distance when the Cell Distance Mode option is Manual.

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

The default is 0 (No Compensation).

4.2.6.2.9.3 Fairness Factor

The Fairness Factor enables to define the level of fairness in providing services to different SUs. When set to 100%, all SUs have the same probability of getting services when competing for bandwidth. If set to X%, then SUs located up to X% of the maximum distance from the AU will have an advantage in getting services over SUs located farther than this distance.

The range is 0 to 100 (%)

The default is 100 (%).

4.2.6.2.9.4 Show Cell Distance Parameters

Select Show Cell Distance Parameters to view the Cell Distance parameters. In addition, the Measured Maximum Cell Distance and the MAC address of the unit that the mechanism found to be the farthest from the AU are displayed. A distance of 1 km means any distance below 2 km.

4.2.6.2.10 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 one or two time slots. 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 or 2 (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. In this case, the Minimum Contention Window parameter in both units must be configured to 0 to disable the contention window back-off algorithm.

4.2.6.2.11 Maximum Number of Associations (AU only)

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 for AU-BS and AU-SA range from 0 to 512. For AUS-BS and AUS-SA the range is from 0 to 5.

Default value for AU-BS and AU-SA is 512. For AUS-BS and AUS-SA the default is 5.

NOTE



When the Data Encryption Option is enabled, the actual maximum number of SUs that can associate with the AU-BS or AU-SA is limited to 124. The number displayed for the Maximum Number of Associations is the value configured for this parameter, which might be higher than the actual limit. 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 conditions:

- A SNAP frame is received from another AU indicating that the SU is now associated with the other AU.
- 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 reset the AU.

4.2.6.2.12 Wireless Link Trap Threshold (AU only)

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

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

The default is 30 (%).

4.2.6.2.13 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. During the spectrum analysis period the unit security mode is changed to promiscuous to enable gathering information regarding all legal frames received by the unit. At the end of the period the unit will reset automatically regaining normal operability upon start up.

The Spectrum Analysis submenu includes the following options:

4.2.6.2.13.1 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.

4.2.6.2.13.2 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.

4.2.6.2.13.3 Automatic Channel Selection (AU only)

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.

4.2.6.2.13.4 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.

4.2.6.2.13.5 Reset Spectrum Analysis Information

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

4.2.6.2.13.6 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 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.

4.2.6.2.13.7 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.

4.2.6.2.14 Lost Beacons Transmission 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, its default value being 218. When the parameter is set to 0, this feature is disabled, i.e. internal refresh will never be performed.

4.2.6.2.15 Disassociate (AU only)

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, including the search for the best AU (or a preferred AU) using the Best AU 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

4.2.6.3 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 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 SU via the wireless link, setting the Access to Network Management parameter to From Ethernet Only completely blocks your management access to the unit. In this case, a technician may be required to change the settings at the user's site.

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 Ranges

The Set/Change Network Management IP Address Ranges 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.

4.2.6.3.7 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.

4.2.6.4 Bridge Parameters

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

The Bridge Parameters menu includes the following options:

- VLAN Support
- Ethernet Broadcast Filtering (SU only)
- Ethernet Broadcast/Multicast Limiter
- Bridge Aging Time
- Roaming Option (SU only)
- Broadcast Relaying (AU only)
- Unicast Relaying (AU only)
- MAC Address Deny List (AU only)

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 BreezeACCESS 4900 units supports frame routing by port information, whereby each port is connected to only one VLAN.

The VLAN Support menu includes the following parameters:

- VLAN Link Type
- VLAN ID – Data (SU only)
- VLAN ID – Management
- VLAN Forwarding

- VLAN Relaying (AU only)
- VLAN Traffic Priority

4.2.6.4.1.1 VLAN ID-Data (SU only)

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

Valid values range from 1 to 4094.

Default value: 1.

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

- Only tagged frames with a VLAN ID (VID) equal to the **VLAN ID-Data** defined in the unit are forwarded to the Ethernet port.
- The tag headers are removed from the data frames received from the wireless link before they are transmitted on the Ethernet port.

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

- A VLAN Data Tag is inserted in all untagged frames received from the Ethernet port before transmission on the wireless link. The tag includes the values of the **VLAN ID-Data** and the **VLAN Priority-Data** parameters.
- Tagged frames received on Ethernet port, which are meant to be forwarded to the wireless link port, are discarded. This includes frames with tagging for prioritization purposes only.

4.2.6.4.1.2 VLAN ID-Management

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

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

The default value is 65535.

If the VLAN ID-Management is other than 65535:

- Only tagged management frames with a matching VLAN ID received on either the Ethernet or wireless link ports are forwarded to the unit.
- A VLAN Management Tag is inserted in all management frames generated by the unit before transmission on either the Ethernet or wireless link port. The tag includes the values of the **VLAN ID-Management** and the **VLAN Priority-Management** parameters.

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

- Only untagged management frames received on either the Ethernet or wireless link ports are forwarded to the unit.
- Management frames generated by the unit are not tagged.

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

Table 4-6: VLAN Management Port Functionality	
Action	Management Port - Internal
Receive from Ethernet	Tagged frames, matching VID-M Untagged frames when VID-M=65535
Receive from Wireless	Tagged frames, matching VID-M Untagged frames when VID-M=65535
Transmit	Insert VID-M, PID-M

Table Legend:

- **VID-M:** VLAN ID-Management
- **PID-M:** VLAN Priority-Management

4.2.6.4.1.3 VLAN Link Type

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

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

The default selection is Hybrid Link.

4.2.6.4.1.3.1 Access Link (SU only)

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

Table 4-7 summarizes the functionality of the data port for an Access link.

Table 4-7: VLAN Data Port Functionality - Access Link	
Action	Data Port - SU
Receive from Ethernet	Untagged frames
Accept from Wireless	Tagged frames, matching VID-D
Tag Insert	VID-D, PID-D (to wireless)
Tag Remove	Yes (to Ethernet)

Table Legend:

- VID-D: VLAN ID-Data
- PID-D: VLAN Priority-Data

4.2.6.4.1.3.2 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 in an AU, 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

4.2.6.4.1.3.3 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

4.2.6.4.1.4 VLAN Forwarding (AU and SU)

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

The VLAN Forwarding submenu provides the following options:

4.2.6.4.1.4.1 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.

4.2.6.4.1.4.2 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.

4.2.6.4.1.4.3 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.

4.2.6.4.1.4.4 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.

4.2.6.4.1.5 VLAN Relaying (AU only)

The VLAN Relaying feature is applicable for Trunk Links only. It enables defining the VLAN ID values to be included in the VLAN Relaying List. If the Link Type is defined as 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:

4.2.6.4.1.5.1 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.

4.2.6.4.1.5.2 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.

4.2.6.4.1.5.3 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.

4.2.6.4.1.5.4 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.

4.2.6.4.1.6 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. In version 3.2 all parameters that affect prioritization within the BreezeACCES 4900 system, including VLAN-based prioritization, are located in the Services > Traffic Prioritization menu.

The VLAN Traffic Priority menu includes the following parameters:

- VLAN Priority – Data (SU only)
- VLAN Priority – Management

4.2.6.4.1.6.1 VLAN Priority - Data (SU only)

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

Valid values range from 0 to 7.

The default value is 0.

4.2.6.4.1.6.2 VLAN Priority - Management

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

Valid values range from 0 to 7.

The default value is 4 for SUs and 0 for AUs.

4.2.6.4.1.7 Show VLAN Parameters

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

4.2.6.4.2 Ethernet Broadcast Filtering (SU only)

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

The Ethernet Broadcast Filtering menu includes the following parameters:

- Filter Options
- DHCP Broadcast Override Filter
- PPPoE Broadcast Override Filter
- ARP Broadcast Override Filter

4.2.6.4.2.1 Filter Options

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

- **Disable** - no Ethernet Broadcast Filtering.
- **On Ethernet Port Only** - filters broadcast messages received from the Ethernet port.
- **On Wireless Port Only** - filters broadcast messages received from the wireless link port.
- **On Both Ethernet and Wireless Ports** - filters broadcast messages received from both the Ethernet and wireless link ports.

The default selection is Disable.

4.2.6.4.2.2 DHCP Broadcast Override Filter

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

- **Disable** - DHCP Broadcast messages are filtered or transmitted according to the general filtering criteria in the Filter Options parameter.
- **Enable** - DHCP Broadcast messages are transmitted regardless of the selected value of the Filter Options parameter.

The default selection is Disable.

4.2.6.4.2.3 PPPoE Broadcast Override Filter

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

- **Disable** - PPPoE Broadcast messages are filtered or transmitted according to the general filtering criteria in the Filter Options parameter.
- **Enable** - PPPoE Broadcast messages are transmitted regardless of the selected value of the Filter Options parameter.

The default selection is Disable.

4.2.6.4.2.4 ARP Broadcast Override Filter

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

- **Disable** - ARP messages are filtered or transmitted according to the general filtering criteria in the Filter Options parameter.
- **Enable** - ARP messages are transmitted regardless of the selected value of the Filter Options parameter.

The default selection is Enable.

4.2.6.4.3 Ethernet Broadcast/Multicast Limiter

The Ethernet Broadcast/Multicast Limiter parameters, available in both AU and SU, 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.

In SUs, the limiter is placed after the Ethernet Broadcast Filters. For this reason, the limiter will receive only the packets that pass through these filters. If the Ethernet filters of the SU are disabled, the limiter will be applied to all relevant packets received.

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:

4.2.6.4.3.1 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.

4.2.6.4.3.2 Ethernet Broadcast/Multicast Limiter Threshold

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.

4.2.6.4.3.3 Ethernet Broadcast/Multicast Limiter Send Trap Interval

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.

4.2.6.4.4 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 4900 units.

The available range is 20 to 2000 seconds.

The default value is 300 seconds.

4.2.6.4.5 Broadcast Relaying (AU only)

The Broadcast Relaying option enables selecting whether the unit performs broadcast relaying. When the Broadcast Relaying parameter is enabled, broadcast packets 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. If disabled, these packets are sent only to the local wired LAN and are not sent back to the wireless link. Disable the broadcast relaying only if all broadcast messages from the wireless link are certain to be directed to the wired LAN.

The default selection is Enable.

4.2.6.4.6 Unicast Relaying (AU only)

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.

4.2.6.4.7 MAC Address Deny List (AU only)

The MAC Address Deny List submenu enables to define units that are not authorized to receive services. The AU will not provide services to a unit whose MAC Address is included in the deny list. This feature enables to disconnect units from the services in cases such as when the user had fraudulently succeeded to configure the unit to values different than his subscription plan. The deny list can include up to 100 MAC Addresses.

The MAC Address Deny List submenu includes the following:

4.2.6.4.8 Add MAC Address to Deny List

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

4.2.6.4.9 Remove MAC Address from Deny List

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

4.2.6.4.9.1 Show MAC Address Deny List

Select Show MAC Address Deny List to display the current list of MAC Addresses included in the Deny List.

4.2.6.4.10 Roaming Option (SU only)

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

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

The default is Disable.

4.2.6.4.11 Ports Control (SU only)

The Ports Control sub-menu includes the Ethernet Port Control option:

4.2.6.4.11.1 Ethernet Port Control

The Ethernet Port Control option allows enabling or disabling non-management traffic to/from the Ethernet port. When changed to Disable, all current data sessions will be terminated. The unit is still manageable via the Ethernet port even if it is disabled for data traffic.

The default selection is Enable.

4.2.6.4.12 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
- Minimum Contention Window
- Maximum Contention Window
- Multicast Modulation Level (AU only)
- Maximum Modulation Level
- Average SNR Memory Factor
- Number of HW Retries
- Burst Mode
- Adaptive Modulation Algorithm

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 4032 bytes.

The default value is 60 bytes for SUs. For AUs the default is 4032. It is recommended that these values 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 BreezeACCESS 4900 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 [4.2.6.2.10](#)) 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.

**CAUTION**

A value of 0 disables the contention window back-off algorithm. It should only be used in point-to-point applications. For more details on configuring units in a point-to-point link refer to section [4.2.6.2.10](#).

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 (AU only)

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

The Multicast Modulation Level parameter is applicable only to data frames. Beacons and other wireless management and control frames are always transmitted at the lowest modulation level, modulation level 1.

The range is from 1 to 8.

The default is 1 (the lowest 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 or retransmissions before the modulation level is being reduced by the Adaptive Modulation Algorithm. A high number of retransmissions reduces the overall throughput of the 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 SU at the AU, which can be viewed in the MAC Address Database option in the Site Survey menu. If the measured SNR is less than a certain threshold, it is recommended that the maximum modulation level of the SU be decreased in accordance with Table 4-10, 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. If necessary, use the Ping Test utility in the Site Survey menu to verify data transmission.

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

The range is from 1 to 8.

The default is 8 (the highest 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

The Average SNR Memory Factor defines the weight of history (value of last calculated average SNR) in the formula used for calculating the current average SNR for received data frames. This average SNR is used by the ATPC algorithm in the 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 15.

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).

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 from 1 to 10 milliseconds. The default is 5 milliseconds.

4.2.6.5.9 Adaptive Modulation Algorithm (Multi Rate)

The Adaptive Modulation Algorithm enables adapting the modulation level of transmitted data to the prevailing conditions of the applicable radio link. 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 information on received signal quality (SNR) that is received periodically from the destination unit, the time that has passed since last transmission to the relevant unit, and the recent history of successful and unsuccessful transmissions/retransmissions. In the AU 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 (Modulation Level 1) 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 Minimum Interval Between Adaptive Modulation Messages

The Minimum Interval Between Adaptive Modulation Messages sets the minimum interval between two consecutive adaptive modulation messages, carrying information on the SNR of received signals. The messages in the AU include SNR information on all the SUs associated with it.

The available range is from 1 to 3600 seconds.

The default is 4 seconds.

4.2.6.5.9.3 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.

4.2.6.5.10 Concatenation Parameters

The Concatenation mechanism enables bundling several data frames into a single frame for transmission to the wireless link. This feature improves throughput and reduces the overhead in the wireless medium, by requiring only one CRC for each concatenated frame, one RTS/CTS cycle if applicable, and a single waiting period according to the contention window mechanism before transmission. When concatenation is enabled, data packets in the queue of the internal bridge can be accumulated before the concatenated frame is transmitted to the wireless medium. Up to 8 data frames can be accumulated, to a maximum total size of 4032 bytes. In the AU, the concatenation process is performed separately for each destination SU.

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

- The frame is a data frame
- The destination is an entity behind the destination AU/SU.

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

- If there is no concatenated frame designated to the same destination unit in the queue:
 - ◇ If the hardware queue is empty – the frame is transmitted immediately.
 - ◇ Otherwise (the queue is not empty) – the frame is inserted to the queue as a concatenated frame.
- If a concatenated frame designated to the same destination unit exists in the queue:
 - ◇ If the combined size of both frames is above the maximum allowed concatenated frame size – both frames are transmitted as two separate frames.
 - ◇ Otherwise (the combined frames size is below the maximum size) – the new frame is added to the concatenated frame. If the number of data frames in the concatenated frame has reached the maximum allowed – the concatenated frame will be transmitted to the wireless medium. Otherwise – the concatenated frame remains in the queue (until the hardware queue becomes free).

NOTE



When a frame is marked as a candidate for concatenation, it will be transmitted as a concatenated frame. If it is not bundled with another data frame before transmission, it will be a concatenated frame with a single data frame (Concatenated Frame Single). If it is bundled with two or more data frames, it will be a concatenated frame with either double data frames (Concatenated Frame Double) or more data frames (Concatenated Frame More).

The Concatenation Parameters submenu includes:

4.2.6.5.10.1 Concatenation Option

The Concatenation Option enables or disables the concatenation mechanism.

The default is Enable.

4.2.6.5.10.2 Maximum Number of Frames

The Maximum Number of Frames parameter defines the maximum number of data frames that can be bundled into a single concatenated frame.

The range is from 2 to 8 frames.

The default is 8 frames.

4.2.6.6 Service Parameters

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

The Service Parameters menu includes the following parameters:

- User Filtering Parameters (SU only)
- MIR and CIR Parameters
- Traffic Prioritization

4.2.6.6.1 User Filtering Parameters (SU only)

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.
- **PPPoE Protocol Only** - only PPPoE messages pass (Ethernet type 0x8863 and 0x8864).

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 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 CIR (Committed Information Rate) specifies the minimum data rate guaranteed to the relevant subscriber. 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 applicable CIR and MIR values, based on the following formula:

$$IR=CIR+K(MIR - CIR).$$

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. In some situations the minimum rate (CIR) cannot be provided. This may result from high demand and poor wireless link conditions and/or high demand in over-subscribed cells. When this occurs, the actual information rate is lower than the CIR.

The simple solution for managing the information rate in such cases can result in an unfair allocation of resources, as subscribers with a higher CIR actually

receive an IR lower than the CIR designated for subscribers in a lower CIR bracket.

A special algorithm for graceful degradation is incorporated into the AU, ensuring that the degradation of performance for each individual Subscriber Unit is proportional to its CIR.

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 is received from the Ethernet port during the last N seconds, the unit is allowed to transmit N times its CIR value without any delay. For example, after a period of inactivity of 0.5 seconds, a unit with CIR = 128 Kbps can transmit up to 128 Kbits x 0.5 = 64 Kbits without any delay.

4.2.6.6.2.1 MIR: Downlink (SU only)

Sets the Maximum Information Rate of the downlink from the AU to the SU. The MIR value cannot be lower than the corresponding CIR value.

Available values range is from 128 to 53888 Kbps.

The default is 53888 Kbps.

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

4.2.6.6.2.2 MIR: Uplink (SU only)

Sets the Maximum Information Rate of the up-link from the SU to the AU. The MIR value cannot be lower than the corresponding CIR value.

Available values range is from 128 to 53888 Kbps.

The default is 53888 Kbps.

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

4.2.6.6.2.3 CIR: Downlink (SU only)

Sets the Committed Information Rate of the downlink from the AU to the SU. The CIR value cannot be higher than the corresponding MIR value.

Available values range is from 0 to 45056 Kbps.

The default is 0 Kbps.

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

4.2.6.6.2.4 CIR: Uplink (SU only)

Sets the Committed Information Rate of the uplink from the SU to the AU. The CIR value cannot be higher than the corresponding MIR value.

Available values range is from 0 to 45056 Kbps.

The default is 0 Kbps.

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

4.2.6.6.2.5 Maximum Burst Duration (SU and AU)

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.

4.2.6.6.2.6 Maximum Delay (SU only)

Sets the maximum permitted delay in the buffers system. As certain applications are very sensitive to delay, if relatively high delays are permitted, these applications may suffer from poor performance due to data accumulation in the buffers from other applications, such as FTP. The Maximum Delay parameter limits the number of available buffers. Data that is delayed more than the permitted maximum delay is discarded. If the SU supports applications that are very sensitive to delay, the value of the Maximum Delay should be decreased.

Valid values range from 300 to 10000 (milliseconds).

The default value is 5000 (milliseconds).

4.2.6.6.2.7 Graceful Degradation Limit (AU only)

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 $k \leq K$, 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 (%).

4.2.6.6.2.8 MIR Only Option (AU only)

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.

4.2.6.6.2.9 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.

4.2.6.6.3.1 VLAN Priority Threshold

The VLAN Priority Threshold is applicable for Trunk and Hybrid Links only. It enables defining the value of the VLAN Priority Threshold. 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 7, which means that all packets get a low priority (equivalent to disabling the IP Precedence-based classifier).

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 63, which means that all packets get a low priority (equivalent to disabling the IP Precedence-based classifier).

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 start and end port numbers. A comma is used to separate 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 start and end port numbers. A comma is used to separate 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 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 Show Traffic Prioritization

Displays the current values of the Traffic Prioritization parameters, including the lists of UDP and TCP priority port ranges.

4.2.6.6.4 Show Service Parameters

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

4.2.6.7 Security Parameters

BreezeACCESS 4900 systems can support encryption of authentication messages and/or data frames using one of three encryption standards:

- **WEP** Wireless Equivalent Privacy algorithm. WEP is defined in the IEEE 802.11 Wireless LAN standard and is based on the RSA's RC4 encryption algorithm.
- **AES/OCB** Advanced Encryption Standard. AES is defined by the National Institute of Standards and Technology (NIST) and is based on Rijndael block cipher. AES/OCB (Offset Code Book) is a mode that operates by augmenting the normal encryption process by incorporating an offset value.
- **AES/CCM** Advanced Encryption Standard. AES is defined by the National Institute of Standards and Technology (NIST) and is based on Rijndael block cipher. AES/CCM mode provides encryption and message integrity in one solution.

NOTE



The AES/CCM encryption functionality in BreezeACCESS 4900 is FIPS (Federal Information Processing Standards) 197 certified.

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

- Authentication Algorithm
- Data Encryption Option
- Security Mode
- Default Key (SU only)
- Default Multicast Key (AU only)
- Key # 1 to Key # 4
- Promiscuous Authentication (AU only)

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

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

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.
- An SU with Data Encryption Option enabled can accept non-encrypted data frames.
- When the Data Encryption Option is enabled, the maximum number of SUs that can associate with the AU is limited to 124. The Maximum Number of Associations Limit 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.

