BreezeACCESS™ 900

System Manual

SW Version 4.5
April 2004
P/N 213773

Legal Rights

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

Trade Names

Alvarion, BreezeCOM, WALKair, WALKnet, BreezeNET, BreezeMANAGE, BreezeACCESS, BreezeLINK, BreezePHONE, MGW, eMGW and/or other products and/or services referenced here in are either registered trademarks, trademarks or service marks of Alvarion.
All other names are or may be the trademarks of their respective owners.
The content herein is subject to change without further notice.

Statement of Conditions

The information contained in this manual is subject to change without notice. Alvarion 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 products purchased from Alvarion or through any of Alvarion's authorized resellers are subject to the following warranty and product liability terms and conditions.

Exclusive Warranty

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

Disclaimer

(a) UNITS OF PRODUCT (INCLUDING ALL THE SOFTWARE) DELIVERED TO PURCHASER HEREUNDER ARE NOT FAULT□TOLERANT AND ARE NOT DESIGNED, MANUFACTURED OR INTENDED FOR USE OR RESALE IN APPLICATIONS WHERE THE FAILURE, MALFUNCTION OR INACCURACY OF PRODUCTS CARRIES A RISK OF DEATH OR BODILY INJURY OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE ("HIGH RISK ACTIVITIES"). HIGH RISK ACTIVITIES MAY INCLUDE, BUT ARE NOT LIMITED TO, USE AS PART OF ON□LINE CONTROL SYSTEMS IN HAZARDOUS ENVIRONMENTS REQUIRING FAIL-SAFE PERFORMANCE, SUCH AS IN THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, AIR TRAFFIC CONTROL, LIFE SUPPORT MACHINES, WEAPONS SYSTEMS OR OTHER APPLICATIONS REPRESENTING A SIMILAR DEGREE OF POTENTIAL HAZARD. ALVARION SPECIFICALLY DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY OF FITNESS FOR HIGH RISK ACTIVITIES.

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

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

Limitation of Liability

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

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

Electronic Emission Notices

This device complies with Part 15 of the FCC rules.

Operation is subject to the following two conditions:

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

FCC Radio Frequency Interference Statement

The Access Unit 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. 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.

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. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential environment notwithstanding use in commercial, business and industrial environments. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

FCC Radiation Hazard Warning

To comply with FCC RF exposure requirement in section 1.1307 of the FCC rules, the antenna used for this transmitter (AU and SU-I) must be fixed-mounted on an outdoor permanent structure with a separation distance of at least 2 meters (79 inches) from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

Safety Considerations

For the following safety considerations, "Instrument" means the BreezeACCESS 900 units' components and their cables.

Caution

To avoid electrical shock, do not open any of the instrument components and do not perform any servicing unless you are qualified to do so. Power connections should be made only by a licensed electrician.

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.

Installation Codes

The system must be installed according to country national electrical codes. For North America, equipment must be installed in accordance to the US National Electrical Code (NEC) Articles 110-16, 110-17 and 110-18 and the Canadian Electrical Code (CEC), Sections 2__-202 and 2-308. Wiring methods are to be in accordance to NEC Article 300 and CEC Section 12.

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 Units and Antennas Installation and Grounding

Be sure that the outdoor unit, the antennas and the supporting structures are properly installed to eliminate any physical hazard to either people or property. Verify that the outdoor units and the antenna masts are grounded so as to provide protection against voltage surges and static charges. Make sure that the installation of the outdoor units, antennas, supporting structures and cables is performed in accordance with all relevant national and local building and safety codes.

Important Notice

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

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

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

About this Guide

This manual describes the BreezeACCESS 900 Broadband Wireless Access System Release 4.5 and how to install, initialize and operate the system components.

This guide is intended for technicians responsible for installing, setting up and operating the BreezeACCESS 900 system.

This guide contains the following chapters and appendices:

- **Chapter 1** – **System description:** Describes the BreezeAccess 900 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 antennas and validate unit operation.
- **Appendix A** –**Mounting the Subscriber's Antenna**: Describes how to install the Subscriber's antenna.
- **Appendix B – SU-I Lightning and Grounding Kit Installation**: Describes how to install and connect the lightning protection and grounding for the Subscriber's antenna.
- **Appendix C – Parameters Summary:** Provides a summary of all configurable parameters, including available values, default value and whether the parameter is configurable in run-time or only after reset.
- **Appendix D** – **RSSI to dBm Conversion:** provides conversion table between RSSI arbitrary units used in the system and dBm.
- **Appendix E** – **Configuration File Download and Upload:** Describes the procedure for configuration file download/upload using TFTP.
- **Appendix F** – **Software Version Loading Procedure:** Describes the procedure for loading new SW versions using TFTP.

This page left intentionally blank.

Contents

Figures

Tables

This page left intentionally blank.

1

Chapter 1 - System Description

In this Chapter

Introducing BreezeACCESS 900

BreezeACCESS 900 system allows operators that provide IP services to extend the reach of their system and provide services to clusters of customers that cannot otherwise be reached due to being obstructed by heavy foliage or other obstacles. Operators can benefit from the advantage of operating locally in the 900 MHz band, being able to provide services to customers within an average radius of up to two miles in non line of sight environments with heavy foliage and other obstacles.

BreezeACCESS 900 system includes the following components:

- **Stand-Alone Access Unit (AU):** Provides all the functionality necessary to communicate with the Subscriber Units and to connect to the backbone of the Service Provider.
- **Modular Base Station Equipment:** Provides cost-effective solution for multiple collocated access units.
- **Subscriber Units (CPE):** provide the customer's data connection to the Access Unit, supporting high speed Internet and Intranet services.

Alvarion also provides Cell Extender (CX) equipment, providing an interface with repeater functionality between the local system operating in the 900 MHz band and a primary broadband wireless access system operating in either the 2.4 GHz or the 5.8 GHz band. For more details on the Cell extender, refer to the BreezeACCESS Cell Extender User's Guide.

ATTENTION

Alvarion also offers to its customers a special spectrum sweep and analysis tool to enable optimal selection of frequencies and antenna polarization. This tool is particularly important in the heavily crowded 900 MHz band and it is recommend for use before deployment of the subscriber units. For information on the spectrum sweep and analysis tool, refer to the Breeze Access Spectrum Sweep & Analysis Utility User's Guide (www.alvarion-usa.com).

Stand-Alone Access Unit

The Access Unit (AU) provides all the functionality necessary to communicate with the remote Subscriber Units as well as to connect to the backbone of the service provider.

The AU-E-NI Access Unit is comprised of an AU-NI indoor unit, and a 900 MHz outdoor radio unit that connects to an antenna. The AU-NI is a desktop or wall-mountable unit that is powered from the mains (100-250 VAC) through an external power transformer and connects to the network through a standard IEEE 802.3 Ethernet 10BaseT (RJ 45) interface.