Available options are WEP, AES/OCB and AES/CCM.

The default is WEP.

4.2.6.7.4 Default Key (SU only)

The Default Key defines the Key to be used for encrypting/decrypting the authentication messages (Shared Key mode) and/or data frames (Data Encryption enabled). The AU learns the Default Key from the SU provided it is one of the Keys defined in the AU. The AU may use different keys when authenticating and/or communicating with different SUs.

Available values range from 1 to 4.

The default is KEY # 1.

4.2.6.7.5 Default Multicast Key (AU only)

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

Available values range from 1 to 4.

The default is KEY # 1.

4.2.6.7.6 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 no key.

4.2.6.7.7 Promiscuous Authentication (AU only)

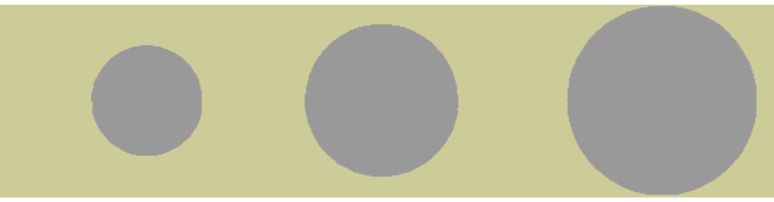
The Promiscuous Authentication mode enables new SUs to join an active cell where Shared Key operation and/or Data Encryption are used, even if this SU does not have the correct security parameters. In promiscuous mode, all downlink transmissions (from AU to SUs) are not encrypted, allowing remote configuration of security parameters, regardless of the current settings in the SUs of the parameters related to data encryption. After a new SU joins the cell it should be remotely configured with the proper parameters (or upgraded). When the SU is configured properly, the Promiscuous Mode should be disabled.

The default is Disable.

NOTE



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



A

Appendix A - Software Version Loading Using TFTP



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

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

CAUTION



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



To load software versions:

- 1 Verify that IP connectivity to the required unit is established.
- 2 Ensure that the IP address of the PC from which the upgrade is to be performed belongs to the same subnet as the unit to be upgraded, unless the unit is behind a router. If the unit is behind a router, verify that the unit is configured with the correct **Default Gateway Address**.
- 3 To view the current IP parameters of the unit, use the Monitor program by connecting the PC to the unit either directly or via Telnet. To access the IP parameters via the Monitor program:
 - a From the *Main Menu* select **1 - Info Screens**.
 - b From the *Info Screen* menu select **2 - Show Basic Configuration**. The current basic configuration is displayed, including the run time values for the IP Address, Subnet Mask and Default Gateway Address parameters.
- 4 To modify any of the IP parameters:
 - a From the *Main Menu*, select **3 - Basic Configuration**.
 - b To configure the IP address, select: **1 - IP Address**.
 - c To configure the subnet mask, select **2 - Subnet Mask**.
 - d To configure the default gateway address, select **3 - Default Gateway Address**.
- 5 To verify the connection, PING the unit's IP address and verify that PING replies are being received.
- 6 Use the TFTP utility, with the following syntax, to perform the upgrade:

```
tftp -i hostaddress put sourcefile [destinationfile]
```

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

- 7 The original *sourcefile* name of SW files is in the structure *uX_Y_Z.bz*, where *u* is the unit type (a for AU, s for SU) and *X.Y.Z* is the version number.
- 8 *destinationfile* is the name of the file to be loaded. Use the SNMP write community *<SnmpWriteCommunity>.bz* to define the destination filename. The default SNMP write community is *private*. For example, to load the upgrade file *a1_0_6.bz* to an AU whose IP address is *206.25.63.65*: *tftp -i 206.25.63.65 put a1_0_6.bz private.bz*
- 9 When the loading is complete, the following message is displayed, indicating completion of the TFTP process:

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

- 10 The unit decompresses the loaded file and checks the integrity of the new version. The new version replaces the previous shadow version only after verification. If verification tests fail, the loaded version will be rejected. Among other things that are tested, the unit will reject a file if either the file name or the version number matches the current Main versions. The unit will also reject a file designated for a different unit type, e.g. an AU upgrade file with the prefix *a* in the original file name will not be accepted by SUs.
- 11 The FLASH memory can store two software versions. One version is called Current and the second version is called *Shadow*. The new version is loaded into the Shadow (backup) FLASH memory. To check that the new firmware was properly downloaded and verified, view the firmware versions stored in the FLASH, as follows:
 - a From the Main Menu, select **2 - Unit Control**.
 - b From the Unit Control menu, select **5 - Flash Memory Control**.
 - c From the *Flash Memory Control* menu, select **S - Show Flash Versions**. The following information is displayed:

```
Flash Versions
=====
Running from           :Main Version
Main Version File Name :1_0_5.bz
Main Version Number    :1.0.5
Shadow Version File Name :1_0_6.bz
File Name Number       :1.0.6
```




B

Appendix B - 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 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 will be ignored. A known parameter with a value that is invalid or out of range will be set by the unit to its default value.

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

Use the extension *cfg* for a configuration file.

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

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

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

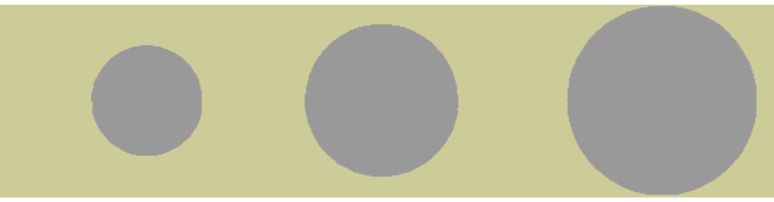
Feature license and country code files include multiple strings, where each string is applicable only for a certain unit identified by its MAC address. When uploading a feature license or a country code file to multiple units, each unit will accept only the parts that are applicable for itself.

Examples:

- 1 To upload the configuration file using a DOS based TFTP Client to an SU whose IP address is 206.25.63.65, enter:
tftp 206.25.63.65 put Suconf private.cfg
- 2 To download the Operator Defaults file from the same unit, enter:
tftp 206.25.63.65 get private.cmr Suconf
- 3 To upload the Feature Upgrade file to the same unit, enter:
tftp 206.25.63.65 put private.fln Suconf
- 4 To upload the Country Code file from to same unit, enter:
tftp 206.25.63.65 put private.ccf Suconf

**NOTE**

The Configuration File mechanism is common to BreezeACCESS 4900, BreezeACCESS VL and BreezeNET B product lines. The Configuration File includes also parameters that are not applicable to BreezeACCESS 4900, such as DFS parameters. Do not attempt to change the default values of these parameters.



C

Appendix C - Using the Set Factory Defaults Utility



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

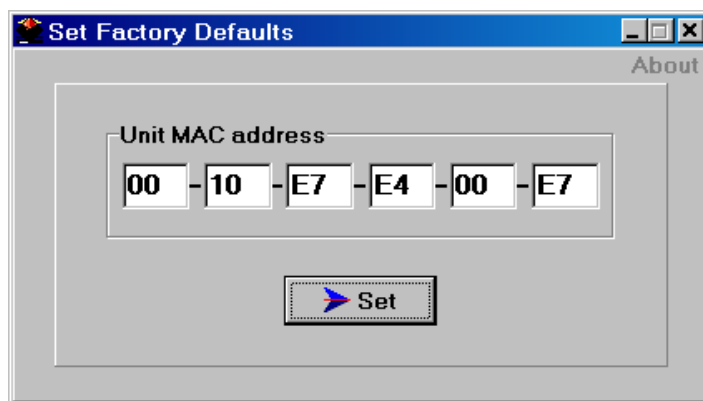
The utility accesses the unit by sending a special packet. Access to the unit is based on its MAC address, which must be entered in the **Unit MAC address** field.

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



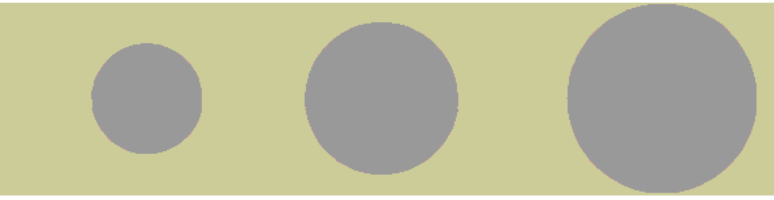
To set factory defaults:

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



- 2 Enter the unit's MAC address.
- 3 Click on the **Set** button.

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



D

Appendix D - Preparing the Indoor to Outdoor SU Cable



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

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

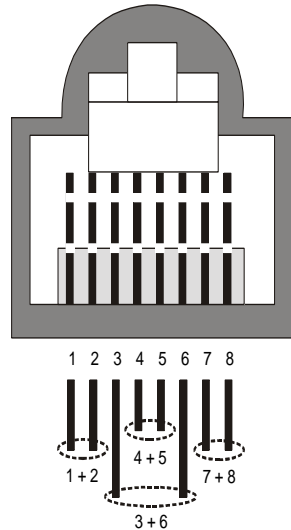


Figure D-1: Ethernet Connector Pin Assignments

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

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

Use a crimp tool for RJ-45 connectors to prepare the wires, insert them into the appropriate pins and use the crimp tool to crimp the connector. Make sure to do the following:

- 1 Remove as small a length as possible of the external jacket. Verify that the external jacket is well inside the service box to ensure good sealing.
- 2 Take back the shield drain wire before inserting the cable into the RJ-45 connector, to ensure a good connection with the connector's shield after crimping.

Appendix E - Supported MIBS and Traps

In This Appendix:

BreezeACCESS 4900 agents support the following MIBs:

- MIB-II (RFC1213)
- BRIDGE_MIB (RFC1286)
- BreezeACCESS VL Private MIB (breezeAccessVLMib)

The following are described in this Appendix:

- [System Object Identifiers](#), page 160
- [breezeAccessVLMib](#), page 162
- [Supported Traps](#), page 209



NOTE

The BreezeAccessVLMib is used for BreezeACCESS 4900 (AU, SU), BreezeACCESS VL (AU, SU) and BreezeNET B (BU, RB) product lines. Some of the parameters are only applicable to one or two of the product lines.

Generally, all parameters that are applicable to BreezeACCESS VL are also applicable to BreezeACCESS 4900 (note that in BreezeACCESS 4900 DFS is always Not Supported).

E.1 System Object Identifiers

Object	Path
alvarion	OID = 1.3.6.1.4.1.12394 {(iso(1) org(3) dod(6) internet(1) private(4) enterprises(1) alvarion(12394)}
products	OID = 1.3.6.1.4.1.12394.1 {alvarion 1}
breezeAccessVLMib	OID = 1.3.6.1.4.1.12394.1.1 {products 1}
alvarionOID	OID = 1.3.6.1.4.1.12394.4 {alvarion 4}
brzAccessVLOID	OID = 1.3.6.1.4.1.12394.4.1 {alvarionOID 1}
brzAccessVLAU	OID = 1.3.6.1.4.1.12394.4.1.1 {brzAccessVLOID 1}
brzAccessVLSU	OID = 1.3.6.1.4.1.12394.4.1.2 {brzAccessVLOID 2}
brzAccessVLAU-BS	OID = 1.3.6.1.4.1.12394.4.1.4 {brzAccessVLOID 4}
brzAccessVLAU-SA	OID = 1.3.6.1.4.1.12394.4.1.5 {brzAccessVLOID 5}
brzAccessVLAUS-BS	OID = 1.3.6.1.4.1.12394.4.1.6 {brzAccessVLOID 6}
brzAccessVLAUS-SA	OID = 1.3.6.1.4.1.12394.4.1.7 {brzAccessVLOID 7}
brzAccessVLSU-6-1D	OID = 1.3.6.1.4.1.12394.4.1.11 {brzAccessVLOID 11}
brzAccessVLSU-6-BD	OID = 1.3.6.1.4.1.12394.4.1.12 {brzAccessVLOID 12}
brzAccessVLSU-24-BD	OID = 1.3.6.1.4.1.12394.4.1.13 {brzAccessVLOID 13}
brzAccessVLSU-BD	OID = 1.3.6.1.4.1.12394.4.1.14 {brzAccessVLOID 14}
brzAccessVLSU-54-BD	OID = 1.3.6.1.4.1.12394.4.1.15 {brzAccessVLOID 15}
brzAccessVLSU-3-1D	OID = 1.3.6.1.4.1.12394.4.1.16 {brzAccessVLOID 16}
brzAccessVLSU-3-4D	OID = 1.3.6.1.4.1.12394.4.1.17 {brzAccessVLOID 17}
brzNetB-BU-B14	OID = 1.3.6.1.4.1.12394.4.1.21 {brzAccessVLOID 21}
brzNetB-BU-B28	OID = 1.3.6.1.4.1.12394.4.1.22 {brzAccessVLOID 22}
BrzNetB-RB-B14	OID = 1.3.6.1.4.1.12394.4.1.31 {brzAccessVLOID 31}
brzNetB-RB-B28	OID = 1.3.6.1.4.1.12394.4.1.32 {brzAccessVLOID 32}
brzAccess 4900-AU-BS	OID = 1.3.6.1.4.1.12394.4.1.41 {brzAccessVLOID 41}
brzAccess 4900-AU-SA	OID = 1.3.6.1.4.1.12394.4.1.42 {brzAccessVLOID 42}

Object	Path
brzAccess 4900-SU-BD	OID = 1.3.6.1.4.1.12394.4.1.51 {brzAccessVLOID 51}
brzAccessVLProducts	OID = 1.3.6.1.4.1.12394.4.1.3 {brzAccessVLOID 3}

E.2 breezeAccessVLMib

OBJECT IDENTIFIER = 1.3.6.1.4.1.12394.1.1

NOTE



An * is used instead of the brzaccVL prefix.

E.2.1 System Information Parameters

MIB Parameter	Description	Value/Range
*SysInfo (breezeAccessVLMib 1)	System Information Parameters	
*UnitHwVersion (*SysInfo 1)	Applicable to all units. Read-only: Hardware platform version.	DisplayString (SIZE(0..32))
*RunningSoftwareVersion (*SysInfo 2)	Applicable to all units. Read-only: Running software version.	DisplayString (SIZE(0..32))
*RunningFrom (*SysInfo 3)	Applicable to all units. Read-only: The memory (main or shadow) from which the current version is running from.	Integer mainVersion (1) shadowVersion (2)
*MainVersionNumber (*SysInfo 4)	Applicable to all units. Read only: Main software version number.	DisplayString (SIZE(0..32))
*MainVersionFileName (*SysInfo 5)	Applicable to all units. Read-only: Main software version file name.	DisplayString (SIZE(0..32))
*ShadowVersionNumber (*SysInfo 6)	Applicable to all units. Read-only: Shadow software version number.	DisplayString (SIZE(0..32))
*ShadowVersionFileName (*SysInfo 7)	Applicable to all units. Read-only: Shadow software version file name.	DisplayString (SIZE(0..32))
*UnitMacAddress (*SysInfo 8)	Applicable to all units. Read-only: Unit hardware MAC address.	MAC address

MIB Parameter	Description	Value/Range
*UnitType (*SysInfo 9)	Applicable to all units. Read-only: Unit type.	Integer auBS (1) auSA (2) su-6-BD (3) su-24-BD (4) su-6-1D (5) bu-B14 (6) bu-B28 (7) rb-B14 (8) rb-B28 (9) su-BD (10) su-54-BD (11) su-3-1D (12) su-3-4D (13) ausBS(14) ausSA(15) auBS4900(16) auSA4900(17) suBD4900(18)
*AssociatedAU (*SysInfo 10)	Applicable to SU/RB. Read-only: Associated AU/BU MAC address.	MAC address
*NumOfAssociationsSinceLastReset (*SysInfo 11)	Applicable to all units. Read-only: The number of associations since last reset, including duplicate associations (re-associations).	Integer
*CurrentNumOfAssociations (*SysInfo 13)	Applicable to AU only. Not applicable to BreezeNET B products. Read-only. The number of subscriber units currently associated with the AU.	Integer na (65535)
*UnitBootVersion (*SysInfo 14)	Applicable to all units. Read-only: The Boot software version.	DisplayString (SIZE(0..32))
*RadioBand (*SysInfo 15)	Applicable to all units. Read-only: The radio band of the unit.	Integer band-5-8GHz (1) band-5-4GHz (2) band-4-9GHz (3) band-5-2GHz (4) band-2-4GHz (5) band-5-3GHz (6)
*CurrentEthernetPortState (*SysInfo 16)	Applicable to all units. Read-only. The current state of the Ethernet port.	Integer HalfDuplexAnd10Mbps (1) FullDuplexAnd10Mbps (2) HalfDuplexAnd100Mbps (3) FullDuplexAnd100Mbps (4) linkDown (5)
*TimeSinceLastReset (*SysInfo 17)	Applicable to all units. Read-only. The elapsed time since last reset.	DisplayString (SIZE(0..32))
*CountryDependentParameters (*SysInfo 18)	Country Dependent Parameters	
*CountryCode (*CountryDependentParameters 1)	Applicable to all units. Read only. The country code and country or country group name that is supported by the unit	DisplayString (SIZE(0..32))

MIB Parameter	Description	Value/Range
*CountryDependentParamsTable (*CountryDependentParameters 2)	Applicable to all units. Not accessible. A table of country dependent parameters.	
*CountryDependentParameterEntry (*CountryDependentParamsTable 1)	Applicable to all units. Not accessible. An entry in the country dependent parameters table.	
*CountryDependentParameterTableIdx (*CountryDependentParameterEntry 1)	Applicable to all units. Read only. The sub-band ID of the entry in the Country Dependent Parameters table. Serves also as index for the table entry.	Integer
*CountryDependentParameterFrequencies (*CountryDependentParameterEntry 2)	Applicable to all units. Read only. The frequencies included in the applicable sub-band entry.	DisplayString
*AllowedBandwidth (*CountryDependentParameterEntry 3)	Applicable to all units. Read only. The bandwidth when using the applicable the sub-band.	Integer
*RegulationMaxTxPowerAtAntennaPort (*CountryDependentParameterEntry 4)	Applicable to all units. Read only. The maximum allowed Tx power at the antenna port when using the applicable sub-band.	Integer
*RegulationMaxEIRP (*CountryDependentParameterEntry 5)	Applicable to all units. Read only. The maximum allowed EIRP when using the applicable sub-band.	Integer A Regulation Max EIRP of 100 means no limit.
*MinModulationLevel (*CountryDependentParameterEntry 6)	Applicable to all units. Read only. The minimum supported modulation level.	Integer level1 (1) level2 (2) level3 (3) level4 (4) level5 (5) level6 (6) level7 (7) level8 (8)
*MaxModulationLevel (*CountryDependentParameterEntry 7)	Applicable to all units. Read only. The maximum supported modulation level.	Integer level1 (1) level2 (2) level3 (3) level4 (4) level5 (5) level6 (6) level7 (7) level8 (8)
*BurstModeSupport (*CountryDependentParameterEntry 8)	Applicable to all units. Read only. The supported Burst Mode Option.	Integer supported (1) notSupported (2)
*MaximumBurstDuration (*CountryDependentParameterEntry 9)	Applicable to all units. Read only. Applicable only if Burst Mode Option is supported. The maximum supported burst duration.	Integer

MIB Parameter	Description	Value/Range
*DfsSupport (*CountryDependentParameterEntry 10)	Applicable to AU/BU only. Read only. The supported DFS Option.	Integer supported (1) notSupported (2)
*MinimumHwRevision (*CountryDependentParameterEntry 11)	Applicable to all units. Read only. The Minimum HW Revision needed to support the Sub-Band.	Integer HwRevisionA (1), HwRevisionB (2), HwRevisionC (3), na (255)
*AuthenticationEncryptionSupport (CountryDependentParameters 3)	Applicable to all units. Read only. The supported Authentication Encryption Option.	Integer supported (1) notSupported (2)
*DataEncryptionSupport (CountryDependentParameters 4)	Applicable to all units. Read only. The supported Data Encryption Option.	Integer supported (1) notSupported (2)
*AESEncryptionSupport (CountryDependentParameters 5)	Applicable to all units. Read only. The supported AES Encryption Option.	Integer supported (1) notSupported (2)
*AntennaGainChange (*SysInfo 19)	Applicable to all units. Indicates whether the Antenna Gain parameter is changeable or fixed.	Integer supported (1) notSupported (2)

E.2.2 Unit Control Parameters

MIB Parameter	Description	Value/Range
*UnitControl (breezeAccessVLMib 2)		
*ResetUnit (*UnitControl 1)	Applicable to all units. Resets the unit and applies new parameter values.	Integer cancel (1) resetSystemNow (2)
*SetDefaults (*UnitControl 2)	Applicable to all units. Sets unit configuration to Defaults values after the next reset. completeFactory: All parameters revert to Factory Defaults values partialFactory: All parameters revert to Factory Defaults values, except the parameters required for maintaining wireless connectivity. completeOperator: All parameters revert to Operator Defaults values partialOperator: All parameters revert to Operator Defaults values, except the parameters required for maintaining wireless connectivity.	Integer NoDefaultSettingRequested (0), completeFactory (1) partialFactory (2) completeOperator (3) partialOperator (4) cancelCurrentPendingRequest (5)
*UnitName (*UnitControl 3)	Applicable to all units. The unit name.	DisplayString (SIZE(32)) A string of up to 32 printable ASCII characters.