A coaxial Intermediate Frequency (IF) cable connects between the AU-NI indoor unit and the outdoor unit. This cable carries 440 MHz IF signals, power (12 VDC) and management and control signals from the indoor unit to the outdoor unit.

Modular Base Station Equipment

The Base Station equipment is based on the BS-SH 3U chassis, which is suitable for installation in 19" racks. The chassis contains one or two power supply modules, up to six active Access Unit Network Interface (BS-AU) modules and an optional BS-GU GPS and Alarms module.

Two different types of power supply modules are available: the BS-PS that is powered from a –48 VDC power source, and the BS-PS-AC, powered from the 110/230 VAC mains. The optional use of two power supply modules is for fail-safe operation through power supply redundancy.

Each BS-AU module, together with its outdoor radio unit comprises an AU-E-BS Access Unit that serves a single sector. The AU-RE outdoor unit contains the radio module and a RF connector for a separate external antenna.

The BS-AU modules connect to the network through standard IEEE 802.3 Ethernet 10BaseT (RJ 45) interfaces. A coaxial Intermediate Frequency (IF) cable connects the indoor module to the outdoor unit. This cable carries 440 MHz IF signals, power (12 VDC) and management and control signals from the indoor unit to the outdoor unit.

GU-A-BS GPS and Alarms System

The optional GU-A-BS system can be used to synchronize the frequency hopping mechanisms of collocated AU-BS BreezeACCESS units (where such synchronization is permitted by local regulations) as well as to provide alarm management.

The GU-A-BS system is comprised of two units:

- An outdoor GPS Receiver and Antenna unit, the GU-RA.
- An indoor GPS and Alarms module, the BS-GU.

The BreezeACCESS BS-GU module is designed for insertion into the BS-SH 19" base station chassis to provide hopping synchronization signals to the BS-AU Access Unit modules. The card uses timing signals derived from signals received from the GU-RA GPS antenna. These signals, generated by the GPS global satellites network, allow accurate synchronization of systems located in different locations. Any number of base stations can be synchronized, guaranteeing that all AUs (Access Units) hop in unison from frequency to frequency. In addition, the GPS signal insures that all units begin their pre-defined hopping sequence at the same time.

The BS-GU module is connected to the GU-RA GPS antenna via a cable that carries power from the module to the antenna, timing signals from the antenna to the module and management signals between the two units.

The BS-GU also provides synchronization signals to other BS-GU modules by daisy-chaining any number of modules, allowing a single GU-RA GPS antenna to synchronize multiple AUs in several collocated BS-SH chassis.

When a GU-RA GPS antenna is not connected to the module (or if the connected GPS antenna is not functioning properly), the BS-GU module provides self-generated synchronization signals to all AUs.
Daisy-chained BS-GU modules use the synchronization signals generated by the first unit in the chain (the Master unit).

The BS-GU module also supports the management of alarm inputs and outputs. The module receives Alarms In indications from other BreezeACCESS modules in the base station shelf (internal alarms) and external alarms from other devices via the AL IN connector. Alarms Out management allows activation of external devices upon occurrence of user-defined events, using relays via the AL OUT connector.

Subscriber Unit

The Subscriber Unit (SU) installed at the customer premises enables the customer data connection to the Access Unit.

The Subscriber Unit provides an efficient platform for high speed Internet and Intranet services. 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 SU-I-1D-900 miniature Subscriber Unit is designed for desktop or wall-mount installation. It supports a single Ethernet device and connects to the customer's data equipment via a standard IEEE 802.3 10Base-T (RJ-45) interface. The unit is powered from the 110/220 VAC mains. It has one RF connector for an indoor or outdoor antenna.

BreezeCONFIG™ ACCESS

The BreezeCONFIG ACCESS utility is an SNMP-based application designed to manage BreezeACCESS system components and upgrade unit software versions. The system administrator can use the BreezeCONFIG ACCESS utility to control a large number of units from a single location. BreezeCONFIG ACCESS provides a single point of control for BreezeACCESS 900 system components as well as for devices belonging to other GFSK based BreezeACCESS families such as BreezeACCESS II. In addition, BreezeCONFIG ACCESS enables you to load an updated configuration file to multiple units simultaneously, thus radically reducing the time spent on unit configuration and maintenance.

Specifications

900 MHz Radio specifications

Table 1-1: 900 MHz Radio Specifications

Item	Description
Frequency	903 – 927 MHz ISM band
Operation Mode	Time Division Duplex (TDD)
Radio Access Method	FH-CDMA
Standard Compliance	FCC Part 15.247
Channel Bandwidth	2 MHz
Central Frequency Resolution	1 MHz
SU Antenna	■ 10 dBi, 55°x 65°, V/HPOL outdoor pole or wall mountable antenna ■ 7 dBi, 40°x 35°, V/HPOL indoor window or wall mountable antenna ■ Other: See 3rd Party Antenna List in Alvarion web site (www.alvarion-usa.com) for additional Alvarion certified antennas
AU Antenna	■ 10 dBi, 55° x 65°, Flat Panel (V/HPOL) pole or wall mountable antenna ■ Other: See 3rd Party Antenna List in Alvarion web site (www.alvarion-usa.com) for additional Alvarion certified antennas
Maximum Input Power (@ antenna port)	-20 dBm
Output Power (at antenna port)	SU: 24 dBm typical, control range 3 to 24 dBm in 1 dB steps AU: 23 dBm typical (min), 24.5 dBm max.
Gross Bit Rate	1, 2, 3 Mbps

Table 1-1: 900 MHz Radio Specifications			
Item	**Description**		
Sensitivity, typical (dBm at antenna port, BER 10E-6)	Gross Rate	SU Sensitivity	AU Sensitivity
	1 Mbps	-90 dBm	-91 dBm
	2 Mbps	-84 dBm	-85 dBm
	3 Mbps	-77 dBm	-78 dBm
Modulation	GFSK modulation, 2, 4 8 modulation states (1, 2, 3 bits/symbol)		
Symbol Rate	1 Msymbol/sec		

Data Communication

Table 1-2: 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 ToS according to RFC791

IF Communication Interface (AU)

Table 1-3: IF Communication Interface

Item	Description
IF Frequency	440 MHz
IF Cable Impedance	50 ohm
Maximum IF Cable Attenuation	15dB
Maximum IF Cable DC Resistance	1.5 ohm

GPS Radio

Table 1-4: GPS Radio Specifications

Item	Description
GPS Receiver	L1 frequency, C/A code (SPS) continuous tracking receiver
Update Rate	1 Hz

GPS GU-RA to BS-GU Communication

Table 1-5: GPS GU-RA to BS-GU Communication

Item	Description
Physical interface	RS 422
Cable Type	EIA RS 422 3 x 2 x 26AWG + 1 x 2 x 24 AWG FTP Shielded. 3 x 26 AWG twisted pairs for RS 422 communication and 1x 24 AWG pair for power supply
Cable Impedance	100 +/- 15 ohm @ 1 MHz (RS 422 pairs)
DC Resistance	■ RS 422 pairs: 145 ohm/km ■ Power supply pair: 94 ohm/km
Maximum Cable Length	120 meters

Configuration and Management

Table 1-6: Configuration and Management

Type	Standard
Management	■ Monitor program via Telnet ■ SNMP ■ Configuration upload/download using TFTP
Management Access	From Wired LAN, Wireless Link
Management access protection	■ Multilevel password ■ Configuration of remote access direction (from Ethernet only, from wireless link only or from both sides) ■ Configuration of IP addresses of authorized stations
SNMP Agents	SNMP ver 1 client MIB II, Bridge MIB, Private BreezeACCESS MIB
Security	■ Association protocol – ESSID ■ RC4 WEP option (encryption of the authentication process) ■ VLAN according to IEEE 802.1Q ■ d. IP level filtering for user addresses or protocols ■ Access direction and IP address filtering for management
Authentication and Accounting	RADIUS client in the SU according to RFC 2865 and 2866
Allocation of IP parameters	Configurable or automatic (DHCP client)
Software upgrade	TFTP

Standards Compliance, General

Table 1-7: Standards Compliance, General		
Type	**Standard**	
EMC	FCC Parts 15.207, 15.209	
Safety	IEC 60 950 US/C (TUV), FCC 1.1307	
Environmental	Operation	ETS 300 019 part 2-3 class 3.2E for indoor units ETS 300 019 part 2-4 class 4.1E for outdoor units
	Storage	ETS 300 019-2-1 class 1.2E
	Transportation	ETS 300 019-2-2 class 2.3
Lightning protection (AU IF and RF connections)	EN 61000-4-5, Class 3 (2kV)	
Radio	FCC part 15.247, 15.203	

Environmental

Table 1-8: Environmental Specifications		
Type	**Unit**	**Details**
Operating temperature	SU-RA, AU-RE	-40° C to 55° C (-40° F to 131° F)
	SU-I, AU-NI	0° C to 40° C (32° F to 104° F)
Operating humidity	Outdoor units	100% RH Condensing
	Indoor equipment	5%-95% non condensing

Physical and Electrical

Subscriber Unit

Mechanical

Table 1-9: Mechanical Specifications, Subscriber Unit

Unit	Structure	Dimensions (cm)	Weight (kg/lb)
General	An indoor SU-I unit and an outdoor antenna		
SU-I	Metal box, desktop or wall mountable	15 x 8.7 x 3.7	0.35 / 0.77
Power supply	Plugged directly into the mains socket (3 AC power pins), 1.5 meter DC cable with a right angle phone jack	7.5 x 3.1 x 5	0.38 / 0.84
Outdoor 10 dBi Antenna	Plastic radome with aluminum base plate, 1.5”-4” pole mountable	30.5 x 30.5 x1.5	1.5 / 3.3
Indoor 7 dBi Antenna	Plastic enclosure, window or wall mountable	18 x 18 x x 3.1	

Electrical

Table 1-10: Electrical Specifications, Subscriber Unit

Unit	Details
General	External power supply AC input power: 100-240 Vr.m.s.,47-63 Hz DC power output: 5.1V, 2A max.

Connectors

Table 1-11: Connectors, Subscriber Unit

Unit	Connector	Description
SU-I	ETH	10BaseT Ethernet (RJ-45) with 2 embedded LEDs. Cable connection to a PC: Straight
	Port 2 (antenna)	Custom SMA jack, 50 ohm
	Monitor	3-pin low profile
	AC IN	Standard DC 2.5 mm jack to external power supply
Indoor 7dBi Antenna	Antenna	Custom SMA Jack, 50 ohm on a 10ft. LMR-195 cable
Outdoor 10dBi Antenna	Antenna	N-Type jack, 50 ohm

Stand-Alone AU

Mechanical

Table 1-12: Mechanical Specifications, Stand-Alone AU

Unit	Structure	Dimensions (cm)	Weight (kg/lb)
General	An indoor AU-NI unit with an external AU-PS power supply unit and an outdoor AU-RE radio unit		
AU-NI	Metal box, desktop or wall mountable	15 x 8.7 x 3.7	0.34 / 0.75
Power supply	Desktop unit with a 1.5 meter DC cable	12 x 6 x 3.6	0.28 / 0.62
AU-RE-900	Metal box, 2”-3” pole mountable	30.6 x 12 x 4.7	1.6 / 3.5
900 MHz antenna, 10 dBi, 65^{o} x 65^{o}, Flat Panel (H/V)	Plastic radome with aluminum base plate, 1.5”-4” pole mountable	30.5 x 30.5 x 1.5	1.5 / 3.3
900 MHz antenna, 12 dBi, 120^{o} x 11^{o}, Dual Polarity (H/V)	Plastic radome with aluminum base plate, 1.5”-4” pole mountable	120 x 16 x 8	6.1 / 13.5

Connectors

Table 1-13: Connectors, Stand-Alone AU

Unit	Connector	Description
AU-NI	IF	TNC female jack, lightning protected
	ETHERNET	10BaseT Ethernet (RJ-45) with 2 embedded LEDs. Cable connection to a PC: crossed
	DC-12 V	Standard DC 2.5 mm jack to external power supply
	Monitor	3-pin low profile
AU-RE	ANT	N-Type female jack
	IF	TNC jack, lightning protected
900 MHz antenna, 10 dBi, 65^{o} x 65^{o}, Flat Panel (H/V)	RF	N-Type jack
900 MHz antenna, 12 dBi, 120^{o} x 11^{o}, Dual Polarity (H/V)	RF	2 x N-Type jacks

Electrical

Table 1-14: Electrical Specifications, Stand-Alone AU

Unit	Details
General	Power consumption: 25 W
AU-NI	External power supply AC input power: 100-240 V r.m.s., 47-63 Hz DC power output: 12 V, 4 A
AU-RE	12 VDC from the AU-NI via the IF cables

Modular Base Station Equipment

Mechanical

Table 1-15: Mechanical Specifications, Modular Base Station Equipment

Unit	Structure	Dimensions (cm)	Weight (kg/lb)
BS-SH	19" rack (3U) or desktop installation	13 x 48.2 x 25.6	4.76 / 10.5
BS-PS	DC power supply module	12.9 x 7 x 25.3	0.7 / 1.54
BS-PS-AC	AC power supply module	12.9 x 7 x 25.3	1.2 / 2.6
BS-AU	Indoor module of the AU-BS access unit	12.9 x 3.5 x 25.5	0.22 / 0.48
BS-GU	Indoor module of the GU-A-BS GPS system	12.9 x 3.5 x 23	0.22 / 0.48
GU-RA	A plastic tubular enclosure, pole mountable	15.5 x 12.7 (diameter)	0.363 / 0.8
AU-RE-900	Metal box, 2"-3" pole mountable	30.6 x 12 x 4.7	1.6 / 3.5
900 MHz antenna, 10 dBi, 65^{o} x 65^{o}, Flat Panel (H/V)	Plastic radome with aluminum base plate, 1.5"-4" pole mountable	30.5 x 30.5 x1.5	1.5 / 3.3
900 MHz antenna, 12 dBi, 120^{o} x 11^{o}, Dual Polarity (H/V)	Plastic radome with aluminum base plate, 1.5"-4" pole mountable	120 x 16 x 8	6.1 / 13.5