MIB Parameter	Description	Value/Range
*FlashMemoryControl (*UnitControl 4)	Applicable to all units. Reset And Boot From Shadow Version: Activates the shadow version. Use Running Version After Reset: The currently active version will become the main version and will be activated after next reset.	Integer resetAndBootFromShadowVersion (1) useRunningVersionAfterReset (2) cancel (3)
*TelnetLogoutTimer (*UnitControl 5)	Applicable to all units. Time-out of management via Telnet. Automatic exit if the program is inactive for the defined time.	Integer 1-999 (minutes)
*SaveCurrentConfigurationAsOperatorDefaults (*UnitControl 6)	Applicable to all units. Saves the current configuration as Operator Defaults.	Integer saveAsDefaults (1) cancel (2)
*ExitTelnet (*UnitControl 7)	Applicable to all units. Exit the Telnet Monitor session.	Integer cancelOperation (1) exit (2)
*UnitPasswords (*UnitControl 8)	Applicable to all units. Unit passwords.	
*ReadOnlyPassword (*UnitPasswords 1)	Applicable to all units. The User (read only) password.	DisplayString (SIZE(8)). Up to 8 printable ASCII characters.
*InstallerPassword (*UnitPasswords 2)	Applicable to all units. The Installer password.	DisplayString (SIZE(8)). Up to 8 printable ASCII characters.
*AdminPassword (*UnitPasswords 3)	Applicable to all units. The Administrator password. This is also the SNMP Write Community String.	DisplayString (SIZE(8)). Up to 8 printable ASCII characters.
*EthernetNegotiationMode (*UnitControl 9)	Applicable to all units. Ethernet port mode of operation.	Integer force10MbpsAndHalfDuplex (1) force10MbpsAndFullDuplex (2) force100MbpsAndHalfDuplex (3) force100MbpsAndFullDuplex (4) autoNegotiationMode (5)
*FTPParameters (*UnitControl 10)	Applicable to all units. FTP parameters	
*FTPServerParams (*FTPParameters 1)	Applicable to all units. General FTP server parameters.	
*FTPServerUserName (*FTPServerParams 1)	Applicable to all units. The user name to be used for access to the FTP server	DisplayString (SIZE(20)). Up to 18 printable ASCII characters.
*FTPServerPassword (*FTPServerParams 2)	Applicable to all units. The password to be used for access to the FTP server	DisplayString (SIZE(20)). Up to 18 printable ASCII characters.
*FTPClientIpAddress (*FTPParameters 3)	Applicable to all units. The IP address of the FTP stack in the unit.	IP address
*FTPServerIpAddress (*FTPServerParams 4)	Applicable to all units. The IP address of the FTP server	IP address
*FTPClientMask (*FTPParameters 5)	Applicable to all units. The IP MASK of the FTP stack in the unit.	IP address
*FTPGatewayIPAddress (*FTPParameters 6)	Applicable to all units. The FTP Default Gateway IP address.	IP address

MIB Parameter	Description	Value/Range
*FTPSwDownload (*FTPPParameters 2)	Applicable to all units. SW download parameters.	
*FTPSwFileName (*FTPSwDownload 1)	Applicable to all units. The name of the SW file to be downloaded.	DisplayString (SIZE(80)). Up to 20 printable ASCII characters. An empty string is not allowed.
*FtpSwDownloadSourceDir (*FTPSwDownload 2)	Applicable to all units. The source directory of the required file in the FTP server	DisplayString (SIZE(80)). Up to 80 printable ASCII characters. Use "." To clear field.
*DownloadSwFile (*FTPSwDownload 3)	Applicable to all units. Execution of the SW download operation.	Integer downloadFile (1) cancel (2)
*ConfigurationFileLoading (*FTPPParameters 3)	Applicable to all units. Configuration file and Operator Defaults file download/upload parameters.	
*ConfigurationFileName (*ConfigurationFileLoading 1)	Applicable to all units. The name of the configuration file to be downloaded/uploaded.	DisplayString (SIZE(80)). Up to 20 printable ASCII characters. An empty string is not allowed.
*OperatorDefaultsFileName (*ConfigurationFileLoading 2)	Applicable to all units. The name of the Operator Defaults file to be downloaded/uploaded.	DisplayString (SIZE(80)). Up to 20 printable ASCII characters. An empty string is not allowed.
*FTPConfigurationFileSourceDir (*ConfigurationFileLoading 3)	Applicable to all units. The source directory of the required file in the FTP server	DisplayString (SIZE(80)). Up to 80 printable ASCII characters. Use "." To clear field.
*ExecuteFTPConfigurationFileLoading (*ConfigurationFileLoading 4)	Applicable to all units. Execution of the file download/upload operation.	Integer executeFTPGetConfiguration File (1) executeFTPPutConfiguration File (2) executeFTPGetOperator Defaults (3) executeFTPPutOperator Defaults (4) cancel (5)
*EventLogFileUploading (*FTPPParameters 4)	Applicable to all units. Event Log file upload parameters.	
*EventLogFileName (*EventLogFileUploading 1)	Applicable to all units. The name of the event log file to be uploaded.	DisplayString (SIZE(80)). Up to 20 printable ASCII characters.
*EventLogDestinationDir (*EventLogFileUploading 2)	Applicable to all units. The destination directory for the event log file in the FTP server	DisplayString (SIZE(80)). Up to 80 printable ASCII characters. Use "." To clear field.
*UploadEventLogFile (*EventLogFileUploading 3)	Applicable to all units. Execution of the event log upload operation	Integer uploadFile (1) cancel (2)
*LoadingStatus (*UnitControl 11)	Applicable to all units. The status of an FTP or TFTP loading process.	Integer inProcess (1) successful (2) failed (3)
*EventLogFileParams (*UnitControl 12)	Event Log parameters	

MIB Parameter	Description	Value/Range
*EventLogPolicy (*EventLogFileParams 1)	Applicable to all units. The lowest severity of events to be logged.	Integer message (1) warning (2) error (3) fatal(4) logNone(5)
*EraseEventLog (*EventLogFileParams 2)	Applicable to all units. Erase the log file.	Integer eraseEventLog (1) cancel(2)
*SysLocation (*UnitControl 13)	Applicable to all units. The unit location.	DisplayString (SIZE(0..34))
*FeatureUpgrade (*UnitControl 14)	Feature Upgrade parameters	
*FeatureUpgradeManually (*FeatureUpgrade 1)	Applicable to all units. Upgrade unit to support new feature.	DisplayString (SIZE(32..64)) License string: 32 to 64 hexadecimal digits.

E.2.3 Network Management Parameters

MIB Parameter	Description	Value/Range
*NwMngParameters (breezeAccessVLMib 3)	Network management parameters.	
*AccessToNwMng (*NwMngParameters 1)	Applicable to all units. The port to be used for remote management.	Integer fromwirelessOnly (1) fromEthernetOnly (2) fromBothWirelessnAndEthernet (3) na (255)
*NwMngFilter (*NwMngParameters 2)	Applicable to all units. Disables or enable IP address based filtering of management messages on one or both ports.	Integer disable (1) activateOnEthernetPort (2) activateOnWirelessPort (3) activateOnBothWirelessAndEthernet (4) na (255)
mngIpFilterTable (*NwMngParameters 3)	Applicable to all units. A table of up to 10 IP addresses of stations that are authorized to access the unit for management purposes. Not accessible.	
mngIpFilterEntry (mngIpFilterTable 1)	Applicable to all units. A Management IP Addresses Table entry. Not accessible.	
*NwMngIpAddress (mngIpFilterEntry 1)	Applicable to all units. An IP address in the Management IP Addresses Table entry.	IP address
*NwMngIpTableIdx (mngIpFilterEntry 2)	Applicable to all units. Read-only. A table index for an entry in the Management IP Addresses Table.	Integer 1-10
*DeleteOneNwIpAddr (*NwMngParameters 4)	Applicable to all units. Deletes a single selected entry from the Management IP Addresses Table.	Integer cancelOperation (0) deleteEntry (1...10) na (255)

MIB Parameter	Description	Value/Range
*DeleteAllNwIpAddr (*NwMngParameters 5)	Applicable to all units. Deletes all entries from the Management IP Addresses Table.	Integer deleteAll (1) cancelOperation (2) na (255)
*AccessToNwTrap (*NwMngParameters 6)	Applicable to all units. Enables or disables the sending of SNMP traps.	Integer disable (1) enable (2)
mngTrapTable (*NwMngParameters 7)	Applicable to all units. A table of up to 10 IP addresses of stations to which to send SNMP traps. Not accessible.	
mngTrapEntry (mngTrapTable 1)	Applicable to all units. A Management Trap Table entry. Not accessible.	
*NwMngTrapCommunity (mngTrapEntry 1)	Applicable to all units. The trap community associated with the applicable entry in the Management Trap Table.	DisplayString (SIZE(14)) Up to 14 printable ASCII characters.
*NwMngTrapAddress (mngTrapEntry 2)	Applicable to all units. An IP address in the Management Trap Table.	IP address
*NwMngTrapTableIdx (mngTrapEntry 3)	Applicable to all units. Read only. Index for an entry in the Management Trap Table.	Integer 1-10
*DeleteOneTrapAddr (*NwMngParameters 8)	Applicable to all units. Deletes a single selected entry from the Management Trap Table.	Integer cancelOperation (0) deleteEntry (1...10) na (255)
*DeleteAllTrapAddrs (*NwMngParameters 9)	Applicable to all units. Deletes all entries from the Management Trap Table.	Integer deleteAll (1) cancelOperation (2) na (255)
*MngIpRangesTable (*NwMngParameters 10)	Applicable to all units. A table of Management IP Address Ranges. Not accessible.	
*MngIpRangesEntry (*MngIpRangesTable 1)	Applicable to all units. An entry in the table of Management IP Address Ranges. Not accessible.	
*MngIpRangeIdx (*MngIpRangesEntry 1)	Applicable to all units. Index of an entry in the IP Address Ranges Table.	Integer 1-10
*MngIPRangeFlag (*MngIpRangesEntry 2)	Applicable to all units. Defines the method of defining the range: Using Start & End Addresses (rangeDefinedByStartEndAddr), or using Start Address and Mask (rangeDefinedByStartAddrMask)	Integer rangeDefinedByStartEndAddr(1), rangeDefinedByStartAddrMask(2)
*MngIpRangeStart (*MngIpRangesEntry 3)	Applicable to all units. Start Address of the range.	IP address
*MngIpRangeEnd (*MngIpRangesEntry 4)	Applicable to all units. End Address of the range. Used only if brzaccVLMngIPRangeFlag is rangeDefinedByStartEndAddr	IP address
*MngIpRangeMask (*MngIpRangesEntry 5)	Applicable to all units. The subnet mask of the range. Used only if brzaccVLMngIPRangeFlag is rangeDefinedByStartAddrMask.	IP address

MIB Parameter	Description	Value/Range
*DeleteOneNwlpRange (*NwMngParameters 11)	Applicable to all units. Deletes a single selected entry from the Management IP Ranges Table.	Integer cancelOperation (0) deleteEntry (1...10) na (255)
*DeleteAllNwlpRanges (*NwMngParameters 12)	Applicable to all units. Deletes all entries from the Management IP Ranges Table.	Integer deleteAll (1) cancelOperation (2) na (255)

E.2.4 IP Parameters

MIB Parameter	Description	Value/Range
*IpParams (breezeAccessVLMib 4)		
*UnitIpAddress (*IpParams 1)	Applicable to all units. IP address of the unit.	IP address
*SubNetMask (*IpParams 2)	Applicable to all units. Subnet mask of the unit.	IP address
*DefaultGWAddress (*IpParams 3)	Applicable to all units. Default gateway IP address of the unit.	IP address
*UseDhcp (*IpParams 4)	Applicable to all units. DHCP client mode of operation. disable: Use regular (manual) methods to configure IP parameters. DHCP Only: Use DHCP server to configure IP parameters. automatic: Use DHCP server to configure IP parameters. If a DHCP server is not available, use manually configured values for *UnitIpAddress, *SubnetMask and *DefaultGWAddress.	Integer disable (1) dHCPOnly (2) automatic (3)
*AccessToDHCP (*IpParams 5)	Applicable to all units. The port to be used for communicating with a DHCP server.	Integer fromWirelessOnly (1) fromEthernetOnly (2) fromBothWirelessAndEthernet (3)
*RunTimeIPAddr (*IpParams 6)	Applicable to all units. Read-only: The run-time IP address. If DHCP is used, the run-time IP address is the address given to the unit by the server. Alternatively the static IP address is used.	IP address
*RunTimeSubNetMask (*IpParams 7)	Applicable to all units. Read-only: The run-time subnet mask. If DHCP is used, the run-time subnet mask is the mask given to the unit by the server. Alternatively the static subnet mask value is used.	IP address

MIB Parameter	Description	Value/Range
*RunTimeDefaultIPGateway (*IpParams 8)	Applicable to all units. Read-only: The run-time Gateway IP address. If DHCP is used, the Run Time Gateway IP Address is the address given to the unit by the server. Alternatively, the static default gateway is used.	IP address

E.2.5 Bridge Parameters

MIB Parameter	Description	Value/Range
*BridgeParameters (breezeAccessVLMib 5)	Bridge parameters.	
*VLANSupport (*BridgeParameters 1)	Applicable to all units. VLAN support parameters. Applicable to Access Link only.	
*VlanID (*VLANSupport 1)	Applicable to SU/RB only. VLAN ID for data frame tagging.	Integer 1-4094. 0 –na (no VLAN ID)
*EthernetLinkType (*VLANSupport 2)	Applicable to all units. VLAN support mode (Link Type). The accessLink option is not available for AU.	Integer accessLink (1) trunkLink (2) hybridLink (3)
*ManagementVID (*VLANSupport 3)	Applicable to all units. VLAN ID for management frame tagging.	Integer 1-4094 65535 - no VLAN tagging.
*VLANForwarding (*VLANSupport 4)	VLAN forwarding feature parameters.	
*VlanForwardingSupport (*VLANForwarding 1)	Applicable to all units. Enables or disables the VLAN forwarding feature. Applicable to Trunk links only.	Integer disable (1) enable (2) na (255)
*VlanForwardingTable (*VLANForwarding 2)	Applicable to all units. A table of up to 20 VLAN IDs of devices to which data frames are forwarded when the VLAN Forwarding feature is Enabled. Applicable to Trunk links only. Not accessible.	
*VlanForwardingEntry (*VlanForwardingTable 1)	Applicable to all units. A VLAN Forwarding Table entry. Applicable to Trunk links only. Not accessible.	
*VlanForwardingTableIdx (*VlanForwardingEntry 1)	Applicable to all units. A read only table index for a VLAN entry in the VLAN Forwarding Table.	Integer 1-20
*VlanIdForwarding (*VlanForwardingEntry 2)	Applicable to all units. The list of VLAN ID's in the VLAN ID Forwarding Table. To remove a VLAN ID - SET the corresponding entry to 0. To add a new VLAN ID SET an entry which is now 0.	Integer 1-4094 0-remove entry.
*VLANRelaying (*VLANSupport 5)	VLAN Relaying feature parameters. Not applicable to BreezeNET B products.	
*VlanRelayingSupport (*VLANRelaying 1)	Applicable to AU only. Not applicable to BreezeNET B products. Enables or disables the VLAN Relaying feature. Applicable to Trunk links only.	Integer disable (1) enable (2) na (255)

MIB Parameter	Description	Value/Range
*VlanRelayingTable (*VLANRelaying 2)	Applicable to AU only. Not applicable to BreezeNET B products. A table of up to 20 VLAN IDs of devices to which data frames are relayed when the VLAN Relaying feature is Enabled. Applicable to Trunk links only. Not accessible.	
*VlanRelayingEntry (*VlanRelayingTable 1)	Applicable to AU only. Not applicable to BreezeNET B products. A VLAN Relaying Table entry. Applicable to Trunk links only. Not accessible.	
*VlanRelayingTableIdx (*VlanRelayingEntry 1)	Applicable to AU only. Not applicable to BreezeNET B products. A read only table index for a VLAN entry in the VLAN Relaying Table.	Integer 1-20
*VlanIdRelaying (*VlanRelayingEntry 2)	Applicable to AU only. Not applicable to BreezeNET B products. The list of VLAN ID's in the VLAN ID Relaying Table. To remove a VLAN ID - SET the corresponding entry to 0. To add a new VLAN ID SET an entry which is now 0.	Integer 1-4094 0-remove entry.
*VLANTrafficPriority (*VLANSupport 6)	VLAN traffic priority parameters.	
*VlanDataPriority (*VLANTrafficPriority 1)	Applicable to SU/RB only. Priority tagging for data frames. Applicable to Access Link only.	Integer 0 – 7 255-na
*VlanManagementPriority (*VLANTrafficPriority 3)	Applicable to all units. Priority tagging for management frames. Applicable to Access Link and Trunk Link only.	Integer 0 – 7 255-na
*VlanPriorityThreshold (*VLANTrafficPriority 4)	Applicable to all units. Not applicable to units with SW version 3.1 and higher where this parameter is replaced by Priority threshold for tagged frames received from Ethernet port. Applicable to Hybrid Link and Trunk Link only.	Integer 0 – 7 255-na
*BridgeAgingTime (*BridgeParameters 2)	Applicable to all units. Bridge aging time for devices learned from both the Ethernet and wireless link ports.	Integer 20 – 2000 (seconds)
*BroadcastRelaying (*BridgeParameters 4)	Applicable to AU only. Not applicable to BreezeNET B products. Enables or disables the relaying of broadcast messages to the wireless link.	Integer disable (1) enable (2) na (255)
*UnicastRelaying (*BridgeParameters 5)	Applicable to AU only. Not applicable to BreezeNET B products. Enables or disables the relaying of unicast messages to the wireless link.	Integer disable (1) enable (2) na (255)
*EthBroadcastFiltering (*BridgeParameters 6)	Applicable to SU/RB only. Enables or disables the filtering of Ethernet (layer2) broadcasts. disable: No filtering. onEthernetOnly: Filters broadcasts received on the Ethernet port only. onWirelessOnly: Filters broadcasts received on the wireless port only. onBothWirelessAndEthernet: Filters broadcasts received on both ports.	Integer disable (1) onEthernetOnly (2) onWirelessOnly (3) onBothWirelessAndEthernet (4) na (255)
*EthBroadcastingParameters (*BridgeParameters 7)		

MIB Parameter	Description	Value/Range
*DHCPBroadcastOverrideFilter (*EthBroadcastingParameters 1)	Applicable to SU/RB only. Enables or disables the broadcasting of DHCP messages, overriding the general *EthBroadcastFiltering Ethernet broadcast filtering option.	Integer disable (1) enable (2) na (255)
*PPPoEBroadcastOverrideFilter (*EthBroadcastingParameters 2)	Applicable to SU/RB only. Enables or disables the broadcasting of PPPoE messages, overriding the general *EthBroadcastFiltering Ethernet broadcast filtering option.	Integer disable (1) enable (2) na (255)
*ARPBroadcastOverrideFilter (*EthBroadcastingParameters 3)	Applicable to SU/RB only. Enables or disables the broadcasting of ARP messages, overriding the general *EthBroadcastFiltering Ethernet broadcast filtering option.	Integer disable (1) enable (2) na (255)
*EthBroadcastMulticastLimiterOption (*EthBroadcastingParameters 4)	Applicable to all units. Enable/disable the limiter for multicast and broadcast packets.	Integer disable (1) limitOnlyBroadcasts(2) limitMulticastsExceptBroadcasts(3) limitAllMulticasts(4)
*EthBroadcastMulticastLimiterThreshold (*EthBroadcastingParameters 5)	Applicable to all units. The limit for the allowed number of multicast and broadcast packets when the Ethernet Broadcast/Multicast Limiter Option is enabled	Integer 0 - 204800
*EthBroadcastMulticastLimiterSendTrapInterval (*EthBroadcastingParameters 5)	Applicable to all units. The minimum time in minutes between two successive traps that are sent, indicating the number of packets that were dropped by the Ethernet Broadcast/Multicast Limiter since the last trap was sent.	Integer 1-60
*ToSPriorityParameters (*BridgeParameters 8)		
*ToSPrecedenceThreshold (*ToSPriorityParameters 1)	Applicable to all units. Not applicable to units with SW version 3.1 and higher. Priority threshold (based on the ToS) for frames received from Ethernet port.	Integer 0-7
*RoamingOption (*BridgeParameters 9)	Applicable to SU/RB only. Disable/enable the roaming feature. When enabled, the SU will start scanning for an AU/RB after one second of not receiving beacons from current AU/BU. Once it found a new AU/BU, it will also send through the wireless network a roaming SNAP on behalf of its clients informing other devices in the network of their new location. When disabled, it will wait for seven seconds before starting scanning, and it will not send roaming SNAPS.	Integer disable (1) enable (2) na (255)
*MacAddressDenyList (*BridgeParameters 10)	MAC Address Deny List parameters	
*MacAddressDenyListTable (*MacAddressDenyList 1)	Applicable to AU only. Not applicable to BreezeNET B units. A list of up to 100 MAC Addresses of SUs that are not allowed to transfer data to the AU. Not accessible.	
*MacAddressDenyListEntry (*MacAddressDenyListTable 1)	Applicable to AU only. Not applicable to BreezeNET B units. An entry in the Mac Address Deny List Table. Not accessible.	