Connectors

Table 1-16: Connectors, Modular Base Station Equipment

Unit	Connector	Description
BS-AU	IF	TNC female jack, lightning protected
	ETHERNET	10BaseT Ethernet (RJ-45) with 2 embedded LEDs. Cable connection to a PC: crossed

Table 1-16: Connectors, Modular Base Station Equipment

Unit	Connector	Description
	Monitor	3-pin low profile
BS-PS	-48V	3 pin DC power plug
BS-PS-AC	AC IN	3 pin AC power plug
BS-GU	ETH	10BaseT Ethernet (RJ 45) with 2 embedded LEDsCable connection to a PC: straight
	SYNC IN	9-pin Micro D-Type jack, Molex 83619-9003 (mates with Molex 83421-9014 or similar);4 contact closure alarm indicators
	SYNC OUT	9-pin Micro D-Type jack, Molex 83619-9003 (mates with Molex 83421-9014 or similar);3 non-latching relays, rating = 24 V (DC or AC) @ 1 A max.
	AL IN	9-pin Micro D-Type jack, Molex 83619-9003 (mates with Molex 83421-9014 or similar)
	AL OUT	9-pin Micro D-Type jack, Molex 83619-9003 (mates with Molex 83421-9014 or similar)
GU-RA	GPS	12-pin round
AU-RE	ANT	N-Type female jack
	IF	TNC jack, lightning protected
900 MHz antenna, 10 dBi, 65^{o} x 65^{o}, Flat Panel (H/V)	RF	N-Type jack
900 MHz antenna, 12 dBi, 120^{o} x 11^{o}, Dual Polarity (H/V)	RF	2 x N-Type jacks

Electrical

Table 1-17: Electrical Specifications, Modular Base Station Equipment

Unit	Details
General	200 W for a fully equipped chassis (1 PS, 6 AU, 1 GU)
BS-PS	DC power input: -48 V, 5.2 A max. DC power output: 12 V; 5 V
BS-PS-AC	AC power input: 85-256 VAC, 47-65 Hz DC power output: 12 V; 5 V; 3.3 V (not used)
BS-AU	5 VDC, 12 VDC from the power supply module(s) via the back plane
AU-RE	12 VDC from the BS-AU via the IF cables
AU-BS (BS-AU module plus AU-RE outdoor unit)	Power consumption: 25 W
BS-GU	5 VDC, 12 VDC from the power supply module(s) via the back plane
GU-RA	12 VDC from the BS-GU over the connecting cable

This page left intentionally blank.

2

Chapter 2 - Installation

In this Chapter

Installing the Stand-Alone AU/ Modular Base Station Equipment

Installation Requirements

This section describes all the supplies required to install the Stand-Alone AU or the modular Base Station equipment, and the items included in the installation packages.

NOTE

Before proceeding beyond this point and installing the Stand-Alone AU or the modular Base Station equipment, the spectrum survey should already be complete using the spectrum analysis tool provided with this equipment (special firmware). The results of the survey will identify the specific clear channels and polarization required to configure and operate the 900 MHz equipment. Refer to the Breeze Access Spectrum Sweep & Analysis Utility User's Guide for detailed instructions on performing the survey. This step is important to ensure the best performance from the product.

Packing List for AU-E-NI-900 Stand-Alone AU

The Stand-Alone AU installation kit includes the following components:

- AU-NI indoor unit
- Wall mounting kit for the AU-NI
- AU-PS power supply with a mains power cord
- AU-RE-900 MHz Radio Unit with a connection to an external antenna
- Pole mounting kit for the outdoor unit
- A Monitor cable (for configuring the served SUs)
- Documentation and Utilities CD

Packing List for Modular Base Station Equipment

BS-SH Base Station Chassis

- BS-SH chassis (with blank panels)
- Rubber legs for optional desktop installation
- BS-PS DC power supply
- DC power cable
- Documentation and Utilities CD

BS-SH-AC Base Station Chassis

- BS-SH-AC Chassis (with blank panels)
- Rubber legs for optional desktop installation
- BS-PS-AC AC Power Supply
- AC Power Cable
- Documentation CD

AU-E-BS Access Units (up to six per chassis)

- AU-RE-900 MHz Radio Unit with a connection to an external antenna
- Pole mounting kit for the outdoor unit
- BS-AU Network Interface module
- A Monitor cable (for configuring the served SUs)

BS-PS DC Power Supply (one or two per chassis)

- BS-PS power supply module
- DC power cable

BS-PS-AC Power Supply (one or two per chassis)

- BS-PS-AC power supply module
- AC power cable

GU-A-BS GPS and Alarms System

- BS-GU module
- GU-RA GPS antenna and receiver

- 1” threaded mounting pole for the GU-RA GPS antenna
- Antenna Mounting kit

Additional General Item Required for the Installation

The following items are also required to install the Stand-Alone AU or modular Base Station equipment:

- 900 MHz antenna(s) (see list of approved antennas in Table 2-3 on page 2-7)
- Grounding cables and other lightning protection materials according to specific installation requirements
- Ethernet cable(s)

Table 2-1: Required Ethernet Cables

Unit Type	Connection to a PC	Connection to a hub/router
AU (AU-NI, BS-AU)	Crossed	Straight
GPS BS-GU module	Straight	Crossed

- For configuring basic parameters – a portable PC with Terminal Emulation software (connected to the equipment using the appropriate Monitor cable)
  OR
  A portable PC with Ethernet NIC, an Ethernet cable (see Table 2-1) and Telnet software (or BreezeCONFIG ACCESS Configuration Utility)

NOTE

The BS-GU does not have an external Monitor port and it should be configured via the Ethernet port using Telnet.

- Installation tools and materials, including appropriate means (e.g. poles) for installing the system components and antennas.

Equipment Location Guidelines

This section provides key guidelines for selecting the optimal installation locations for the various BreezeACCESS 900 system components.

WARNING

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 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:

- Units should be installed in easily accessible locations to facilitate installation and testing.
- The higher the placement of the antennas, the better the achievable link quality. Locate the AU's antenna at least 20 cm (8 in.) away from any other antenna.
- The antenna of the AU should be installed as close as possible to the AU-RE Radio Unit to minimize loss in the RF cable. The antenna should be installed so as to provide coverage to all Subscriber Units within its service area.

NOTE

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

Refer to Alvarion web site (www.alvarion-usa.com) for recommendations regarding grounding and lightning protection.

IF Cables

The AU-RE Radio Unit is connected to the indoor unit via an IF cable carrying both signals and power. The IF frequency is 440 MHz. The maximum permitted attenuation of the IF cable is 15dB at 440 MHz and the maximum permitted DC resistance (the sum of the DC resistance of the inner and outer conductors) is 1.5 ohms. This enables a cable length of up to 30m when using the standard RG 58 cable.

If longer cables are required, a cable with lower attenuation and/or DC resistance should be used.

Table 2-2 provides detailed information about common cables such as the RG 58 and RG 213. If the spectral environment is polluted with noise in the 440 MHz band, it is recommended that a higher quality double-shielded cable, such as the LMR 200, LMR 240 and LMR 400, be used. (These cables are manufactured by Times Communications).

Table 2-2: IF Cables

Cable Type	RG 58	RG 213	LMR 200	LMR 240	LMR 400
Maximum Cable Length (m)	30	100	45	65	150

If you are using coaxial cables other than those listed above, consult the cable manufacturers' specification to ensure that the cable's attenuation at 440 MHz does not exceed 15dB, and its DC loss (center conductor plus shield) does not exceed 1.5 ohms.

AU's 900 MHz Antennas

Table 2-3: AU FCC Approved Antenna

Antenna Model	Part Number
902-928 MHz, 10 dBi Panel Antenna, V/HPOL pole or wall mount, N-Type connector	999436

NOTE

Alvarion reserves the right to change the antenna specifications and models offered at any time. Consult with Alvarion sales on the availability of other antennas for use with the Access Unit, or visit the Alvarion website and see the list of third party antennas shown in the "Alvarion Certified Third Party Antennas" list.

WARNING

It is the responsibility of the professional installer to ensure that when using the outdoor antenna kits, only these antenna configurations shown in the table above are used along with the minimum cable lengths provided with the product. The use of any antenna other than those listed is expressly forbidden in accordance to FCC rules CFR47 part 15.204.

Installing the Radio Unit

The following sections describe how to install the AU-RE Radio Unit, including pole mounting the unit, and connecting the IF and grounding cables.

Pole Mounting the Radio Unit

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

- Special brackets and open-ended bolts are supplied with each unit. There are two pairs of threaded holes on the back of the unit, enabling the special brackets to be mounted on diverse pole widths.
- Special grooves on the sides of the unit enable the use of metal bands to secure the unit to a pole. The bands must be 9/16 inches wide and at least 12 inches long. The metal bands are not included with the installation package.

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

NOTE

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

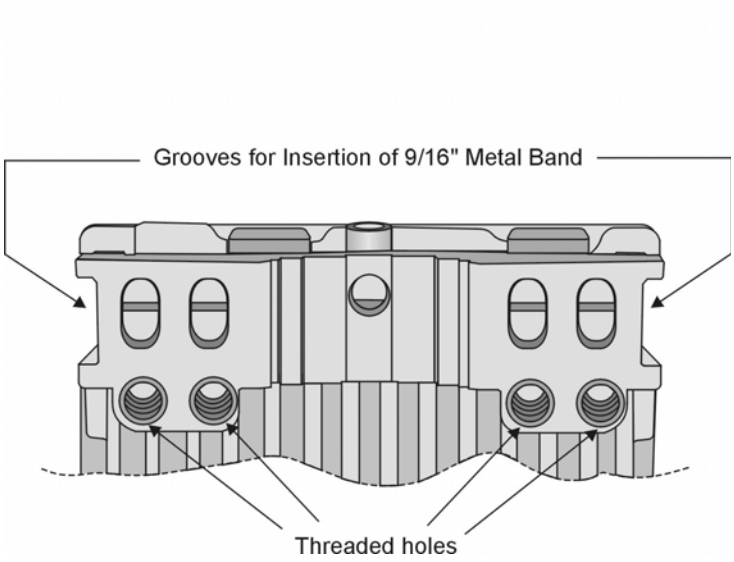


Figure 2-1: Threaded Holes/Grooves

Figure 2-2 illustrates the method of installing a Radio Unit on a pole, using the brackets and open-ended bolts.

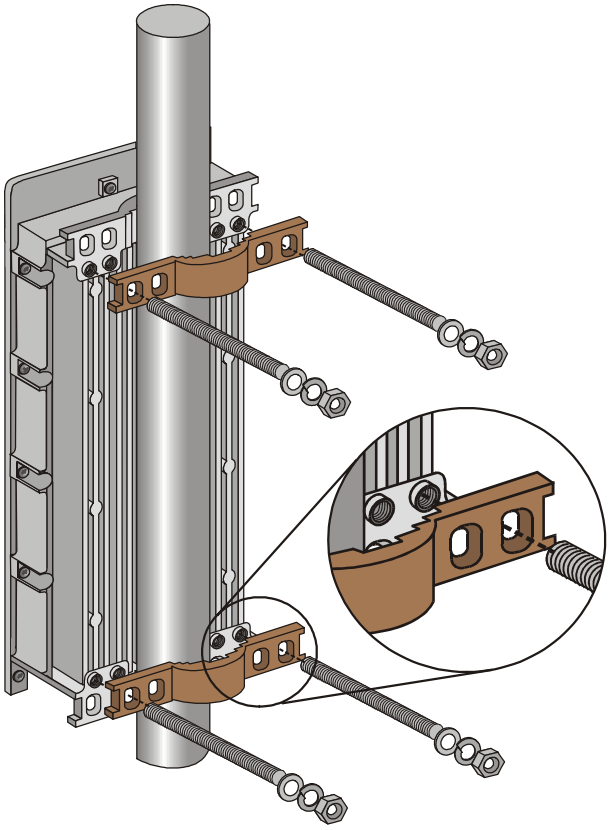


Figure 2-2: 3" Pole Installation Using Special Brackets

NOTE

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

Connecting the Ground and IF Cables

The Ground terminal (marked ⏚) and the IF cable connector (marked IF) are located on the bottom panel of the Radio Unit, as shown in Figure 2-3.