MIB Parameter	Description	Value/Range
*MacAddressDenyListTableIdx (*MacAddressDenyListEntry 1)	Applicable to AU only. Not applicable to BreezeNET B units. A read only table index for a MAC Address entry in the Mac Address Deny List Table.	Integer Range: 1 to 100
*MacAddressDenyListId (*MacAddressDenyListEntry 2)	Applicable to AU only. Not applicable to BreezeNET B units. The list of MAC Addresses in the MAC Address Deny List Table. To Remove a MAC Address - SET the corresponding entry to 0. To Add a new MAC Address - SET an entry which is currently 0.	MAC Address
*MacAddressDenyListAdd (*MacAddressDenyList 2)	Applicable to AU only. Not applicable to BreezeNET B units. Add a MAC address to the MAC Address Deny List Table	MAC Address
*MacAddressDenyListRemove (*MacAddressDenyList 3)	Applicable to AU only. Not applicable to BreezeNET B units. Remove a MAC address from the MAC Address Deny List Table	MAC Address
*NumberOfMacAddressesInDenyList (*MacAddressDenyList 4)	Applicable to AU only. Not applicable to BreezeNET B units. Read only. The number of MAC addresses in the MAC Address Deny List Table.	Integer Range: 0 to 100 Na (255)
*PortsControl (*BridgeParameters 11)	Ports Control parameters. Applicable to SU/RB only.	
*EthernetPortControl (*PortsControl 1)	Applicable to SU/RB only. Enable/disable the Ethernet port. When disabled, only data frames are blocked. Management frames are accepted.	Integer disable (1), enable (2), na (255)

E.2.6 Air Interface Parameters

MIB Parameter	Description	Value/Range
*AirInterface (breezeAccessVLMib 6)	Applicable to all units. Air Interface parameters.	
*ESSIDParameters (*AirInterface 1)	Applicable to all units. ESSID Parameters.	
*ESSID (*ESSIDParameters 1)	Applicable to all units. The Extended Service Set ID (ESSID) used to prevent the merging of collocated systems. The ESSID is accessible only with the write community string (administrator password).	DisplayString (SIZE(31)) Up to 31 printable case sensitive ASCII characters.
*OperatorESSIDOption (*ESSIDParameters 2)	Applicable to AU/BU only. Enabling/disabling the use of the Operator ESSID	Integer disable (1) enable (2) na (255)
*OperatorESSID (*ESSIDParameters 3)	Applicable to AU/BU only. A secondary ESSID to support easy installation of SUs as well as the use of the Best AU/BU feature. Accessible only with SNMP Write Community string (administrator password).	DisplayString (SIZE(31)) Up to 31 printable case sensitive ASCII characters.

MIB Parameter	Description	Value/Range
*RunTimeESSID (*ESSIDParameters 1)	Applicable to SU/RB only. The ESSID of the associated AU/BU. Accessible only with SNMP Write Community string (administrator password).	DisplayString (SIZE(31)) Up to 31 printable case sensitive ASCII characters.
*MaximumCellDistance (*AirInterface 2)	Applicable to all units. For AU/BU: read-write. For SU/RB: read-only. The distance is learned from the AU/BU. In units with SW version 2.0 and up - applicable only when the Cell Distance Mode is set to Manual. The highest distance from the AU/BU of any SU/RB served by it. Affects the maximum time the units wait for a response message and the slot size by taking into account the round trip propagation delay.	Integer Range: For units with SW version bellow version 2.0 the range is 0 - 50000 Meters. For units with SW version 2.0 and up the range is 0 to 54 Kilometers. 0 means no compensation (minimum slot size, maximal delay timeout).
*AIFS (*AirInterface 3)	Applicable to AU and SU. Not applicable to BreezeNET B products. Arbitration Inter-Frame Spacing (AIFS). This is the number of time slots that define the DIFS. (DIFS=SIFS+AIFS). A value of 1 should be used only in point-to-point applications to allow one unit to have advantage over the other unit.	Integer oneSlot (1) twoSlots (2) na (255)
*WirelessTrapThreshold (*AirInterface 4)	Applicable to AU/BU only. A wireless link quality threshold, expressed in % of retransmissions, for sending the brzaccVLAUWirelessQuality TRAP. This trap indicate whether the quality has gone below or above the specified threshold	Integer 1-100 (%)
*TransmitPowerTable (*AirInterface 5)	Applicable to all units. Not accessible. Transmit Power parameters table.	
*TransmitPowerEntry (*TransmitPowerTable 1)	Applicable to all units. Not accessible. An entry in the Transmit Power parameters table.	
*TransmitPowerIdx (*TransmitPowerEntry 1)	Applicable to all units. Read-only. An index of an entry in the Transmit Power parameters table.	Integer 1-4

MIB Parameter	Description	Value/Range
*ApplicableModulationLevel (*TransmitPowerEntry 2)	Applicable to all units. Read-only. The applicable modulation level for an entry in the Transmit Power parameters table. Level 8 is not applicable to units with HW revision A.	Level1to5 (1) Level6 (2) Level7 (3) Level8 (4)
*MaximumTxPowerRange (*TransmitPowerEntry 3)	Applicable to all units. Read-only. The allowed range for the *TxPower parameter at the applicable modulation level.	DisplayString Range: -10 to the maximum allowed for the applicable modulation level.
*TxPower (*TransmitPowerEntry 4)	Applicable to all units. AU/BU: The transmit power defined for the applicable modulation level. SU/RB: If ATPC is disabled, this is The transmit power defined for the applicable modulation level. If ATPC is enabled, it serves as the initial transmit power for the ATPC algorithm.	DisplayString Range: In SU/RB: The range is -10 dBm to the power value defined by *MaximumTxPower for the applicable modulation level. In AU/BU: The range is -10 dBm to the power value defined by *MaximumTxPowerRange for the applicable modulation level
*CurrentTxPower (*TransmitPowerEntry 5)	Applicable to SU/RB. The actual transmit power in dBm at the applicable modulation level.	DisplayString Range: -17 to the maximum value defined by *MaximumTxPowerRange for the applicable modulation level.
*MaximumTransmitPowerTable (*AirInterface 6)	Applicable to SU /RB. Not accessible. Maximum Transmit Power parameters table.	
*MaximumTransmitPowerEntry (*TransmitPowerTable 1)	Applicable to SU/RB. Not accessible. An entry in the Maximum Transmit Power parameters table.	
*MaximumTransmitPowerIdx (*MaximumTransmitPowerEntry 1)	Applicable to SU/RB. Read-only. An index of an entry in the Maximum Transmit Power parameters table.	Integer 1-4
*MaxTxApplicableModulationLevel (*MaximumTransmitPowerEntry 2)	Applicable to SU/RB. Read-only. The applicable modulation level for an entry in the Maximum Transmit Power parameters table. Level 8 is not applicable to units with HW revision A.	Level1to5 (1) Level6 (2) Level7 (3) Level8 (4)
*DefinedMaximumTxPowerRange (*MaximumTransmitPowerEntry 3)	Applicable to SU/RB. Read-only. The allowed range for the *MaxTxPower parameter at the applicable modulation level.	DisplayString Range: -10 to the maximum allowed for the applicable modulation level.

MIB Parameter	Description	Value/Range
*MaxTxPower (*MaximumTransmitPowerEntry 4)	Applicable to SU/RB. The maximum transmit power level that can be either configured for the *TxPower parameter or reached by the ATPC algorithm.	DisplayString Range: -10 to the maximum defined by the *DefinedMaximumTxPowerRange for the applicable modulation level.
*MaxNumOfAssociations (*AirInterface 10)	Applicable to AU. Not applicable to BreezeNET B products. The upper limit for the number of Subscriber Units that can be associated with the AU.	Integer AU-BS, AU-SA: 0-512 (0-124 if Data Encryption Option is enabled). AUS-BS, AUS-SA: 0-5. na (65535)
*BestAu (*AirInterface 11)	Best AU/BU parameters. Applicable to SU/RB.	
*BestAuSupport (*BestAu 1)	Applicable to SU/RB. Disable/enable the Best AU/BU selection mechanism	Integer disable (1) enable (2) na (255)
*BestAuNoOfScanningAttempts (*BestAu 2)	Applicable to SU/RB. The number of scanning attempts to collect information for the Best AU/BU decision	Integer 1-255
*PreferredAuMacAddress (*BestAu 3)	Applicable to SU only. The MAC address of the preferred AU/BU (overriding the Best AU/BU selection process).	Mac Address 000000000000 means no preferred AU
*NeighborAuTable (*BestAu 4)	Applicable to SU/RB. Not accessible. Neighboring AUs/BUs table.	
*NeighborAuEntry (*NeighborAuTable 1)	Applicable to SU only. Not accessible. An entry in the Neighboring AUs table.	
*NeighborAuldx (*NeighborAuEntry 1)	Applicable to SU/RB. Read-only. An Index of an entry in the Neighboring AU/BU Table	Integer Range: 1...20
*NeighborAuMacAdd (*NeighborAuEntry 2)	Applicable to SU/RB. Read-only. The MAC Address of the AU/BU associated with the entry in the Neighboring AU/BU Table	MAC Address
*NeighborAuESSID (*NeighborAuEntry 3)	Applicable to SU/RB. Read-only. The ESSID of the AU/BU associated with the entry in the Neighboring AU/BU Table. Accessible only with the SNMP Write community string (Administrator Password).	DisplayString
*NeighborAuSNR (*NeighborAuEntry 4)	Applicable to SU/RB. Read-only. The average SNR at which the SU/RB receives the AU/BU associated with the entry in the Neighboring AU/BU Table.	Integer Na (255)

MIB Parameter	Description	Value/Range
*NeighborAuAssocLoadStatus (*NeighborAuEntry 5)	Applicable to SU/RB. Read-only. The load status of the AU/BU associated with the entry in the Neighboring AU/BU Table. Full means that it has reached its maximum permitted load, meaning in AU that the number of associated SUs is the Maximum Number Of Associations (for AU) or in BU that it is already associated with an RB.	Integer full (1) notFull (2) na (255)
*NeighborAuMark (*NeighborAuEntry 6)	Applicable to SU/RB. Read-only. The overall mark given by the Best AU/BU algorithm to the AU/BU associated with the entry in the Neighboring AU/BU Table.	Integer
*NeighborAuHwRevision (*NeighborAuEntry 7)	Applicable to SU/RB. Read-only. The HW revision of the AU/BU associated with the entry in the Neighboring AU/BU Table.	Integer HwRevisionA (1), HwRevisionB (2), HwRevisionC (3), na (255)
*NeighborAuCountryCode (*NeighborAuEntry 8)	Applicable to SU/RB. Read-only. The Country Code of the AU/BU associated with the entry in the Neighboring AU/BU Table.	Integer
*NeighborAuSwVer (*NeighborAuEntry 9)	Applicable to SU/RB. Read-only. The SW Version of the AU/BU associated with the entry in the Neighboring AU/BU Table.	DisplayString
*NeighborAuAtpcOption (*NeighborAuEntry 10)	Applicable to SU/RB. Read-only. The current ATPC Option of the AU/BU associated with the entry in the Neighboring AU/BU Table.	Integer disable (1), enable (2), na (255)
*NeighborAuAdapModOption (*NeighborAuEntry 11)	Applicable to SU/RB. Read-only. The current Adaptive Modulation Option of the AU/BU associated with the entry in the Neighboring AU/BU Table.	Integer disable (1), enable (2), na (255)
*NeighborAuBurstModeOption (*NeighborAuEntry 12)	Applicable to SU/RB. Read-only. The current Burst Mode Option of the AU/BU associated with the entry in the Neighboring AU/BU Table.	Integer disable (1), enable (2), na (255)
*NeighborAuDfsOption (*NeighborAuEntry 14)	Applicable to SU/RB. Read-only. The current DFS Option of the AU/BU associated with the entry in the Neighboring AU/BU Table.	Integer disable (1), enable (2), na (255)

MIB Parameter	Description	Value/Range
*NeighborAuConcatenationOption (*NeighborAuEntry 15)	Applicable to SU/RB. Read-only. The current Concatenation Option of the AU/BU associated with the entry in the Neighboring AU/BU Table.	Integer disable (1), enable (2), na (255)
*NeighborAuLearnCountryCodeBy SU (*NeighborAuEntry 17)	For future use. Applicable to SU/RB. Read-only. The current Country Code Learning by SU option of the AU/BU associated with the entry in the Neighboring AU/BU Table.	Integer disable (1), enable (2), na (255)
*NeighborAuSecurityMode (*NeighborAuEntry 18)	For future use. Applicable to SU/RB. Read-only. The current Security Mode of the AU/BU associated with the entry in the Neighboring AU/BU Table.	Integer wep (1), aes (2), na (255)
*NeighborAuAuthOption (*NeighborAuEntry 19)	For future use. Applicable to SU/RB. Read-only. The current Authentication algorithm of the AU/BU associated with the entry in the Neighboring AU/BU Table.	Integer openSysteme (1), sharedKey (2), na (255)
*NeighborAuDataEncryptOption (*NeighborAuEntry 20)	For future use. Applicable to SU/RB. Read-only. The current Data Encryption option of the AU/BU associated with the entry in the Neighboring AU/BU Table.	Integer disable (1), enable (2), na (255)
*FrequencyDefinition (*AirInterface 12)	Frequency Definition parameters	
*SubBandLowerFrequency (*FrequencyDefinition 1)	Applicable to SU/RB. Not applicable to units with SW version 2.0 or higher. The lowest frequency in the subset to be used for scanning. For 5.8 GHz products the range is 5740 to 5830 MHz using a 10 MHz resolution. For 4.9GHz products the range is 4920 to 5080 MHz using a 10 MHz resolution. For HW Revision C and above this leaf is not relevant - shall return 0.	Integer

MIB Parameter	Description	Value/Range
*SubBandUpperFrequency (*FrequencyDefinition 2)	Applicable to SU/RB. Not applicable to units with SW version 2.0 or higher. The lowest frequency in the subset to be used for scanning. For 5.8 GHz products the range is 5740 to 5830 MHz using a 10 MHz resolution. For 4.9G Hz products the range is 4920 to 5080 MHz using a 10 MHz resolution. For HW Revision C and above this leaf is not relevant - shall return 0.	Integer
*ScanningStep (*FrequencyDefinition 3)	Applicable to all units - For flexible Sub-Bands only. For units with version 2.0 and above this is a read-only parameter. The scanning step to be used for generating the frequency subset.	Integer mhz-5 (1), mhz-10 (2), mhz-20 (3) na (255)
*FrequencySubsetTable (*FrequencyDefinition 4)	Applicable to all units. Not accessible. The Frequency Subset table that includes all frequencies from the Sub-band Lower Frequency to the Sub-band Upper Frequency, using steps as defined by the Scanning Step	
*FrequencySubsetEntry (FrequencySubsetTable 1)	Applicable to all units. Not accessible. An entry in the Frequency Subset table.	
*FrequencySubsetTableIdx (*FrequencySubsetEntry 1)	Applicable to all units. Read-only. The index of an entry in the Frequency Subset table.	Integer
*FrequencySubsetFrequency (*FrequencySubsetEntry 2)	Applicable to all units with HW revision B and lower (for units with HW revision C and higher replaced by *FrequencySubsetFrequencyNew to support a resolution of 0.5 MHz). Read-only. The frequency in MHz of an entry in the Frequency Subset table.	Integer
*FrequencySubsetActive (*FrequencySubsetEntry 3)	Applicable to all units. Read-only. The status of an entry in the Frequency subset Table. Only frequencies of active entries will be included in the final list of frequencies to be used for scanning.	Integer active (1) notActive (2)

MIB Parameter	Description	Value/Range
*FrequencySubsetFrequencyNew (*FrequencySubsetEntry 4)	Applicable to all units. Read-only. The frequency in MHz of an entry in the Frequency Subset table. (Replaces *FrequencySubsetFrequency to support a resolution of 0.5 MHz for units with HW revision C and higher).	DisplayString
*SetSelectedFreqsSubset (*FrequencyDefinition 5)	Applicable to all units. Apply the selected subset. After the next reset the new subset will be used for scanning.	Integer SetSelectedFreqsSubset (1) cancel (2)
*CurrentFrequencySubsetTable (*FrequencyDefinition 6)	Applicable to all units. Not accessible. The Current Frequency Subset table that includes all frequencies that are currently used for scanning.	
*CurrentFrequencySubsetEntry (CurrentFrequencySubsetTable 1)	Applicable to all units. Not accessible. An entry in the Current Frequency Subset table.	
*CurrentFrequencySubsetTableIdx (*CurrentFrequencySubsetEntry 1)	Applicable to all units. Read-only. The index of an entry in the Current Frequency Subset table.	Integer
*CurrentFrequencySubsetFrequency (*FrequencySubsetEntry 2)	Applicable to all units with HW revision B and lower (for units with HW revision C and higher replaced by *CurrentFrequencySubsetFrequencyNew to support a resolution of 0.5 MHz). Read-only. The frequency in MHz of an entry in the Current Frequency Subset table.	Integer
*CurrentFrequencySubsetFrequencyNew (*FrequencySubsetEntry 3)	Applicable to all units. Read-only. The frequency in MHz of an entry in the Current Frequency Subset table. (Replaces *CurrentFrequencySubsetFrequency to support a resolution of 0.5 MHz for units with HW revision C and higher).	DisplayString
*CurrentAUOperatingFrequency (*FrequencyDefinition 7)	Applicable to AU/BU with HW revision B and lower (for units with HW revision C and higher replaced by *CurrentUOperatingFrequencyNew to support a resolution of 0.5 MHz). Read-only. The operating frequency in MHz.	Integer For 5.8 GHz products with SW version below 2.0 the range is 5740 to 5830 MHz using a 10 MHz resolution. For units with SW version 2.0 and up the range is as defined in the selected Sub-Band.

MIB Parameter	Description	Value/Range
*AUDefinedFrequency (*FrequencyDefinition 8)	Applicable to AU/BU with HW revision B and lower (for units with HW revision C and higher replaced by *DefinedAUOperatingFrequencyNew to support a resolution of 0.5 MHz). Read-only. For 5.8 GHz products with SW version below 2.0 this is the frequency in MHz of the AU/BU after the next reset. For units with SW version 2.0 and up this is the frequency in MHz to use when the DFS Option is disabled.	Integer For 5.8 GHz products with SW version below 2.0 the range is 5740 to 5830 MHz using a 10M Hz resolution. For units with SW version 2.0 and up the range is as defined in the selected Sub-Band.
*CurrentSUOperatingFrequency (*FrequencyDefinition 9)	Applicable to SU/RB. Read only. The current operating frequency in MHz.	DisplayString For 5.8 GHz products with SW version below 2.0 the range is 5740 to 5830 MHz using a 10 MHz resolution. For units with SW version 2.0 and up the range is as defined in the selected Sub-Band.
*SubBandSelect (*FrequencyDefinition 10)	Sub-Band Selection parameters	
*SelectSubBandIndex (*SubBandSelect 1)	Applicable to all units. The ID of the sub-band used by the unit.	Integer
*DFSPParameters (*FrequencyDefinition 11)	DFS Parameters. Applicable to AU/BU.	
*DFSOption (*DFSPParameters 1)	Applicable to AU/BU. Enabling/disabling the DFS Algorithm. Not applicable if DFS Option is not supported by the current Sub-Band.	Integer disable (1) enable (2) na (255)
*DFSChannelCheckTime (*DFSPParameters 3)	Applicable to AU/BU. Defines the time the unit checks the channel for presence of radar signals and does not transmit after power up or association or after moving to a new channel due to detecting radar in the previously used channel.	Integer Range: 1 to 3600 (seconds).
*DFSChannelAvoidancePeriod (*DFSPParameters 4)	Applicable to AU/BU. Defines the time after detecting radar signals in a channel of avoiding using the channel or adjacent channels in accordance with the bandwidth.	Integer Range: 1 to 60 (minutes).