To connect the ground cable:

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

To connect the IF cable:

1. Connect one end of the coaxial IF cable to the IF connector on the bottom panel of the unit
2. Verify that the length of the IF cable is sufficient to reach the indoor unit.
3. The IF cable connectors should be sealed properly to protect against rain and moisture

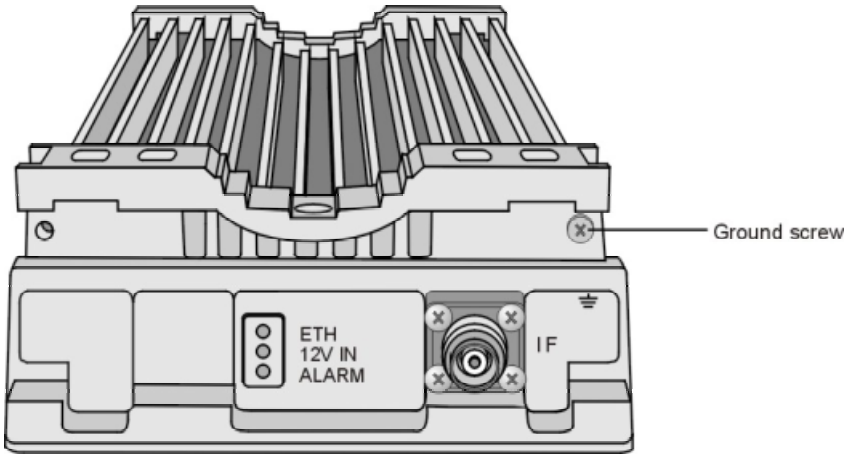


Figure 2-3: AU-RE-900 Bottom Panel

Installing the 900 MHz Antenna

Locate the 900 MHz antenna at least 20 cm (8 in.) away from the any other antenna. Refer to the installation instructions included in the antenna kit. Use only the antennas stated in Table 2-3.

NOTE

Verify that you use the correct polarization according to the results of the spectrum analysis survey.

WARNING

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 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.

Connecting the RF Cable

Connect a coaxial RF cable between the antenna connector of the AU-RE and the antenna.

NOTE

All RF cables connections must be adequately sealed against water.

Installing the AU-NI Indoor Unit

NOTE

Refer to Installing the Radio Unit on page 2-8 for details on the AU-RE outdoor unit.

Place the unit in an appropriate location on a shelf or a table. The unit can be wall mounted using the installation materials provided with the unit. Use a 6 mm (1/4") drill and the supplied template plate for easy and accurate marking of the holes.

To connect the IF, RF and power cables:

1. Connect a coaxial IF cable between the IF connector of the AU-NI and the IF connector of the AU-RE.

CAUTION

Do not connect or disconnect the IF cables while the AU-NI unit is powered.

2. Connect a coaxial RF cable between the antenna connector of the AU-RE and the antenna.

NOTE

All IF and RF cables connections must be adequately sealed against water.

3. Connect an Ethernet cable between the Ethernet port and the network. Use a straight cable to connect to a hub/switch.
4. Connect the power supply DC power cord to the DC In jack (marked 12VDC) located on the rear panel of the AU-NI unit.
5. Connect the mains power cord to the power supply unit. Connect the mains power plug to a mains power outlet.

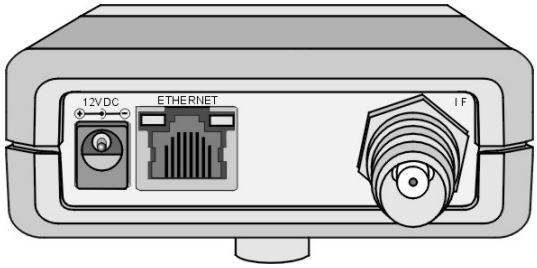


Figure 2-4: The AU-NI Rear Panel

Installing Modular Base Station Equipment

BS-SH Slot Assignments

The base station chassis has ten slots.

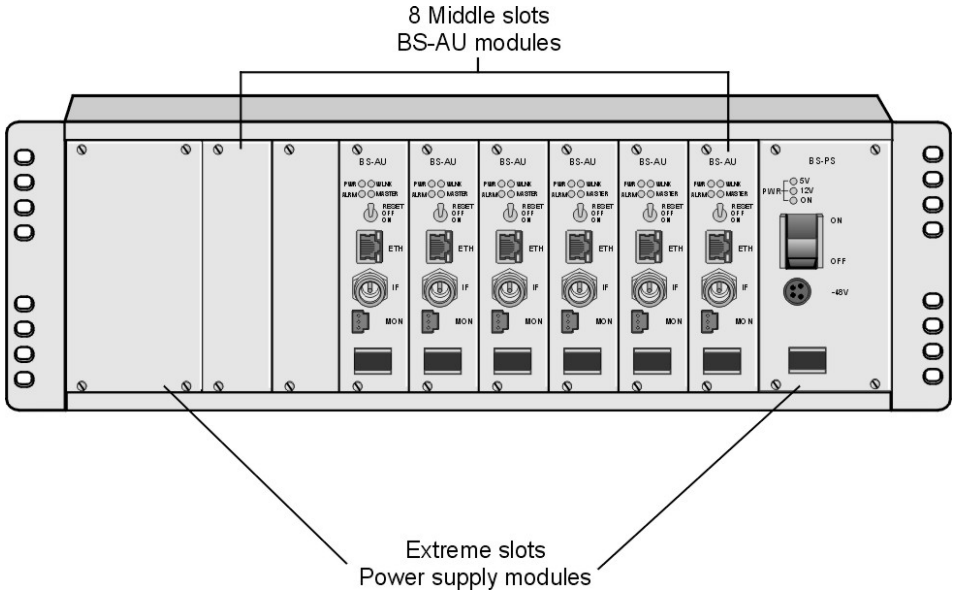


Figure 2-5: BS-SH Chassis Slot Assignments

The two wide slots on both sides of the shelf accommodate the BS-PS or BS_PS-AC power supply modules. The shelf is designed to support power supply redundancy through the use of two power supply modules. If a single power supply is used, it can be inserted in any of the two available slots. When using two power supply modules, both modules must be the same type (either both BS-PS or both BS-PS-AC).

The remaining eight slots can accommodate up to six active BS-AU modules. Two extra slots are for an optional BS-GU GPS module and/or for future use. Active BS_AU modules can be installed in any of the eight slots. Unused slots should be covered by blank panels.

The BS-PS

The BS-PS provides power to all the modules installed in the BS-SH chassis.

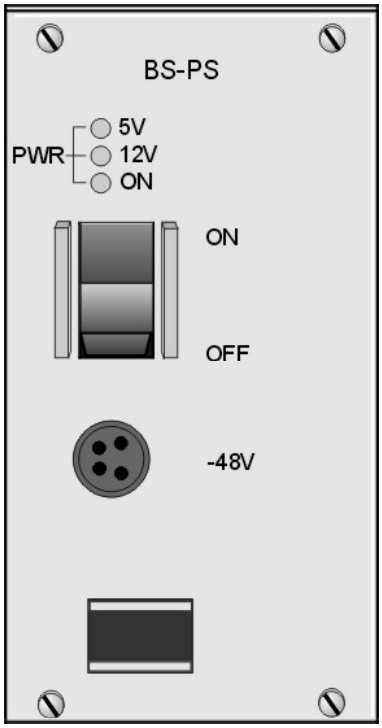


Figure 2-6: BS-PS Front Panel

The BS-PS provides a power input connector (marked -48V) for connecting the -48VDC power source to the module. The color codes of the cable wires are:

Black -48 VDC

Red + (Return)

The power switch turns the mains power to the power supply ON and OFF.

The BS-PS-AC

The BS-PS-AC is an AC to DC converter that provides power to all the modules installed in the BS-SH chassis.

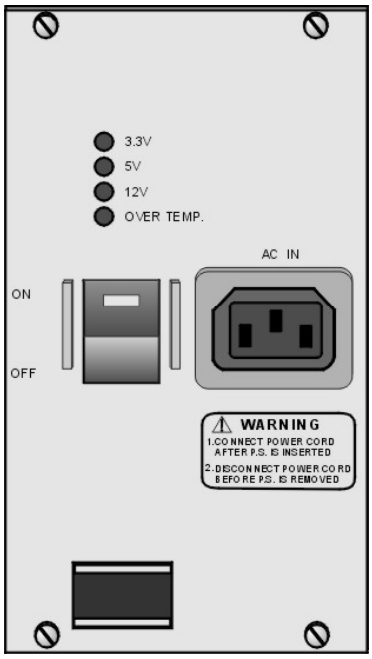


Figure 2-7: BS-PS-AC Front Panel

The BS-PS-AC provides a power input connector (marked AC IN) for connecting the AC power cable to the mains.

The ON/OFF power switch controls the connection of the mains power to an AC to DC converter.

WARNING

If two power supply modules are used in the same chassis for redundancy, both power supplies must be of the same type. Do not use a mix of AC and DC power supply modules in the same chassis.

The BS-AU

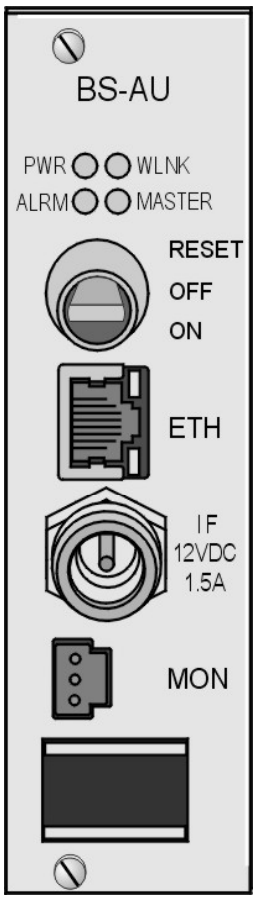


Figure 2-8: BS-AU Front Panel

The BS-AU provides the following interfaces:

- **ETH**: An Ethernet 10Base-T 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.
- **IF**: An IF connector for connecting the BS-AU to an AU-RE outdoor unit.
- **MON**: A Monitor connector for connecting an ASCII terminal with terminal emulation software for configuration and maintenance purposes.

The switch on the BS-AU front panel controls the supply of 12 VDC power to the outdoor unit via the IF cable. The momentary RESET position of this switch is for resetting the outdoor unit. In the OFF position, power is not supplied to the outdoor unit, even when the BS-AU unit is still on.

BS-SH Chassis and Modules Installation Procedure

1. Install the BS-SH chassis in a 19" cabinet (or place on an appropriate shelf/table). When mounting the BS-SH chassis on a desktop, screw on the rubber legs shipped with the unit. To prevent over-heating, leave a free space of at least 1 U between the upper/lower covers of the chassis and other units.
2. Connect a ground cable between the ground terminal (located on the back panel of the BS-SH chassis) and a grounding point (or to the rack when appropriate).
3. Carefully insert the BS-PS or BS-PS-AC Power Supply and the BS-AU modules into their intended slots and push firmly until they are securely locked. Before inserting the modules, verify that the switches of all BS-AU modules are in the OFF position. Close the captive screws attached to each module. Place blank covers over all the unused slots.
4. Connect the IF cable(s) to the connector(s) marked IF located on the front panel(s) of the BS-AU module(s). The other side of the IF cable should already be connected to the outdoor unit.
5. If a BS-PS DC power supply is used, connect the DC power cable to the -48 VDC jack located on the front panel of the BS-PS. If a redundant power supply module is installed, connect a power cable to it as well. Connect the power cable(s) to the -48 VDC power source. Connect the black wire to the -48 VDC contact of the power source. Connect the red wire to the + (Return) contact. Connect the shield to the ground.
6. If a BS-PS-AC AC power supply is used, connect the AC power cable to the AC IN jack located on the front panel of the BS-PS-AC. If a redundant power supply module is installed, connect a power cable to that unit as well. Connect the power cable(s) to the AC mains.
7. Switch the BS-PS or BS-PS-AC power supplies to ON. Verify that all the power indicator LEDs on the front panel are on. In BS-PS-AC modules, verify that the OVERTEMP alarm indicator is off.
8. Configure the basic parameters in all BS-AU modules as described in Chapter 3 - Commissioning. Set the switches on the front panel of all BS-AU modules in the chassis to ON only after all the basic parameters have been configured properly. This is to avoid transmitting at undesired frequencies.

CAUTION

Disconnect the IF cable from the BS-AU module before inserting or removing it to/from the BS-SH chassis.

Installing the GU-A-BS GPS and Alarms System

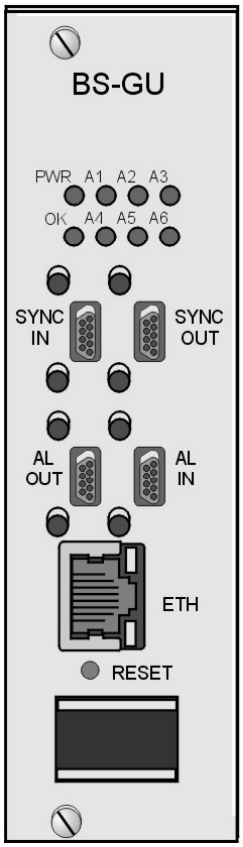


Figure 2-9: BS-GU Front Panel

The BS-GU provides the following interfaces:

- **SYNC IN**: Received signals from the GPS antenna unit. If several collocated BS-GU modules are daisy-chained, this connector is used by a "Slave" module to receive signals from the "Master" module's SYNC OUT connector.
- **SYNC OUT**: Transfers the signals received on the SYNC IN port. If the module is a "Master" operating in "local" mode, the internally generated synchronization signals are also transferred to the "Slave" via this connector.
- **AL IN**: Four dry contact connections for alarm-in indications from external devices.
- **AL OUT**: Three relay outputs to external devices.
- **ETH**: Ethernet 10Base-T interface. Use a straight cable to connect directly to a PC. Use a crossed cable to connect to a hub.

To reset the GPS module, press the RESET button with a paper clip or a similar object.

Installing the GU-RA GPS Antenna

WARNING

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 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.