MIB Parameter	Description	Value/Range
*DFSSuWaitingOption (*DFSPParameters 5)	Applicable to AU/BU. Defines whether the associated SUs may should wait for this AU/BU after it stopped transmitting due to radar detection, before they starts scanning for other AUs/BUs.	Integer disable (1) enable (2) na (255)
*DFSClearRadarChannels (*DFSPParameters 6)	Applicable to AU/BU. Clear Radar Detected and Adjacent to Radar channels after unit reset. Returns the unit to operate in default frequency	Integer cancel (1) clearRadarChannels (2) na (255)
*DFSRadarDetectionChannelsTable (*DFSPParameters 7)	Applicable to AU/BU. Applicable only when DFS option is on. Displays the current channels defined in the sub-band and their radar detection status.	
*DFSRadarDetectionChannelsEntry (*DFSRadarDetectionChannelsTable 1)	Applicable to AU/BU. An entry in the DFS Radar Detection Channels Table.	
*DFSChannelIdx (*DFSRadarDetectionChannelsEntry 1)	Applicable to AU/BU. Read-only. The index of the entry in the DFS Radar Detection Channels Table.	Integer
*DFSChannelFrequency (*DFSRadarDetectionChannelsEntry 2)	Applicable to AU/BU with HW revision B and lower (for units with HW revision C and higher replaced by *DFSChannelFrequencyNew to support a resolution of 0.5 MHz). Read-only. The frequency in MHz of a channel in the DFS Radar Detection Channels Table.	Integer
*DFSChannelRadarStatus (*DFSRadarDetectionChannelsEntry 3)	Applicable to AU/BU. The radar detection status of a channel in the DFS Radar Detection Channels Table.	Integer radarFree (1) adjacentToRadar (2) radarDetected (3)
*DFSChannelFrequencyNew (*DFSRadarDetectionChannelsEntry 4)	Applicable to AU/BU. Read-only. The frequency of a channel in the DFS Radar Detection Channels Table. (Replaces *DFSChannelFrequency to support a resolution of 0.5 MHz for units with HW revision C and higher).	DisplayString
*DFSMinimumPulsesToDetect (*DFSPParameters 8)	Applicable to AU/BU. Defines the minimum number of pulses to detect radar.	Integer 1 - 100
*DFSChannelReuseParameters (*DFSPParameters 9)	Channel Reuse Parameters	

MIB Parameter	Description	Value/Range
*DFSChannelReuseOption (*DFSChannelReuseParameters 1)	Applicable to AU/BU. Enabling/disabling the DFS Channel Reuse Algorithm.	Integer disable (1) enable (2) na (255)
*DFS RadarActivityAssessmentPeriod (*DFSChannelReuseParameters 2)	Applicable to AU/BU. The period in hours for assessment of radar activity when the Channel reuse algorithm is enabled.	Integer 1 – 12 hours.
*DFSMaximumNumberOfDetection sInAssessmentPeriod (*DFSChannelReuseParameters 3)	Applicable to AU/BU. The maximum number of radar detection in the original channel during the Radar Activity Assessment Period that is required for reaching a decision to try again the original channel.	Integer 1 – 10 detections.
*CountryCodeLearningBySU (*FrequencyDefinition 12)	Applicable to AU only. Defines weather the SU should learn the country code of the AU.	Integer disable (1) enable (2) na (255)
*CurrentAUOperatingFrequencyNew (*FrequencyDefinition 13)	Applicable to AU/BU. Read-only. The operating frequency in MHz. (Replaces *CurrentAUOperatingFrequency to support a resolution of 0.5 MHz for units with HW revision C and higher).	DisplayString For 5.8 GHz products with SW version below 2.0 the range is 5740 to 5830 MHz using a 10 MHz resolution. For units with SW version 2.0 and up the range is as defined in the selected Sub-Band.
*AUDefinedFrequencyNew (*FrequencyDefinition 14)	Applicable to AU/BU. Read-only. For 5.8 GHz products with SW version below 2.0 this is the frequency in MHz of the AU/BU after the next reset. For units with SW version 2.0 and up this is the frequency in MHz to use when the DFS Option is disabled. (Replaces *AUDefinedFrequency to support a resolution of 0.5 MHz for units with HW revision C and higher).	DisplayString For 5.8 GHz products with SW version below 2.0 the range is 5740 to 5830 MHz using a 10 MHz resolution. For units with SW version 2.0 and up the range is as defined in the selected Sub-Band.
*ATPC (*AirInterface 13)	ATPC parameters	
*AtpcOption (*ATPC 1)	Applicable to all units. Enabling/disabling the ATPC Algorithm	Integer disable (1) enable (2) na (255)

MIB Parameter	Description	Value/Range
*DeltaFromMinSNRLevel (*ATPC 2)	Applicable to AU/BU. The Minimum SNR Level plus the value of this parameter define the maximum desired level of the average SNR at the AU/BU. If the ATPC Option is enabled, then if the received SNR is above the maximum desired level, the AU/BU will transmit Power-Down messages to the applicable SU/RB.	Integer 4-20 (dB)
*MinimumSNRLevel (*ATPC 3)	Applicable to AU/BU. Defines the minimum desired level in dB of the average SNR at the AU/BU. Below this level, if ATPC Option is enabled, the AU/BU will transmit ATPC Power-Up messages to the applicable SU/RB.	Integer 4-60 (dB)
*MinimumIntervalBetweenATPC Messages (*ATPC 4)	Applicable to AU/BU. The minimal time between consecutive power-up/power-down messages.	Integer Range: 1 to 3600 (seconds)
*PowerLevelSteps (*ATPC 6)	Applicable to AU/BU. The step in dB that the SU/RB will use when receiving an ATPC Power-Up/Power-Down message	Integer 1-20 (dB)
*CellDistanceParameters (*AirInterface 15)	Cell distance Parameters	
*CellDistanceMode (*CellDistanceParameters 1)	Applicable AU/BU. The selected mode of deciding on Cell Distance.	Integer automatic (1) manual (2) na (255)
*FairnessFactor (*CellDistanceParameters 2)	Applicable AU/BU. Not applicable to BreezeNET B products. The percentage of the maximum distance that is taken into account in the time slot calculation.	Integer Range: 0 to 100 (Percent). A value of 0 means the minimal slot size (9 microseconds). Na (255)
*MeasuredMaxCellDistance (*CellDistanceParameters 3)	Applicable AU/BU. The Maximum Cell Distance as calculated by the AU/BU.	Integer Range: 0 to 54 (Kilometers). 1 means "below 2 km".
*UnitWithMaxDistance (*CellDistanceParameters 4)	Applicable AU only. Not applicable to BreezeNET B units. The MAC address of the unit with the maximum distance from the AU.	MAC Address
*ScanningMode (*AirInterface 16)	Applicable to SU/RB. The scanning mode. In cells where the DFS Option is enabled Scanning Mode is forced to Passive.	Integer passive (1) active (2)

MIB Parameter	Description	Value/Range
*Antenna Gain (*AirInterface 17)	Applicable to all units. Read-write in units where *AntennaGainChange is supported. Read-only in units where *AntennaGainChange is not supported. The net gain (including cable attenuation for detached antennas) of the antenna.	Integer 0-50 (dB) -1 (not configurable) means "Not Set Yet". -2 (not configurable) means "Don't Care".
*SpectrumAnalysisParameters (*AirInterface 18)	Spectrum Analysis Parameters.	
*SpectrumAnalysisChannelScanPeriod (*SpectrumAnalysisParameters 1)	Applicable to all units. The period in seconds of staying on each channel for information gathering during each cycle when performing Spectrum analysis.	Integer Range: 2-30 seconds.
*SpectrumAnalysisChannelScanCycles (*SpectrumAnalysisParameters 2)	Applicable to all units. The number of scanning cycles when performing Spectrum Analysis.	Integer Range: 1-100 seconds.
*AutomaticChannelSelection (*SpectrumAnalysisParameters 3)	Applicable to AU/BU. Defines weather the AU/BU shall choose the most noise free channel upon startup after spectrum analysis.	Integer disable (1), enable (2), na (255)
*SpectrumAnalysisActivation (*SpectrumAnalysisParameters 4)	Applicable to all units. Activates the spectrum analysis. The unit is automatically reset upon activation.	Integer cancelOperation (1), activateNow (2)
*SpectrumAnalysisStatus (*SpectrumAnalysisParameters 5)	Applicable to all units. Read-only. Indicates whether the unit is currently performing a spectrum analysis process.	Integer inactive (1), currentlyActive (2)
*ResetSpectrumCounters (*SpectrumAnalysisParameters 6)	Applicable to all units. Resets the spectrum analysis counters.	Integer cancelOperation (1), resetCounters (2)
*SpectrumAnalysisInformationTable (*SpectrumAnalysisParameters 7)	Applicable to all units. Not accessible. The spectrum analysis information table.	
*SpectrumAnalysisInformationEntry (*SpectrumAnalysisInformationTable 1)	Applicable to all units. Not accessible. An entry in the spectrum analysis information table.	
*SpectrumAnalysisInformationTableIdx (*SpectrumAnalysisInformationEntry 1)	Applicable to all units. Read-only. A table index for a Spectrum Analysis Information Entry in the Spectrum Analysis Information Table.	
*SpectrumAnalysisInformationChannel (*SpectrumAnalysisInformationEntry 2)	Applicable to all units. Read-only. The channel's frequency of the relevant entry in the Spectrum Analysis Information Table.	DisplayString

MIB Parameter	Description	Value/Range
*SpectrumAnalysisInformationSignalCount (*SpectrumAnalysisInformationEntry 3)	Applicable to all units. Read-only. The number of signals (excluding OFDM frames) detected in the channel.	Integer
*SpectrumAnalysisInformationSignalSNR (*SpectrumAnalysisInformationEntry 4)	Applicable to all units. Read-only. The approximate SNR of the signals (excluding OFDM frames) detected in the relevant channel.	Integer
*SpectrumAnalysisInformationSignalWidth (*SpectrumAnalysisInformationEntry 5)	Applicable to all units. Read-only. The average width in microseconds of the signals (excluding OFDM frames) detected in the relevant channel.	Integer
*SpectrumAnalysisInformationOFDMFrames (*SpectrumAnalysisInformationEntry 6)	Applicable to all units. Read-only. The number of OFDM frames received in the relevant channel.	Integer
*MaxNumOfAssociationsLimit (*AirInterface 19)	Applicable to AU only. Not applicable to BreezeNET B products. Shows the limit for the number of SUs that can be associated with the AU.	Integer AU-BS, AU-SA: If Data Encryption is enabled, the upper limit is 124. Otherwise it is 512. AUS-BS, AUS-SA: 5 BreezeNET B products return 65535.
*Disassociate (*AirInterface 20)	Disassociation parameters.	
*DisassociateAllSUs (*Disassociate 1)	Applicable to AU. Disassociate all SUs.	Integer cancelOperation (1), disassociateAllSUs (2)
*DisassociateSuByMacAddress (*Disassociate 2)	Applicable to AU. Disassociate specified SU.	MacAddress
*TxControl (*AirInterface 21)	Applicable to AU/BU. Enables to turn the transmitter Off and On. The unit is reset automatically upon configuration.	Integer on(1) off (2)
*LostBeaconsWatchdogThreshold (*AirInterface 22)	Applicable to AU/BU. The number of unsuccessful consecutive transmissions of beacons before internal refresh is performed.	Integer Range: 100..1000 or '0' A value of '0' means that the lost beacons watchdog is not used and internal refresh is not performed

E.2.7 Service Parameters

MIB Parameter	Description	Value/Range
*ServiceParameters (breezeAccessVLMib 7)	Applicable to all units. Service parameters.	
*MirDownlink (*ServiceParameters 2)	Applicable to SU/RB. The Maximum Information Rate (MIR) from AU/BU to SU/RB. MIR must be above brzaccVLCirDownlink value.	Integer Range for Set: SU-3: 128 – 2,048 (Kbps) SU-6: 128 – 3,968 (Kbps) SU-54: 128 – 53,888 (Kbps) RB-14: 128 – 6,912 (Kbps) RB-28: 128 – 22,016 (Kbps) The actual value (Get) will be the entered value rounded to the nearest multiple of 128 (N*128)
*MirUplink (*ServiceParameters 3)	Applicable to SU/RB. The Maximum Information Rate (MIR) from SU/RB to AU/BU. MIR must be above brzaccVLCirUplink value.	Integer Range for Set: SU-3: 128 – 2,048 (Kbps) SU-6: 128 – 3,968 (Kbps) SU-54: 128 – 53,888 (Kbps) RB-14: 128 – 6,912 (Kbps) RB-28: 128 – 22,016 (Kbps) The actual value (Get) will be the entered value rounded to the nearest multiple of 128 (N*128)
*CirDownlink (*ServiceParameters 4)	Applicable to SU only. Not applicable to BreezeNET B products. The Committed Information Rate (CIR) from AU to SU. CIR must be below brzaccVLMirDownlink value.	Integer Range for Set: SU-3: 0 – 2,048 (Kbps) SU-6: 0 – 3,968 (Kbps) SU-54: 0 – 45,056 (Kbps) The actual value (Get) will be the entered value rounded to the nearest multiple of 128 (N*128). BreezeNET B products will return 65535 for na.
*CirUplink (*ServiceParameters 5)	Applicable to SU only. Not applicable to BreezeNET B products. The Committed Information Rate (CIR) from SU to AU. CIR must be below brzaccVLMirUplink value.	Integer Integer Range for Set: SU-3: 0 – 2,048 (Kbps) SU-6: 0 – 3,968 (Kbps) SU-54: 0 – 45,056 (Kbps) The actual value (Get) will be the entered value rounded to the nearest multiple of 128 (N*128). BreezeNET B products will return 65535 for na.
*MaxDelay (*ServiceParameters 6)	Applicable to SU only. Not applicable to BreezeNET B products. The maximal time packets may be delayed by the CIR/MIR mechanism. Above the configured maximal period the packets are discarded.	Integer Range: 300 - 10000 (milliseconds) BreezeNET B products will return 65535 for na.

MIB Parameter	Description	Value/Range
*MaxBurstDuration (*ServiceParameters 7)	Applicable to AU and SU. Not applicable to BreezeNET B products. The maximum time during which inactivity bonus time can be accumulated for future burst transmissions.	Integer Range: 0 – 2000 (milliseconds) BreezeNET B products will return 65535 for na.
*GracefulDegradationLimit (*ServiceParameters 8)	Applicable to AU only. Not applicable to BreezeNET B products. The maximum limit for activating the graceful degradation algorithm.	Integer Range: 0 – 70 (%) na (255)
*MirOnlyOption (*ServiceParameters 9)	Applicable only to AU. Not applicable to BreezeNET B products. When enabled, it overrides the CIR/MIR algorithm for determining actual information rate and forces the algorithm to operate with MIR parameters' settings only. When enabled, the Graceful Degradation algorithm is disabled.	Integer disable (1) enable (2) na (255)
*TrafficPrioritization (*ServiceParameters 10)	Traffic Prioritization parameters. Applicable to all units.	
*VLTrafficPriVLAN (*TrafficPrioritization 1)	VLAN Prioritization parameters. Applicable to all units.	
*LANPriorityThreshold (*VLTrafficPriVLAN 1)	Applicable to all units. If the VLAN Priority's value of the frame is less than or equal to this threshold, the frame will get Low priority, otherwise the frame will get High priority. Untagged frames will get Low priority.	Integer 0-7
*TrafficPriIPToS (*TrafficPrioritization 2)	ToS Prioritization parameters. Applicable to all units.	

MIB Parameter	Description	Value/Range
*ToSPrioritizationOption (*TrafficPriIPToS 1)	Applicable to all units. Disable/Enable IP ToS prioritization and chooses the interpretation of the IP ToS field from IP header: ipPrecedence(2): The IP ToS field is defined by RFC791. In this case the prioritization will be done using the Precedence sub-field of IP ToS. This sub-field has 3 bits, so it can be between 0 and 7. dSCP(3): The IP ToS field is defined by RFC2474. In this case the prioritization will be done using the DSCP sub-field. The size of the sub-field is 6 bits, so the range is 0 to 63.	Integer disable(1), ipPrecedence(2), dSCP(3)
*IPPrecedenceThreshold (*TrafficPriIPToS 2)	Applicable to all units. The threshold of Precedence sub-field of IP ToS field from IP Header (RFC791) to be used when the ToS Prioritization Option is set to IP Precedence. If the Precedence sub-field of a frame is less than or equal to this threshold the frame will have Low priority, otherwise it will get High priority.	Integer 0-7
*IPDSCPThreshold (*TrafficPriIPToS 3)	Applicable to all units. The threshold of DSCP sub-field of IP ToS field from IP Header (RFC2474) to be used when ToS Prioritization Option is set to DSCP. If the DSCP sub-field of a frame is less than or equal to this threshold the frame will have Low priority, otherwise it will get High priority.	Integer 0-63
*TrafficPriUdpTcpPortRange (*TrafficPrioritization 3)	UDP/TCP Port Ranges Prioritization parameters. Applicable to all units.	
*UdpTcpPortRangePrioritizationOption (*TrafficPriUdpTcpPortRange 1)	Applicable to all units. Disable/Enable Prioritization using UDP and/or TCP Port Ranges. udpOnly(2): prioritization will be done only for UDP packets tcpOnly(3): prioritization will be done only for TCP packets udpANDtcp(4): prioritization will be done for UDP and TCP packets	Integer disable(1), udpOnly(2), tcpOnly(3), udpANDtcp(4)

MIB Parameter	Description	Value/Range
*UdpPortRangeConfig (*TrafficPriUdpTcpPortRange 2)	UDP Port Range parameters. Applicable to all units.	
*UdpPortPriRTPRTCP (*UdpPortRangeConfig 1)	Applicable to all units. RTP/RTCP ports prioritization option for UDP packet. rtpANDrtcp(1): the possible RTP and RTCP packet with destination port in the defined port ranges will get High priority. rtpOnly(2): only possible RTP packet (packet with even destination port) with destination port in the defined port ranges will get High priority.	Integer rtpANDrtcp(1), rtpOnly(2)
*UdpPortRangeNum (*UdpPortRangeConfig 2)	Applicable to all units. Read-only. The number of entries in the UDP Port Range Table.	Integer
*UdpPortRangeTable (*UdpPortRangeConfig 3)	Applicable to all units. Not accessible. A table of UDP port ranges used for prioritization. The user can define up to 64 ranges. An entry is empty if start is 65535 and end is 0.	
*UdpPortRangeEntry (*UdpPortRangeTable 1)	Applicable to all units. Not accessible. A UDP Port Ranges Table entry.	
*UdpPortRangeStart (*UdpPortRangeEntry 1)	Applicable to all units. Read-only. Start port of an UDP Port Range	Integer 0-65535
*UdpPortRangeEnd (*UdpPortRangeEntry 2)	Applicable to all units. Read-only. End port of an UDP Port Range	Integer 0-65535
*UdpPortRangeIdx (*UdpPortRangeEntry 3)	Applicable to all units. Read-only. Index of an UDP Port Range entry	Integer 1-64
*UdpPortRangeAdd (*UdpPortRangeConfig 4)	Applicable to all units. Add port range(s) to UDP Port Ranges Table. Get operation will return an empty string.	DisplayString A range is defined by <start>-<end> or <start>, where <start> is the Start Port of the range and <end> is the End Port. If only <start> is specified the range is <start>-<start>. The value of <start> and <end> are between 0 and 65535. The user can add several ranges using a comma to separate between ranges. Example: 10-26,99,987-900.

MIB Parameter	Description	Value/Range
*UdpPortRangeDelete (*UdpPortRangeConfig 5)	Applicable to all units. Delete port range(s) from UDP Port Ranges Table. Get operation will return an empty string.	DisplayString A range is defined by <start>-<end> or <start>, where <start> is the Start Port of the range and <end> is the End Port. If only <start> is specified the range is <start>-<start>. The value of <start> and <end> are between 0 and 65535. The user can delete several ranges using a comma to separate between ranges. Example: 10-26,99,987-900.
*UdpPortRangeDeleteAll (*UdpPortRangeConfig 6)	Applicable to all units. Delete all entries form UDP Port Ranges Table. Get operation will return 1	Integer deleteAll(1), cancelOperation (2)
*TcpPortRangeConfig (*TrafficPriUdpTcpPortRange 3)	UDP Port Range parameters. Applicable to all units.	
*TcpPortPriRTPRTCP (*TcpPortRangeConfig 1)	Applicable to all units. RTP/RTCP ports prioritization option for TCP packets. rtpANDrtcp(1): the possible RTP and RTCP packet with destination port in the defined port ranges will get High priority. rtpOnly(2): only possible RTP packet (packet with even destination port) with destination port in the defined port ranges will get High priority.	Integer rtpANDrtcp(1), rtpOnly(2)
*TcpPortRangeNum (*TcpPortRangeConfig 2)	Applicable to all units. Read- only. The number of entries in the TCP Port Range Table.	Integer
*TcpPortRangeTable (*TcpPortRangeConfig 3)	Applicable to all units. Not accessible. A table of TCP port ranges used for prioritization. The user can define up to 64 ranges. An entry is empty if start is 65535 and end is 0.	
*TcpPortRangeEntry (*TcpPortRangeTable 1)	Applicable to all units. Not accessible. A TCP Port Ranges Table entry.	
*TcpPortRangeStart (*TcpPortRangeEntry 1)	Applicable to all units. Read- only. Start port of an TCP Port Range	Integer 0-65535
*TcpPortRangeEnd (*TcpPortRangeEntry 2)	Applicable to all units. Read- only. End port of an TCP Port Range	Integer 0-65535
*TcpPortRangeIdx (*TcpPortRangeEntry 3)	Applicable to all units. Read- only. Index of an TCP Port Range entry	Integer 1-64

MIB Parameter	Description	Value/Range
*TcpPortRangeAdd (*TcpPortRangeConfig 4)	Applicable to all units. Add port range(s) to TCP Port Ranges Table. Get operation will return an empty string.	DisplayString A range is defined by <start>-<end> or <start>, where <start> is the Start Port of the range and <end> is the End Port. If only <start> is specified the range is <start>-<start>. The value of <start> and <end> are between 0 and 65535. The user can add several ranges using a comma to separate between ranges. Example: 10-26,99,987-900.
*TcpPortRangeDelete (*TcpPortRangeConfig 5)	Applicable to all units. Delete port range(s) from TCP Port Ranges Table. Get operation will return an empty string.	DisplayString A range is defined by <start>-<end> or <start>, where <start> is the Start Port of the range and <end> is the End Port. If only <start> is specified the range is <start>-<start>. The value of <start> and <end> are between 0 and 65535. The user can delete several ranges using a comma to separate between ranges. Example: 10-26,99,987-900.
*TcpPortRangeDeleteAll (*TcpPortRangeConfig 6)	Applicable to all units. Delete all entries form TCP Port Ranges Table. Get operation will return 1	Integer deleteAll(1), cancelOperation (2)

E.2.8 User Filtering Parameters

MIB Parameter	Description	Value/Range
*UserFilterParams (breezeAccessVLMib 8)	Applicable to SU/RB. User filtering parameters.	
*UserFilterOption (*UserFilterParams 1)	Applicable to SU/RB. Defines user-filtering options. disable: No filtering. ipOnly: Only IP protocol packets pass. userDefinedAddrOnly: Only IP frames from/to user defined IP addresses pass. pPPoE Only: Only PPPoE frames pass.	Integer disable (1) ipOnly (2) userDefinedAddrOnly (3) pPPoEOnly (4) na (255)
*IpFilterTable (*UserFilterParams 2)	Applicable to SU/RB. A table of up to 8 user defined addresses, or address groups, to be used if the User Filtering Option (*UserFilterOption) is userDefinedAddrOnly. Not accessible.	

MIB Parameter	Description	Value/Range
*IpFilterEntry (*IpFilterTable 1)	Applicable to SU/RB. An IP Filter table entry. Not accessible.	
*IpID (*IpFilterEntry 1)	Applicable to SU/RB. An IP address in the IP Filter table.	IP Address
*MaskID (*IpFilterEntry 2)	Applicable to SU/RB. An IP mask for the IP Filter entry. Either a mask or a range, but not both can be used to define an address group. If the range is other than 0, then the mask is ignored and only the range value is used to define the address group.	IP Address
*IpFilterRange (*IpFilterEntry 3)	Applicable to SU/RB. An address range for the IP Filter entry. The first address in the range is the IP address (*iPID). 0 means that the range is not used. Either a mask or a range, but not both can be used to define an address group. If the range is other than 0, then the mask is ignored and only the range value is used to define the address group.	Integer 0 - 255
*IpFilterIdx (*IpFilterEntry 4)	Applicable to SU/RB. Read-only. A table index for the IP Filter entry.	Integer 1-8
*DeleteOneUserFilter (*UserFilterParams 3)	Applicable to SU/RB. Deletes a single selected entry from the IP Filter table.	Integer deletefirstEntry (1) deletesecondEntry (2) deletethirdEntry (3) deletefourthEntry (4) deletefifthEntry (5) deletesixthEntry (6) deleteseventhEntry (7) deleteeighthEntry (8) cancelOperation (9) na (255)
*DeleteAllUserFilters (*UserFilterParams 4)	Applicable to SU/RB. Deletes all entries from the IP Filter table.	Integer deleteAll (1) cancelOperation (2) na (255)
*DHCPUnicastOverrideFilter (*UserFilterParams 5)	Applicable to SU/RB. Enables or disables the unicast DHCP messages, overriding the IP Filtering option.	Integer disable (1) enable(2) na (255)

E.2.9 Security Parameters

MIB Parameter	Description	Value/Range
*SecurityParams (breezeAccessVLMib 9)		
*AuthenticationAlgorithm (*SecurityParameters 1)	Applicable to all units. Enables/disables the authentication encryption option. openSystem: Authentication messages are not encrypted. sharedKey : Authentication messages are encrypted.	Integer openSystem (1) sharedKey (2)
*DefaultKey (*SecurityParameters 2)	Applicable to SU/RB. The ID of the key to be used for encrypting/decrypting the authentication messages.	Integer Range: 1 to 4.
*DataEncryptionOption (*SecurityParameters 3)	Applicable to all units. Enables/disables the data encryption option.	Integer disable (1) enable (2)
*DefaultMulticastKey (*SecurityParameters 4)	Applicable to AU/RB. The ID of the key to be used for encrypting/decrypting multicasts.	Integer Range: 1 to 4.
*SecurityMode (*SecurityParameters 5)	Applicable to all units. The encryption algorithm to be used for authentication messages and/or data encryption	Integer wep (1) aesOCB (2) aesCCM (3)
*PromiscuousAuthenticationMode (*SecurityParameters 6)	Applicable to AU/RB. Enabling/disabling the promiscuous mode, where any SU can be authenticated by and communicate with the AU.	Integer disable (1) enable (2)
*Key1 (*SecurityParameters 7)	Applicable to all units. Key number 1. Accessible only with SNMP Write Community String (administrator password).	DisplayString 32 hexadecimal digits
*Key2 (*SecurityParameters 8)	Applicable to all units. Key number 2. Accessible only with SNMP Write Community String (administrator password).	DisplayString 32 hexadecimal digits
*Key3 (*SecurityParameters 9)	Applicable to all units. Key number 3. Accessible only with SNMP Write Community String (administrator password).	DisplayString 32 hexadecimal digits
*Key4 (*SecurityParameters 10)	Applicable to all units. Key number 4. Accessible only with SNMP Write Community String (administrator password).	DisplayString 32 hexadecimal digits

MIB Parameter	Description	Value/Range
*SecurityModeSupport (SecurityParameters 12)	Applicable to all units. Returns types of encryption that are supported	Integer (0..7) No encryption (0) WEP (1) AES/OCB (2) WEP + AES/OCB (3) AES/CCM (4) WEP + AES/CCM (5) AES/OCB + AES/CCM (6) WEP + AES/OCB +AES/CCM (7)

E.2.10 Performance Parameters

MIB Parameter	Description	Value/Range
*PerformanceParams (breezeAccessVLMib 10)		
*RTSThreshold (*PerformanceParams 1)	Applicable to SU and AU. Not applicable to BreezeNET B products. The minimum frame size that requires an RTS/CTS handshake.	Integer 20-4032 (bytes) (20-1600 for units running SW version below 3.0, 20-3400 for units with SW version 3.0) na (65535)
*MinContentionWindow (*PerformanceParams 3)	Applicable to SU and AU. Not applicable to BreezeNET B products. The initial value to be used by the contention window calculation algorithm. A value of 0 disables the back-off algorithm and should be used only in point-to-point applications.	Integer 0, 7, 15, 31, 63, 127, 255, 511, 1023. na (65535)
*MaxContentionWindow (*PerformanceParams 4)	Applicable to SU and AU. Not applicable to BreezeNET B products. The maximum value to be used by the contention window calculation algorithm.	Integer 7, 15, 31, 63, 127, 255, 511, 1023 na (65535)
*MaximumModulationLevel (*PerformanceParams 5)	Applicable to all units. If the Adaptive Modulation algorithm is enabled, it sets the maximum modulation level to be used. If The Adaptive Modulation algorithm is disabled, it set the fixed modulation level to be used.	Integer Range: 1 to 8* *Range depends on HW version and Min/Max Modulation Levels as defined by Sub-Band.

MIB Parameter	Description	Value/Range
*MulticastModulationLevel (*PerformanceParams 6)	Applicable to AU/BU. The modulation level for multicast and broadcast data frames.	Integer Range: 1 to 8* *Range depends on HW version and Min/Max Modulation Levels as defined by Sub-Band.
*AvgSNRMemoryFactor (*PerformanceParams 7)	Applicable to all units. The weight of history in average RSSI calculation for the ATPC (AU only) and Adaptive Modulation algorithm. The higher is the value, the higher is the weight of history	DisplayString -1 (Disregard History) to 32
*HardwareRetries (*PerformanceParams 8)	Applicable to all units. The maximum number of trials to transmit an unacknowledged frame in each Hardware Retrials phase.	Integer 1-15
*AdaptiveModulationParams (*PerformanceParams 9)	Adaptive Modulation Parameters	
*AdaptiveModulationAlgorithmOption (*AdaptiveModulationParams 1)	Applicable to all units. Enabling/disabling the Adaptive Modulation algorithm.	Integer disable (1) enable (2)
*SoftwareRetrySupport (*AdaptiveModulationParams 2)	Applicable to all units. Read-only for units with version 2.0. Not applicable for units with SW version 3.0 and higher. The status of the Software Retry mechanism. Enabled when the Adaptive Modulation algorithm is enabled and the Burst Mode Option is disabled. Otherwise it is disabled.	Integer disable (1) enable (2) na (255)
*NumberOfSoftwareRetries (*AdaptiveModulationParams 3)	Applicable to all units. Read-only for units with version 2.0. Not applicable for units with SW version 3.0 and higher. The maximum number of times to use the Software Retry mechanism when it is enabled.	Integer 0-14
*MinimumIntervalBetweenAdaptiveModulationAlgorithmMessages (*AdaptiveModulationParams 4)	Applicable to all units. The minimum interval between two consecutive adaptive modulation algorithm messages carrying information on the SNR of received signals.	Integer 1-3600 (seconds)
*AdaptiveModulationDecisionThresholds (*AdaptiveModulationParams 5)	Applicable to all units. Defines the setting of thresholds for the rate decision algorithm. high (2) should typically be used when the SNR is lower than 13 dB.	Integer normal (1) high (2) na (255)
*BurstMode (*PerformanceParams 10)	Burst Mode Parameters. Applicable to all units.	

MIB Parameter	Description	Value/Range
*BurstModeOption (*BurstMode 1)	Applicable to all units. Applicable only if Burst Mode Option is supported by the Sub-Band. Enabling/disabling burst mode operation. blocked (3) value is returned when trying to enable Burst Mode when it should not be used due to the configuration of certain other parameters. These limitations depend on HW revision and unit type.	Integer disable (1) enable (2) blocked (3) na (255)
*BurstInterval (*BurstMode 2)	Applicable to all units. The burst interval in milliseconds.	Integer 1-the maximum value as defined in the Sub-Band. (milliseconds) na (255)
*ConcatenationParameters (*PerformanceParams 11)	Concatenation Parameters. Applicable to all units.	
*ConcatenationOption (*ConcatenationParameters 1)	Applicable to all units. Enabling/disabling the concatenation mechanism.	Integer disable (1) enable (2) na (255)
*ConcatenationMaximumNumberOfFrames (*ConcatenationParameters 2)	Applicable to all units. Defines the maximum number of data frames that can be concatenated.	Integer 2 – 8

E.2.11 Site Survey Parameters

MIB Parameter	Description	Value/Range
*SiteSurvey (breezeAccessVLMib 11)		
*AverageReceiveSNR (*SiteSurvey 1)	Applicable to SU/RB. Read-only. The average Signal to Noise Ratio of received frames.	Integer
*TrafficStatistics (*SiteSurvey 2)	Applicable to all units. Traffic statistics parameters.	
*ResetTrafficCounters (*TrafficStatistics 1)	Applicable to all units. Resets the traffic counters.	Integer reset (1) cancel (2)
*EthCounters (*TrafficStatistics 2)	Applicable to all units. Ethernet counters.	
*TotalRxFramesViaEthernet (*EthCounters 1)	Applicable to all units. Read-only. Total number of frames received via the Ethernet port.	Counter 32
*TxWirelessToEthernet (*EthCounters 2)	Applicable to all units. Read-only. Total number of frames transmitted to the Ethernet port.	Counter 32
*WirelessLinkCounters (*TrafficStatistics 3)	Applicable to all units. Wireless link counters.	
*TxFramesToWireless (*WirelessLinkCounters 1)	Transmitted frames counters	

MIB Parameter	Description	Value/Range
*AUBeaconsToWireless (*TxFramesToWireless 1)	Applicable to AU/BU. Read-only. The number of Beacon frames transmitted to the wireless medium.	Counter 32
*DataAndOtherMngFramesToWireless (*TxFramesToWireless 3)	Applicable to AU/BU. Read-only. The number of data and other management frames (excluding beacons) transmitted to the wireless medium. The count includes multicasts/broadcasts and one count for each unicast frame transmitted successfully (excluding retransmissions).	Counter 32
*TotalTxFramesToWireless (*TxFramesToWireless 4)	Applicable to all units. Read-only. The number of frames transmitted to the wireless medium. The count includes one count for each data frame transmitted successfully (excluding retransmissions), and the number of transmitted control and wireless management frames.	Counter 32
*TotalTransmitted Unicasts (*TxFramesToWireless 5)	Applicable to AU. Not applicable to BreezeNET B products. Read-only. The total number of unicast frames successfully transmitted to the wireless medium, excluding retransmissions.	Counter 32
*TotalTransmittedConcatenatedFramesDouble (*TxFramesToWireless 6)	Applicable to all units Read-only. The total number of double concatenated frames that were successfully transmitted to the wireless medium, excluding retransmissions.	Counter 32
*TotalTransmittedConcatenatedFramesSingle (*TxFramesToWireless 7)	Applicable to all units Read-only. The total number of single concatenated frames that were successfully transmitted to the wireless medium, excluding retransmissions.	Counter 32
*TotalTransmittedConcatenatedFramesMore (*TxFramesToWireless 8)	Applicable to all units Read-only. The total number of concatenated frames with more than two data frames that were successfully transmitted to the wireless medium, excluding retransmissions.	Counter 32

MIB Parameter	Description	Value/Range
*TotalRxFramesFromWireless (*WirelessLinkCounters 2)	Applicable to all units. Read-only. The total number of frames received from the wireless medium. The count includes data and control and wireless management frames, including beacons received from the AU. The count does not include frames discarded internally, bad frames and duplicate frames.	Counter 32
*TotalRetransmittedFrames (*WirelessLinkCounters 3)	Applicable to all units. Read-only. The total number of retransmissions of data frames (counts all unsuccessful transmissions/retransmissions).	Counter 32
*FramesDropped (*WirelessLinkCounters 4)	Applicable to all units. Read-only. The number of dropped frames. The frames retransmitted to the maximum allowed number of retransmissions without being acknowledged.	Counter 32
*DataFramesSubmittedToBridge (*WirelessLinkCounters 5)	Submitted frames counters	
*DataFramesSubmittedViaHighQueue (*DataFramesSubmittedToBridge 1)	Applicable to all units. Read-only. The number of data frames submitted to the internal bridge via the high priority queue for transmission to the wireless medium.	Counter 32
*DataFramesSubmittedViaMidQueue (*DataFramesSubmittedToBridge 2)	Applicable to all units. Read-only. The number of data frames submitted to the internal bridge via the mid priority queue for transmission to the wireless medium.	Counter 32
*DataFramesSubmittedViaLowQueue (*DataFramesSubmittedToBridge 3)	Applicable to all units. Read-only. The number of data frames submitted to the internal bridge via the low priority queue for transmission to the wireless medium.	Counter 32
*TotalNoOfDataFramesSubmitted (*DataFramesSubmittedToBridge 4)	Applicable to all units. Read-only. The total number of data frames submitted to the internal bridge for transmission to the wireless medium.	Counter 32
*TotalRecievedDataFrames (*WirelessLinkCounters 6)	Applicable to all units. Read-only. The total number of data frames received from the wireless medium, including duplicate frames.	Counter 32
*RecievedBadFrames (*WirelessLinkCounters 7)	Applicable to all units. Read-only. The number of frames received from the wireless medium with errors (CRC errors).	Counter 32

MIB Parameter	Description	Value/Range
*NoOfDuplicateFramesDiscarded (*WirelessLinkCounters 8)	Applicable to all units. Read-only. The number of frames discarded due to receiving multiple copies.	Counter 32
*InternallyDiscardedMirCir (*WirelessLinkCounters 9)	Applicable to all units. Read-only. The number of data frames received from the Ethernet port that were discarded by the MIR/CIR mechanism to avoid exceeding the maximum allowed information rate	Counter 32
*TotalRxConcatenatedFramesDouble (*WirelessLinkCounters 10)	Applicable to all units Read-only. The total number of double concatenated frames that were received from the wireless medium, including duplicate frames.	Counter 32
*TotalRxConcatenatedFramesSingle (*WirelessLinkCounters 11)	Applicable to all units Read-only. The total number of single concatenated frames that were received from the wireless medium, including duplicate frames.	Counter 32
*TotalRxConcatenatedFramesMore (*WirelessLinkCounters 12)	Applicable to all units Read-only. The total number of concatenated frames with more than two data frames that were received from the wireless medium, including duplicate frames.	Counter 32
*WirelessLinkEvents (*TrafficStatistics 4)	Applicable to all units. Wireless link event counters.	
*TxEvents (*WirelessLinkEvents 1)	Applicable to all units. Read-only. Tx event counters.	
*DroppedFrameEvents (*TxEvents 1)	Applicable to all units. The number frames that were dropped because they were retransmitted to the maximum allowed number of retransmissions without being acknowledged.	Counter 32
*FramesDelayedDueToSwRetry (*TxEvents 2)	Applicable to all units. Not applicable for units running SW version 3.0 and higher. The number of frames that were delayed because the SW retry algorithm was activated on a previous frame designated for the same recipient.	Counter 32
*Underrun Events (*TxEvents 3)	Applicable to all units. The number of frames whose transmission was aborted because the rate of submitting frames for transmission exceeds the available transmission capability.	Counter 32

MIB Parameter	Description	Value/Range
*OtherTxEvents (*TxEvents 4)	Applicable to all units. The number of Tx events due to problems other than those represented by the other Tx Events counters.	Counter 32
*TotalTxEvents (*TxEvents 5)	Applicable to all units. The total number of Tx events.	Counter 32
*RxEvents (*WirelessLinkEvents 2)	Applicable to all units. Read-only. Rx errors counters.	
*PhyErrors (*RxErrors 1)	Applicable to all units. Read-only. Applicable only when DFS is enabled. The number of unidentified signals.	Counter 32
*CRCEvents (*RxEvents 2)	Applicable to all units. Read-only. The number of frames received from the wireless medium containing CRC errors.	Counter 32
*OverflowEvents (*RxEvents 3)	Applicable to all units. Read-only. The number of frames that were discarded because the receive rate exceeded the processing capability or the capacity of the Ethernet port.	Counter 32
*RxDecryptEvents (*RxEvents 4)	Applicable to all units. Read-only. The number of frames that were not received properly due to a problem in the data decryption mechanism.	Counter 32
*TotalRxEvents (*RxEvents 5)	Applicable to all units. Read-only. The total number of Rx events.	Counter 32
*PerModulationLevelCounters (*TrafficStatistics 5)	Per Modulation Level Counters.	
*ResetPerModulationLevelCounters (*PerModulationLevelCounters 1)	Applicable to all units. Resets the Per Modulation Level Counters	Integer resetCounters (1) cancel (2)
*SUPerModulationLevelCountersTable (*PerModulationLevelCounters 2)	Applicable to SU/RB. Not accessible. The Per Modulation Level Counters Table.	
*SUPerModulationLevelCountersEntry (*PerModulationLevelCountersTable 1)	Applicable to SU/RB. Not accessible. An entry in the Per Modulation Level Counters Table.	
*SUPerModulationLevelCountersTableIdx (*PerModulationLevelCountersEntry 1)	Applicable to SU/RB. Read-only. The index of an entry in the Per Modulation Level Counters Table.	
*SUPerModulationLevelCountersApplicableModulationLevel (*PerModulationLevelCountersEntry 2)	Applicable to SU/RB. Read-only. The modulation level applicable for the entry in the Per Modulation Level Counters Table.	Integer Range: 1 to 8* *Level 8 is not applicable to devices with HW revision A
*SUPerModulationLevelCountersTxSuccess (*PerModulationLevelCountersEntry 3)	Applicable to SU/RB. Read-only. The total number of successfully transmitted unicasts at the applicable modulation level.	Counter 32

MIB Parameter	Description	Value/Range
*SUPerModulationLevelCountersTxFailed (*PerModulationLevelCountersEntry 4)	Applicable to SU/RB. Read-only. The total number of failures to successfully transmit a unicast frame during a HW Retry cycle at the applicable modulation level.	Counter 32
*AverageModulationLevel (*PerModulationLevelCounters 3)	Applicable to SU/RB. Read-only. The average modulation level for successful transmission (rounded to nearest integer) since last reset of the Per Modulation Level counters.	Integer 1-8.
*MacAddressDatabase (*SiteSurvey 5)	MAC Address Database	
*AUMacAddressDatabase (*MacAddressDatabase 1)	AU MAC Address Database	
*AdbResetAllCounters (*AUMacAddressDatabase 1)	Applicable to AU/BU. Resets all the counters for all SUs in the MAC Address Database.	Integer reset (1) noReset (2)
*AUadbTable (*AUMacAddressDatabase 2)	Applicable to AU/BU. Not accessible. The AU MAC Address Database Table.	
*AUadbEntry (*AUadbTable 1)	Applicable to AU/BU. Not accessible. An entry in the AU MAC Address Database Table.	
*AdbIndex (*AUadbEntry 1)	Applicable to AU/BU. Read-only. The Index of an entry in the AU MAC Address Database Table.	Integer
*AdbMacAddress (*AUadbEntry 2)	Applicable to AU/BU. Read-only. The MAC Address of an SU entry in the AU MAC Address Database Table.	MAC Address
*AdbStatus (*AUadbEntry 3)	Applicable to AU/BU. Read-only. The wireless status of the relevant SU.	Integer associated (1) authenticated (2) notAuthenticated (3)
*AdbSwVersion (*AUadbEntry 4)	Applicable to AU/BU. Read-only. The SW Version of the relevant SU.	Display String
*AdbSNR (*AUadbEntry 5)	Applicable to AU/BU. Read-only. The average Signal to Noise Ratio in dB of frames received by the AU from the relevant SU.	Integer 0-60
*AdbMaxModulationLevel (*AUadbEntry 6)	Applicable to AU/BU. Read-only. The value configured in the relevant SU for the Maximum Modulation Level parameter.	Integer Range: 1 to 8* *Level 8 is not applicable to devices with HW revision A.
*AdbTxFramesTotal (*AUadbEntry 7)	Applicable to AU/BU. Read-only. Counts the total number of frames (excluding retransmissions) that were transmitted by the AU to the relevant SU.	Counter 32

MIB Parameter	Description	Value/Range
*AdbDroppedFramesTotal (*AUAdbEntry 8)	Applicable to AU/BU. Read-only. Counts the total number of intended to the relevant SU that were dropped because they were retransmitted by the AU to the extent of the maximum allowed number of retransmissions without being acknowledged.	Counter 32
*AdbTxSuccessModLevel1 (*AUAdbEntry 9)	Applicable to AU/BU. Read-only. Counts the total number of unicast frames (excluding retransmissions) that were successfully transmitted to the SU over the wireless link using modulation level 1.	Counter 32
*AdbTxSuccess ModLevel2 (*AUAdbEntry 10)	Applicable to AU/BU. Read-only. Counts the total number of unicast frames (excluding retransmissions) that were successfully transmitted to the SU over the wireless link using modulation level 2.	Counter 32
*AdbTxSuccess ModLevel3 (*AUAdbEntry 11)	Applicable to AU/BU. Read-only. Counts the total number of unicast frames (excluding retransmissions) that were successfully transmitted to the SU over the wireless link using modulation level 3.	Counter 32
*AdbTxSuccess ModLevel4 (*AUAdbEntry 12)	Applicable to AU/BU. Read-only. Counts the total number of unicast frames (excluding retransmissions) that were successfully transmitted to the SU over the wireless link using modulation level 4.	Counter 32
*AdbTxSuccess ModLevel5 (*AUAdbEntry 13)	Applicable to AU/BU. Read-only. Counts the total number of unicast frames (excluding retransmissions) that were successfully transmitted to the SU over the wireless link using modulation level 5.	Counter 32
*AdbTxSuccess ModLevel6 (*AUAdbEntry 14)	Applicable to AU/BU. Read-only. Counts the total number of unicast frames (excluding retransmissions) that were successfully transmitted to the SU over the wireless link using modulation level 6.	Counter 32
*AdbTxSuccess ModLevel7 (*AUAdbEntry 15)	Applicable to AU/BU. Read-only. Counts the total number of unicast frames (excluding retransmissions) that were successfully transmitted to the SU over the wireless link using modulation level 7.	Counter 32

MIB Parameter	Description	Value/Range
*AdbTxSuccess ModLevel8 (*AUAdbEntry 16)	Applicable to AU/BU. Not applicable to units with HW revision A. Read-only. Counts the total number of unicast frames (excluding retransmissions) that were successfully transmitted to the SU over the wireless link using modulation level 8.	Counter 32
*AdbTxFailed ModLevel1 (*AUAdbEntry 17)	Applicable to AU/BU. Read-only. Counts the total number of failures to successfully transmit a unicast frame intended to the SU during a HW Retry cycle using modulation level 1.	Counter 32
*AdbTxFailed ModLevel2 (*AUAdbEntry 18)	Applicable to AU/BU. Read-only. Counts the total number of failures to successfully transmit a unicast frame intended to the SU during a HW Retry cycle using modulation level 2.	Counter 32
*AdbTxFailed ModLevel3 (*AUAdbEntry 19)	Applicable to AU/BU. Read-only. Counts the total number of failures to successfully transmit a unicast frame intended to the SU during a HW Retry cycle using modulation level 3.	Counter 32
*AdbTxFailed ModLevel4 (*AUAdbEntry 20)	Applicable to AU/BU. Read-only. Counts the total number of failures to successfully transmit a unicast frame intended to the SU during a HW Retry cycle using modulation level 4.	Counter 32
*AdbTxFailed ModLevel5 (*AUAdbEntry 21)	Applicable to AU/BU. Read-only. Counts the total number of failures to successfully transmit a unicast frame intended to the SU during a HW Retry cycle using modulation level 5.	Counter 32
*AdbTxFailed ModLevel6 (*AUAdbEntry 22)	Applicable to AU/BU. Read-only. Counts the total number of failures to successfully transmit a unicast frame intended to the SU during a HW Retry cycle using modulation level 6.	Counter 32
*AdbTxFailed ModLevel7 (*AUAdbEntry 23)	Applicable to AU/BU. Read-only. Counts the total number of failures to successfully transmit a unicast frame intended to the SU during a HW Retry cycle using modulation level 7.	Counter 32

MIB Parameter	Description	Value/Range
*AdbTxFailed ModLevel8 (*AUAdbEntry 24)	Applicable to AU/BU. Not applicable to units with HW revision A. Read-only. Counts the total number of failures to successfully transmit a unicast frame intended to the SU during a HW Retry cycle using modulation level 8.	Counter 32
*AdbCirTx (*AUAdbEntry 25)	Applicable to AU Only. Not applicable to BreezeNET B products. Read-only. The value configured in the relevant SU for the CIR: Uplink parameter.	Integer
*AdbMirTx (*AUAdbEntry 26)	Applicable to AU/BU. Read-only. The value configured in the relevant SU for the MIR: Uplink parameter.	Integer
*AdbCirRx (*AUAdbEntry 27)	Applicable to AU. Not applicable to BreezeNET B products. Read-only. The value configured in the relevant SU for the CIR: Downlink parameter.	Integer
*AdbMirRx (*AUAdbEntry 28)	Applicable to AU/BU. Read-only. The value configured in the relevant SU for the MIR: Downlink parameter.	Integer
*AdbCirMaxDelay (*AUAdbEntry 29)	Applicable to AU. Not applicable to BreezeNET B products. Read-only. The value configured in the relevant SU for the Maximum Delay parameter.	Integer
*AdbDistance (*AUAdbEntry 30)	Applicable to AU/BU. Read-only. The measured distance between the relevant SU/RB and the AU/BU (In Kilometers).	Integer 1 means any distance below 2 km
*AdbHwRevision (*AUAdbEntry 31)	Applicable to AU/BU. Read-only. The HW Revision of the relevant SU/RB.	Integer HwRevisionA (1), HwRevisionB (2), HwRevisionC (3), na(255)
*AdbCpldVer (*AUAdbEntry 32)	Applicable to AU/BU. Read-only. The CPLD Version of the relevant SU/RB.	DisplayString
*AdbCountryCode (*AUAdbEntry 33)	Applicable to AU/BU. Read-only. The Country Code of the relevant SU/RB.	Integer
*AdbBootVer (*AUAdbEntry 34)	Applicable to AU/BU. Read-only. The Boot Version of the relevant SU/RB.	DisplayString
*AdbAtpcOption (*AUAdbEntry 35)	Applicable to AU/BU. Read-only. The current ATPC Option of the relevant SU/RB.	Integer disable (1), enable (2), na(255)

MIB Parameter	Description	Value/Range
*AdbAdapModOption (*AUadbEntry 36)	Applicable to AU/BU. Read-only. The current Adaptive Modulation Option of the relevant SU/RB.	Integer disable (1), enable (2), na(255)
*AdbBurstModeOption (*AUadbEntry 37)	Applicable to AU/BU. Read-only. The current Burst Mode Option of the relevant SU/RB.	Integer disable (1), enable (2), na(255)
*AdbConcatenationOption (*AUadbEntry 39)	Applicable to AU/BU. Read-only. The current Concatenation Option of the relevant SU/RB.	Integer disable (1), enable (2), na(255)
*AdbSecurityMode (*AUadbEntry 41)	Applicable to AU/BU. Read-only. The current Security Mode of the relevant SU/RB.	Integer wep (1), aes (2), na(255)
*AdbAuthOption (*AUadbEntry 42)	Applicable to AU/BU. Read-only. The current Authentication Algorithm Option of the relevant SU/RB.	Integer openSystem(1), sharedKey (2), na(255)
*AdbDataEncryptOption (*AUadbEntry 43)	Applicable to AU/BU. Read-only. The current Data Encryption Option of the relevant SU/RB.	Integer disable (1), enable (2), na(255)
*AdbAge (*AUadbEntry 44)	Applicable to AU/BU. Read-only. The time in seconds elapsed since receiving the last packet from the relevant SU/RB.	Integer
*AdbUnitName (*AUadbEntry 45)	Applicable to AU/BU. Read-only. The Unit Name of the relevant SU/RB.	DisplayString
*UpLinkQualityIndicator (*SiteSurvey 6)	UpLink quality Indicator (LQI) parameters. Applicable only to SU/RB.	
*MeasureUpLinkQualityIndicator (*UpLinkQualityIndicator 1)	Applicable to SU/RB. Starts calculation of LQI. The calculation will be for a period of 10 seconds.	Integer start (1), cancel (2)
*ReadUpLinkQualityIndicator (*UpLinkQualityIndicator 2)	Applicable to SU/RB. Read-only. The results of the last LQI calculation.	Integer 1-8.
*UpLinkQualityIndicatorStatus (*UpLinkQualityIndicator 3)	Applicable to SU/RB Only. Indicates the test conditions. fullTest means that there are no limitations on the range of available modulation levels, and that all modulation levels from 1 to 8 can be used. limitedTest indicates that the results may not indicate the true quality since the available range is limited - by HW (HW Revision A), or by the applicable parameters in the country code, or by the configurable Maximum Modulation Level parameter.	Integer fullTest (1), limitedTest (2)
*MacPinpoint (*SiteSurvey 7)	Applicable to AU/BU. MAC Pinpoint parameters.	

MIB Parameter	Description	Value/Range
*MacPinpointTable (*MacPinpoint 1)	Applicable to AU/BU. MAC Pinpoint table. Not accessible.	
*MacPinpointEntry (MacPinpointTable 1)	Applicable to AU/BU. An entry in the MAC Pinpoint table. Not accessible. Each entry contains an Ethernet station MAC address and the MAC address of the wireless device used to connect it to the wireless network	
MptEthernetStationMACAddress (*MacPinpointEntry 1)	Applicable to AU/BU only. Read only. The MAC address of the Ethernet station. It is used as an index in the MAC Pinpoint Table.	MAC address
MptUnitMACAddress (*MacPinpointEntry 2)	Applicable to AU/BU only. Read only. The MAC address of the wireless device used by the station with the MAC Address from the index in order to access the wireless network	MAC address

E.3 Supported Traps

NOTE



An * is used instead of the brzaccVL prefix.

E.3.1 Trap Variables

MIB Parameter	Description	Value/Range
*Traps (breezeAccessVLMib 14)		
*TrapSUMacAddr (*Traps 3)	Applicable to AU/BU. An SU/RB MAC address.	MAC address
*TrapText (*Traps 3)	Applicable to all units. Textual string for future use.	DisplayString
*TrapToggle (*Traps 4)	Applicable to all units. An On/Off toggle status.	Integer on (1) off (2)
*TrapParameterChanged (*Traps 5)	Applicable to all units. A modification to one of the parameters related to IP Filtering, MIR/CIR or VLAN.	Integer cirOrMir (1) ipFilter (2) vlan (3)
*TrapAccessRights (*Traps 6)	Applicable to all units. The access rights used for login.	Integer notLoggedIn (1) readOnly (2) installer (3) administrator (4) factory (5)
*TrapLog (*Traps 7)	Applicable to all units. Login or logout to the Monitor program Telnet.	Integer telnetLogin (1) telnetLogout (2)
*TrapTelnetUserIpAddress (*Traps 8)	Applicable to all units. The IP address of a Telnet user.	IP address
*TrapRTx (*Traps 9)	Applicable to AU/BU. Retransmissions rate.	
*TrapFtpOrTftpStatus (*Traps 10)	Applicable to all units. The status of the last FTP/TFTP loading process.	successful (1) failed (2)
*TrapDFSMoveFreq (*Traps 11)	Applicable to AU/BU with HW revision B and lower (for units with HW revision C and higher replaced by *TrapDFSMoveFreq New to support a resolution of 0.5 MHz). The new frequency in MHz after detecting radar on a previous channel.	Integer

MIB Parameter	Description	Value/Range
*TrapDFSMoveFreqNew (*Traps 12)	Applicable to AU/BU. The new frequency in MHz after detecting radar on a previous channel. (Replaces *TrapDFSMoveFreq to support a resolution of 0.5 MHz for units with HW revision C and higher).	DisplayString
*EthBroadcastThresholdExceeded (*Traps 13)	Applicable to all units. The number of packets that were dropped by the Ethernet broadcast/multicast limiter.	Integer
*TrapSubscriberType (*trap 14)	Applicable to AUS only. The type of subscriber that was rejected by the AUS (AUS can serve up to SUs. Only SU-3 and SU-6 are supported).	Integer unknownSubscriberType(0), su-3(3) su-6(6), rb-14(14), su-24(24), rb-28(28), su-54(54)

E.3.2 Private Traps

Trap (Number)	Description	Variables
*SUassociatedAUTRAP (2)	An AU/BU trap indicating a new association with an SU/RB.	*TrapSUMacAddr
*AUdisassociatedTRAP (3)	An AU/BU trap indicating that an SU/RB has been disassociated from the AU/BU. The AU/BU decides that an SU/RB has been disassociated from it and remove it from the ADB after receiving from another AU/BU a SNAP frame with the SU/RB MAC address. The SNAP frame indicating a network topology change where the SU/RB has associated with another AU/BU will be received if both AUs/BUs are connected to the same Ethernet backbone.	*TrapSUMacAddr

Trap (Number)	Description	Variables
*AUagingTRAP (4)	An AU/BU trap indicating that an SU/RB aged out and was removed from the Associations database following its failure to acknowledge a specified number of consecutive frames.	*TrapSUMacAddr
*SUassociatedTRAP (6)	An SU/RB trap indicating association with an AU/BU. In addition to the MAC address information of the AU/BU, the trap also includes information on the average SNR of frames received from the AU/BU.	*AssociatedAU
*AUwirelessQualityTRAP (20)	An AU/BU trap, indicating that the quality of the wireless link has changed and dropped below (Off) or increased above (On) a threshold defined by the *WirelessTrapThreshold.	*TrapToggle *TrapRTx
*PowerUpFromReset (101)	An AU/BU trap indicating power up after reset.	*UnitMacAddress
*MonitorStatusTRAP (102)	Applicable to all units. A trap indicating that a log-in or log-out has been performed via Telnet. Includes the login access right and the IP address of the PC performing Telnet.	*TrapLog *TrapAccessRights *TrapTelnetUserIpAddress
*ParameterChangedTRAP(103)	Applicable to all units. A trap indicating a change in CIR/MIR, IP Filter or VLAN parameter.	*TrapParameterChanged
*LoadingStatusTRAP(104)	Applicable to all units. A trap indicating the results (successful or failed) of the last FTP/TFTP loading process.	*TrapFtpOrTftpStatus *UnitMacAddress
*PromiscuousModeTRAP (105)	An AU/BU trap indicating that promiscuous mode was enabled (on) or disabled (off)	*TrapToggle *UnitMacAddress
*DFSRadarDetectedTRAP (106)	An AU/BU trap indicating that radar was detected	*UnitMacAddress
*DFSFrequencyTRAP (107)	An AU/BU trap indicating the new frequency after radar was detected.	*UnitMacAddress *TrapDFSMoveFreq

Trap (Number)	Description	Variables
*DFSNoFreeChannelsExistTRAP (108)	An AU/BU trap indicating that radar was detected and there is no free channel.	*UnitMacAddress
*EthBroadcastMulticatLimiterTRAP (109)	Applicable for all units. The trap is send if the Ethernet broadcast filter threshold is exceeded and it contains the number of packets that were dropped since the last trap.	*UnitMacAddress *EthBroadcastThresholdExceeded
*USUnsupportedSubscriberTypeTRAP (110)	Applicable to AUS only. This trap is generated when a subscriber unit that is not supportedt tries to associate with the AUS. The AUS supports only up to 5 SU-3 and/or SU-6 units.	*TrapSUMacAddr *TrapSubscriberType

Appendix F - 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.

F.1 Unit Control Parameters

Parameter	Unit	Range	Default	Run-Time
Change Unit Name	AU, SU	Up to 32 printable ASCII characters	None	Yes
Change Read Only Password	AU, SU	Up to 8 printable ASCII characters	public	No
Change Installer Password	AU, SU	Up to 8 printable ASCII characters	user	No
Change Administrator Password	AU, SU	Up to 8 printable ASCII characters	private	No
FTP SW Version File Name	AU, SU	Up to 20 printable ASCII characters. An empty string is not allowed.	VxWorks.bz	Yes
Configuration File Name	AU, SU	Up to 20 printable ASCII characters. An empty string is not allowed.	config.cfg	Yes
Operator Defaults File Name	AU, SU	Up to 20 printable ASCII characters. An empty string is not allowed.	operator.cmr	Yes
FTP Source Dir	AU, SU	Up to 80 printable ASCII characters. Use "." to clear.	None (empty)	Yes
FTP Client IP Address	AU, SU	IP address	1.1.1.3	No
FTP Client IP Mask	AU, SU	IP address	255.255.255.0	No
FTP Server IP Address	AU, SU	IP address	1.1.1.4	No
FTP Gateway IP Address	AU, SU	IP address	0.0.0.0	No
FTP User Name	AU, SU	Up to 18 printable ASCII characters	vx	No
FTP Password	AU, SU	Up to 18 printable ASCII characters	Vx	No
FTP Log File Name	AU, SU	Up to 20 printable ASCII characters	logfile.log	Yes
FTP Log File Destination Directory	AU, SU	Up to 80 printable ASCII characters. Use "." to clear.	None (empty)	Yes
Event Log Policy	AU, SU	<ul style="list-style-type: none"> ■ Message ■ Warning ■ Error ■ Fatal ■ Log None 	Warning	Yes
Log Out Timer	AU, SU	1-999 minutes	5	Yes

Parameter	Unit	Range	Default	Run-Time
Ethernet Port Negotiation Mode	AU, SU	<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	AU, SU	Up to 34 printable ASCII characters	None	Yes
Manual Feature Upgrade	AU, SU	License string: 32 to 64 hexadecimal digits	None	No

F.2 IP Parameters

Parameter	Unit	Range	Default	Run-Time
IP Address	AU, SU	IP address	10.0.0.1	No
Subnet Mask	AU, SU	IP address	255.0.0.0	No
Default Gateway Address	AU, SU	IP address	0.0.0.0	No
DHCP Option	AU, SU	<ul style="list-style-type: none"> ■ Disable ■ DHCP Only ■ Automatic 	Disable	No
Access to DHCP	AU, SU	<ul style="list-style-type: none"> ■ From Wireless Only ■ From Ethernet Only ■ From Both Wireless and Ethernet 	AU: From Ethernet Only SU: From Wireless Only	No

F.3 Air Interface Parameters

Parameter	Unit	Range	Default	Run-Time
ESSID	AU, SU	Up to 31 printable ASCII characters	ESSID1	No
Operator ESSID Option	AU	<ul style="list-style-type: none"> ■ Disable ■ Enable 	Enable	No
Operator ESSID	AU	Up to 31 printable ASCII characters	ESSID1	No
Best AU Support	SU	<ul style="list-style-type: none"> ■ Disable ■ Enable 	Disable	No
Number of Scanning Attempts	SU	1 – 255	4	No
Preferred AU MAC Address	SU	MAC Address	00-00-00-00-00-00 (no preferred AU)	Yes
Scanning Mode	SU	Passive, Active	Passive	No
Cell Distance Mode	AU	Automatic, Manual	Automatic	No
Maximum Cell Distance	AU	0-54 (Km) 0 means no compensation	0 (no compensation)	Yes
Fairness Factor	AU	0 – 100 (%)	100 (%)	No
Arbitration Inter-Frame Spacing	AU, SU	<ul style="list-style-type: none"> ■ 1 time slot ■ 2 time slots 	2 time slots	Yes
Wireless Trap Threshold	AU	1-100 (%)	30 (%)	Yes
Maximum Number of Associations	AU	1-512 (1-124 if Data Encryption Option is enabled).	512	Yes
Sub-Band Select*	AU, SU	1, 2	1	No
Frequency	AU	4947.5 - 4982.5 MHz, 5MHz steps	4947.5 MHz	No
Frequency Subset Definition (in SU)	SU	According to the Sub-Band. A list of frequency indexes or A for all frequencies supported by the Sub-Band	A (All)	No
Country Code Learning by SU	AU	<ul style="list-style-type: none"> ■ Disable ■ Enable 	Enable	Yes
Tx Power For Modulation Levels 1 to 5	AU, SU	-10 dBm to a value determined by Sub-Band	The highest allowed value	Yes
Tx Power For Modulation Level 6	AU, SU	-10 dBm to a value determined by the Sub-Band.	The highest allowed value	Yes
Tx Power For Modulation Level 7	AU, SU	-10 dBm to a value determined by the Sub-Band	The highest allowed value	Yes

Parameter	Unit	Range	Default	Run-Time
Tx Power For Modulation Level 8	AU, SU	-10 dBm to a value determined by the Sub-Band	The highest allowed value	Yes
Max Tx Power For Modulation Levels 1 to 5	SU	-10 dBm to a value determined by the Sub-Band	The highest allowed value	Yes
Max Tx Power For Modulation Level 6	SU	-10 dBm to a value determined by the Sub-Band	The highest allowed value	Yes
Max Tx Power For Modulation Level 7	SU	-10 dBm to a value determined by the Sub-Band	The highest allowed value	Yes
Max Tx Power For Modulation Level 8	SU	-10 dBm to a value determined by the Sub-Band	The highest allowed value	Yes
ATPC Option	AU, SU	<input type="checkbox"/> Disable <input type="checkbox"/> Enable	Enable	Yes
Delta from Minimum SNR Level	AU	4-20 (dB)	11 dB	Yes
Minimum SNR Level	AU	4-60 (dB)	28 (dB)	Yes
Minimum Interval Between ATPC Messages	AU	1-3600 (seconds)	30 (seconds)	Yes
ATPC Power Level Steps	AU	1-20 (dB)	4	Yes
Tx Control	AU	<input type="checkbox"/> Off <input type="checkbox"/> On	On	Yes (unit is reset automatically)
Antenna Gain	AU, SU***	0 – 50 (dB)	AU: According to the antenna supplied with the unit. SU-E: NA	No
Spectrum Analysis Channel Scan Period	AU, SU	2 – 30 seconds	5 seconds	No
Spectrum Analysis Scan Cycles	AU, SU	1 – 100 cycles	2 cycles	No
Automatic Channel Selection	AU	<input type="checkbox"/> Disable <input type="checkbox"/> Enable	Disable	No (Configured per analysis)
Lost Beacons Watchdog Threshold	AU	100 – 1000, 0 means Not Used	218	Yes

*** Configurable only in units without an integral antenna.

F.4 Network Management Parameters

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

F.5 Bridge Parameters

Parameter	Unit	Range	Default	Run-Time
VLAN ID-Data	SU	1 – 4094	1	No
VLAN ID – Management	AU, SU	1 – 4094, 65535	65535 (no VLAN)	No
VLAN Link Type	AU, SU	<ul style="list-style-type: none"> ■ Hybrid Link ■ Trunk Link ■ Access Link (only in SU) 	Hybrid Link	No
VLAN Forwarding Support	AU, SU	Disable, Enable	Disable	No
VLAN Forwarding ID	AU, SU	1 – 4094 (up to 20 entries)	Empty list	No
VLAN Relaying Support	AU	Disable, Enable	Disable	No
VLAN Relaying ID	AU	1 – 4094 (up to 20 entries)	Empty list	No
VLAN Priority – Data	SU	0 – 7	0	No
VLAN Priority – Management	AU, SU	0 – 7	0	No
Ethernet Broadcast Filtering Options	SU	<ul style="list-style-type: none"> ■ Disable, ■ On Ethernet Port Only ■ On Wireless Port Only ■ On Both Wireless and Ethernet Ports 	Disable	Yes
DHCP Broadcast Override Filter	SU	<ul style="list-style-type: none"> ■ Disable ■ Enable 	Disable	Yes
PPPoE Broadcast Override Filter	SU	<ul style="list-style-type: none"> ■ Disable ■ Enable 	Disable	Yes
ARP Broadcast Override Filter	SU	<ul style="list-style-type: none"> ■ Disable ■ Enable 	Enable	Yes
Ethernet Broadcast/Multicast Limiter Option	AU, SU	<ul style="list-style-type: none"> ■ Disable ■ Limit only Broadcast Packets ■ Limit Multicast Packets that are not Broadcasts ■ Limit All Multicast Packets (including broadcast) 	Disable	Yes
Ethernet Broadcast/Multicast Limiter Threshold	AU, SU	0 – 204800 (packets/second)	50	Yes

Parameter	Unit	Range	Default	Run-Time
Ethernet Broadcast/Multicast Limiter Send Trap Interval	AU, SU	1 – 60 (minutes)	5 (minutes)	Yes
Bridge Aging Time	AU, SU	20 – 2000 seconds	300	No
Broadcast Relaying	AU	Disable, Enable	Enable	No
Unicast Relaying	AU	<input type="checkbox"/> Disable <input type="checkbox"/> Enable	Enable	No
MAC Address Deny List	AU	Up to 100 MAC addresses	None (empty)	Yes
Roaming Option	SU	<input type="checkbox"/> Disable <input type="checkbox"/> Enable	Disable	No
Ethernet Port Control	SU	<input type="checkbox"/> Disable <input type="checkbox"/> Enable	Enable	Yes

F.6 Performance Parameters

Parameter	Unit	Range	Default	Run-Time
RTS Threshold	AU, SU	20 – 4032 (bytes)	AU: 4032 SU: 60	Yes
Minimum Contention Window	AU, SU	0, 7, 15, 31, 63, 127, 255, 511, 1023	15	Yes
Maximum Contention Window	AU, SU	7, 15, 31, 63, 127, 255, 511, 1023	1023	Yes
Maximum Modulation Level	AU, SU	1 - 8	8	Yes
Multicast Modulation Level	AU	1 - 8	1	Yes
Number of HW Retries	AU, SU	1 - 15	10	Yes
Average SNR Memory Factor	AU, SU	-1 to 32	5	Yes
Burst Mode Option	AU, SU	<ul style="list-style-type: none"> ■ Disable ■ Enable 	Enable	No
Burst Mode Time Interval	AU, SU	1 to 10 (milliseconds)	5 milliseconds	Yes
Adaptive Modulation Option	AU, SU	<ul style="list-style-type: none"> ■ Disable ■ Enable 	Enable	No
Minimum Interval Between Adaptive Modulation Messages	AU, SU	1-3600 (seconds)	4 (seconds)	Yes
Adaptive Modulation Decision Threshold	AU, SU	<ul style="list-style-type: none"> ■ Normal ■ High 	Normal	No
Concatenation Option	AU, SU	<ul style="list-style-type: none"> ■ Disable ■ Enable 	Enable	No
Maximum Number of Frames	AU, SU	2 – 8 frames	8	No

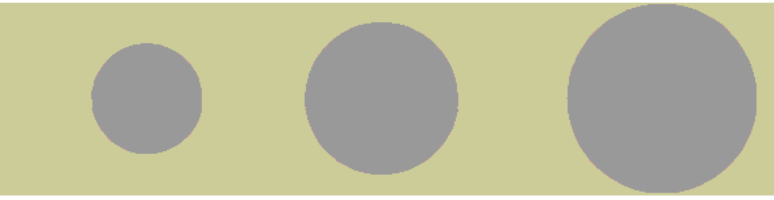
F.7 Service Parameters

Parameter	Unit	Range	Default	Run-Time
User Filtering Option	SU	<ul style="list-style-type: none"> ■ Disable ■ IP Protocol Only ■ User Defined Addresses Only ■ PPPoE Protocol Only 	Disable	Yes
Set/Change Filter IP Address Ranges	SU	<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	SU	<ul style="list-style-type: none"> ■ Disable DHCP Unicast ■ Enable DHCP Unicast 	Disable DHCP Unicast	Yes
MIR: Downlink	SU	128-53888 (Kbps)	53888 (Kbps)	No
MIR: Uplink	SU	128-53888 (Kbps)	53888 (Kbps)	No
CIR: Downlink	SU	0-45056 (Kbps)	0 (Kbps)	No
CIR: Uplink	SU	0-45056 (Kbps)	0 (Kbps)	No
Maximum Delay	SU	300 – 10,000 (ms)	5,000 (ms)	No
Maximum Burst Duration	AU, SU	0 – 2,000 (ms)	5 (ms)	No
Graceful Degradation Limit	AU	0 – 70 (%)	70 (%)	No
MIR Only Option	AU	<ul style="list-style-type: none"> ■ Disable ■ Enable 	Enable	No
VLAN Priority Threshold	AU, SU	0 – 7	7	No
ToS Prioritization Option	AU, SU	<ul style="list-style-type: none"> ■ Disable ■ Enable IP Precedence (RFC791) Prioritization ■ Enable DSCP (RFC2474) Prioritization 	Disable	No
IP Precedence Threshold	AU, SU	0 – 7	7	No
DSCP Threshold	AU, SU	0 – 63	63	No
UDP/TCP Port Ranges Prioritization Option	AU, SU	<ul style="list-style-type: none"> ■ Disable ■ Enable Only for UDP ■ Enable Only for TCP ■ Enable for both UDP and TCP 	Disable	No

Parameter	Unit	Range	Default	Run-Time
UDP RTP/RTCP Prioritization	AU, SU	<ul style="list-style-type: none"> ■ RTP & RTCP ■ RTP Only 	RTP & RTCP	No
TCP RTP/RTCP Prioritization	AU, SU	<ul style="list-style-type: none"> ■ RTP & RTCP ■ RTP Only 	RTP & RTCP	No

F.8 Security Parameters

Parameter	Unit	Range	Default	Run-Time
Authentication Algorithm*	AU, SU	<ul style="list-style-type: none"> ■ Open system ■ Shared Key 	Open system	No
Data Encryption Option*	AU, SU	<ul style="list-style-type: none"> ■ Disable ■ Enable 	Disable	No
Security Mode*	AU, SU	<ul style="list-style-type: none"> ■ WEP ■ AES/OCB ■ AES/CCM 	WEP	No
Default Key	SU	1-4	1	No
Default Multicast Key	AU	1-4	1	No
Key # 1 to Key # 4	AU, SU	32 hexadecimal digits	0...0 (all 0=no key)	No
Promiscuous Authentication	AU	<ul style="list-style-type: none"> ■ Disable ■ Enable 	Disable	Yes (Disable after reset)



G

Appendix G - Using the Feature License Web Application



G.1 The Feature License Web Application

Certain features of BreezeACCESS 4900 products may be upgraded through loading special feature license strings. When you receive the invoice for new license(s) purchased, use the Alvarion web site for getting license strings for specific products.



To access the Feature License Application:

- 1 In the Alvarion web site (www.alvarion.com), select the Customer Service option.
- 2 In the Customer Service page, select the Service Call Entry option.
- 3 In the User Login form, enter your User ID and Password and click Login.
- 4 Select SSM - Customer Service Area.
- 5 Select the Feature License option.

The Get Feature License Key form with the current status of your license(s) is displayed.

Check*	Order	Order Line	Invoice	Product Line	Feature	Qty Ordered	Qty Available
<input type="checkbox"/>		0		BreezeACCESS VL	SU 24Mb to 54Mb	1000	1000
<input type="checkbox"/>		0		BreezeACCESS VL	SU 6Mb to 54Mb	20	20
<input type="checkbox"/>		0		BreezeNET B	Upg BU-B14 to BU-B28	10	10
<input type="checkbox"/>		0		BreezeNET B	Upg RB-B14 to RB-B28	10	10



To get details on the updated status of your licenses:

Check on the License Key Enquiry button to get the updated status of the licenses.

The displayed information includes account history with details on all license strings that were provided.



To get a License Key for a single device:

- 1 Check the required feature license entry and click on the Get Key button. The Enter MAC Address form will be displayed:

- 2 Enter the MAC Address of the device you want to upgrade.
- 3 Click on the Get Key button. The License Key for the device will be displayed.

NOTE



An error message will be displayed upon requesting a key for a non-valid MAC address.



To get License Keys for multiple devices:

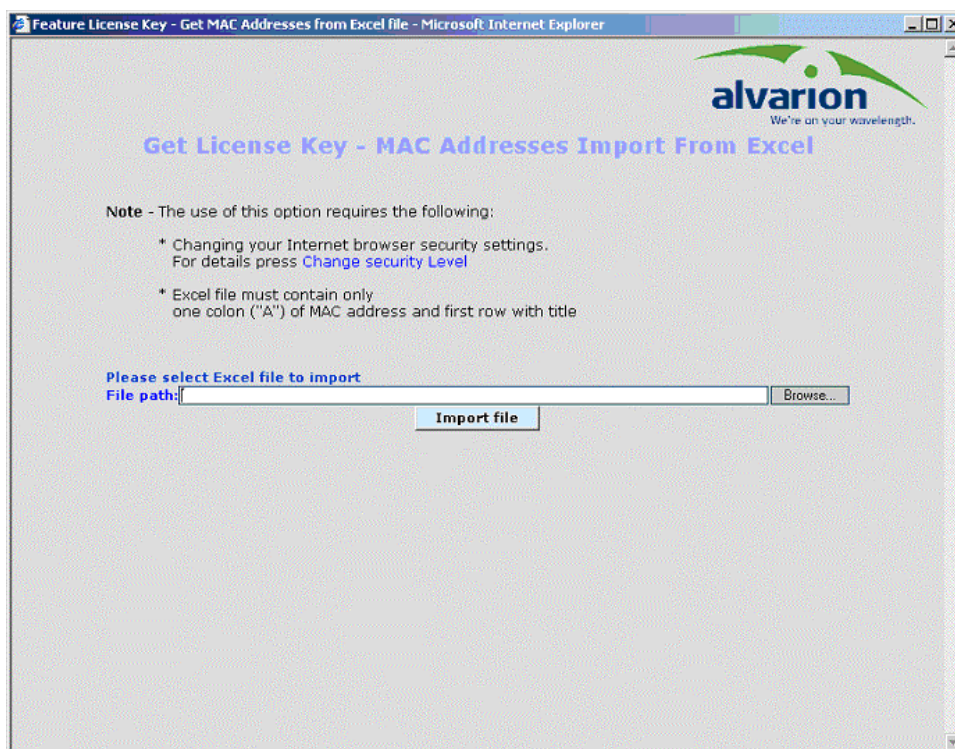
This feature enables you to load a list of MAC Addresses from a pre-prepared Excel file.

NOTE



The Excel file should contain a single column of MAC addresses (no empty cells). This must be column A, starting at row 1, which is the title row.

- 1 Check the required feature license and click on Upload MAC Address List from Excel button. The Get MAC Addresses from Excel File form will be displayed:



NOTE



You may need to change your Browser security settings. For details press the Change Security Level link in the form.

- 2 Use the browser or enter the path to the MAC addresses file. Enter the MAC address of the device you want to upgrade.
- 3 Click on the Import File button to get a list of License Keys for the devices included in the Excel file.

NOTE



An error message will be displayed upon requesting a key for a non-valid MAC address.

G.1.1 Loading License Strings to Devices



To upgrade a single device:

There are several methods of loading a feature license string to a single device:

- **Using Telnet:** Use the Feature Upgrade option in the Unit Control menu.
- **Using TFTP:** Use the file with the extension “.fln” for feature license strings. Refer to [Appendix B](#) (File Upload and Download Using TFTP) for more details.

- **Using BreezeCONFIG:** Enter the license string in the Feature Upgrade field of the Unit Control window. Refer to the *BreezeCONFIG User Manual* for more details.



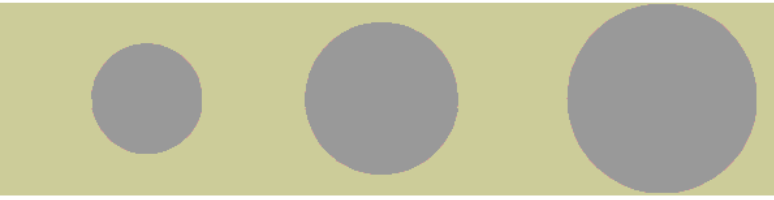
To upgrade multiple devices using a feature licenses file:

- **Using TFTP:** Use the file with the extension “.fln” for feature license strings. Refer to [Appendix B](#) (File Upload and Download Using TFTP) for more details. Note that Feature license files include multiple strings, where each string is applicable only for a certain unit identified by its MAC address. When uploading a feature license or a country code file to multiple units, each unit will accept only the parts that are applicable for it.
- **Using BreezeCONFIG:** Use the File Loading Utility. Refer to the *BreezeCONFIG User Manual* for more details.

NOTE



After completing loading process, reset the unit(s) to apply the change. Use the Info Screens menu (Show Unit Status) to verify that the unit has been upgraded.



H

Appendix H - Troubleshooting



H.1 Ethernet Port Connection Problems

Problem and Indication	Possible Cause	Corrective Action
The Ethernet Integrity Indicator (the yellow LED embedded in the Ethernet connector) is off, and/or the Ethernet Activity Indicator (the green embedded LED) does not blink when there should be traffic on the Ethernet port.	Wrong type of Ethernet cable	If connected directly to PC-use a crossed cable. Otherwise-use a straight cable
	Faulty Ethernet cable	Replace cable
The unit does not respond to ping.	Wrong IP configuration	Make sure that the PC is on the same subnet as the unit*.
	Wrong Ethernet port operation mode	Make sure that the speed and duplex settings in the PC match the configuration in the unit (the default is Auto Negotiation)

* If the IP parameters of the unit are unknown, use the Set Factory Defaults utility to restore the default factory configuration of all parameters (except to Passwords, general FTP parameters and AU's Frequency). The IP address of the unit after setting to factory defaults is 10.0.0.1.

H.2 SU Association Problems

Problem and Indication	Possible Cause	Corrective Action
SU does not associate with AU	Wrong configuration	Check proper configuration of basic parameters: <ul style="list-style-type: none"> ■ ESSID ■ Sub-band and frequencies subset ■ Best AU parameters ■ ATPC Option ■ Transmit Power ■ Maximum Transmit Power ■ Antenna Gain ■ Security parameters: Authentication Algorithm, and Default Key. If necessary-use Promiscuous Mode in AU.
	Access is denied by AU	Verify that the SU is not included in MAC Address Deny List of the AU.
	Link quality is too low	<ul style="list-style-type: none"> ■ Verify that unit is in coverage area of AU according to radio planning. ■ Verify that antenna is directed toward the AU ■ Try to improve location/height of antenna.

H.3 Low Throughput Problems

Problem and Indication	Possible Cause	Corrective Action
Low throughput is suspected (Check the dominant Modulation Level in Per rate Counters and see expected throughput in the “Expected Throughput” table below)	Ethernet link problems	<ul style="list-style-type: none"> ■ Verify proper settings of Ethernet operation mode (actual Ethernet speed of 100 Mbps). ■ Check Ethernet counters
	Wrong configuration of Maximum Modulation level	Verify that Maximum Modulation level is not set to a value that is not too low according to the “Recommended Maximum Modulation Level” table below.
Low throughput of multicast/broadcast traffic	Non-optimal configuration of Multicast Modulation level	A value that is too low (see the “Recommended Maximum Modulation Level” table below) may degrade throughput of broadcast and multicast traffic.
High retransmissions rate	Interference problems (retransmissions rate in excess of 15%)	Check for interference using the Spectrum Analysis Mode. If necessary, change the operating frequency of the AU.

Expected Throughput in Mbps, TCP session, Burst Mode Disabled	
Modulation Level	Expected Throughput (Mbps) @ 10 MHz Bandwidth
1	2.40
2	3.57
3	4.69
4	6.76
5	8.76
6	12.02
7	14.13
8	14.25

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