1. Screw the GPS antenna firmly to the special 1" threaded pole.
2. Use the mounting kit supplied with the unit (or any other suitable means) to secure the GPS antenna pole to an existing pole (e.g. any pole used for mounting base station antennas or the outdoor AU-RE units). Choose the location to ensure an obstacle-free line of sight from the GPS antenna to the sky, extending at least 30 degrees in all directions.

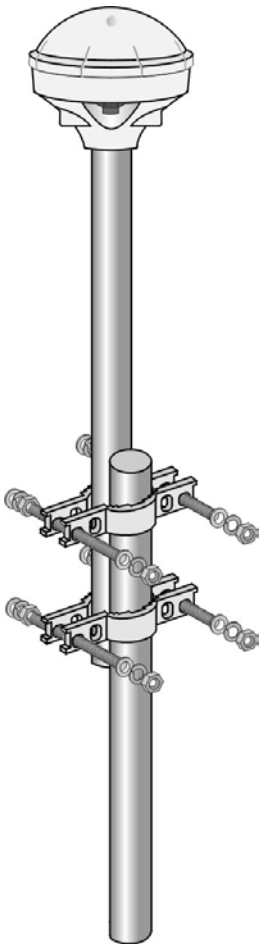


Figure 2-10: GPS GU-RA Installation

3. Secure the GPS cable to the mounting pole, leaving a free length of cable (with the 12-pin round connector at the end) sufficient for connecting to the antenna module.

WARNING

The cable is very heavy and connecting it to the antenna without first securing it to the pole may damage the connector.

4. Connect the 12-pin round connector to the GPS antenna.
5. Route the cable to the location intended for installation of the BS-GU module.

Installing the BS-GU module

NOTE

When adding the BS-GU to an active base station, it is recommended to start by reconfiguring the AU previously defined as Master to Slave, then immediately inserting and configuring the Number of Hopping Frequencies parameter in the BS-GU module. Otherwise both the Master AU and the BS-GU will send conflicting synchronization signals to the Slave AUs. During this process, connectivity with the Subscriber Units will be interrupted. It is recommended to perform the upgrade during a planned downtime or at a time of minimal traffic. Properly configuring the value of the Number of Hopping Frequencies parameter in the BS-GU is mandatory for proper operation of the base station. All other parameters of the BS-GU module may be configured later as they do not impact the operation of the system.

1. Carefully insert the BS-GU module into any of the free suitable slots in the BS-SH chassis and push firmly until it is securely locked. Close the captive screws attached to the module.
2. Connect the 9-pin micro D-Type connector of the GPS cable to the SYNC IN connector (the top-left connector) of the BS-GU module.

WARNING

Deactivate the power to the BS-GU unit before connecting it to a GPS antenna. Switch on the BS-GU only after the GPS antenna has been connected.

Daisy-chaining Two or More BS-GU Modules

If two or more BS-GU modules are installed in different collocated BS-SH chassis, use a synchronization cable (supplied separately) to connect the SYNC OUT connector of the first (Master) module to the SYNC IN connector of the second module. The SYNC OUT of this second module may be connected to the SYNC IN of a third module, and so on.

Installing the SU-I Subscriber Unit

Installation Requirements

This section describes all the supplies required to install the SU-I Subscriber Units and the items included in each installation package.

Packing List for SU-I-1D-900 Subscriber Unit

- SU-I-1D-900 Subscriber Unit
- 5 VDC universal power adaptor
- Mounting bracket for wall or ceiling installation
- A torque key for the antenna connector
- 12 inch jumper cable
- Antenna (optional):
  - UNI-10-900 V/HPOL outdoor antenna, including pole mounting hardware
    Or
  - UNI-7-900 V/HPOL indoor antenna with a 10 ft. cable, including wall/window mounting hardware

Additional Installation Requirements

The following items are also required to install the Subscriber Unit:

- Grounding cables and other lightning protection materials according to specific installation requirements
- Straight Ethernet cable for connecting the Subscriber Unit to a PC
- For configuring basic parameters - A portable PC, with Ethernet NIC and Telnet software (or BreezeCONFIG ACCESS Configuration Utility)
  OR
  A portable PC with Terminal Emulation software and a Monitor cable
- Installation tools and materials, including appropriate means (e.g. a pole) for installing the outdoor antenna. A Wall/Roof Mounting Arm (P/N 872442 is available from Alvarion.

SU's 900 MHz Antennas

Table 2-4: SU FCC Approved Antenna

Antenna Model	Part Number
902-928 MHz, 10 dBi Panel Antenna, V/HPOL outdoor pole or wall mount, N-Type connector	990010
902-928 MHz, 7 dBi, 40°x 35° (V/H POL) indoor window or wall mountable antenna	999437

NOTE

Alvarion reserves the right to change the antenna specifications and models offered at any time. Consult with Alvarion sales on the availability of other antennas for use with the Access Unit, or visit the Alvarion website and see the list of third party antennas shown in the "Alvarion Certified Third Party Antennas" list.

Installation Guidelines

This section describes the installation guidelines and the various considerations that must be taken into account when planning the installation.

Location of the Unit

- The unit can be placed on a desktop or a shelf, or can be attached to a wall.
- The unit should be installed as near as possible to the antenna. The RF cable connecting the unit to the antenna should be as short as possible to guarantee minimum power loss.
- The location of the Subscriber Unit should take into account its connection to a power outlet and the user's data equipment.
- Keep the units well away from sources of heat, such as radiators, air-conditioners, etc.

Location of the Antenna

- The antenna should be installed where it can be directed towards the location of the Access Unit. Any physical object in the path between the unit and the Access Unit other than foliage should be avoided. Any buildings or other physical structure such as hills or other natural geographic features higher than the antenna and situated in the path between the two sites can constitute obstructions.
- **Outdoor Antenna**: The outdoor antenna should be pole mounted on the rooftop or on a sidewall.

WARNING

It is the responsibility of the professional installer to ensure that when using the outdoor antenna kit, that only this antenna provided with the subscriber unit is used along with the minimum cable lengths provided. The use of any antenna other than those listed is expressly forbidden in accordance to FCC rules CFR47 part 15.204.

- **Window Mounting the Indoor Antenna**: For a window installation of the indoor antenna, choose a window location with best line of sight to AU antenna. Generally, the higher the antenna on the window the better the signal strength. Keep in mind that some windows can be made of lead or metal-based materials, which may have an adverse effect on antenna performance. If it is found that a windows properties affect performance, try a wall mount for better performance by bypassing the window and enabling propagation through a near front wall.
- **Wall Mounting the Indoor Antenna**: For an indoor wall mounting, choose a wall location with best line of sight to AU antenna. Generally, the higher the antenna on the wall the better the signal strength. Keep in mind when using a wall mount configuration the indoor antenna may point through windows to the base station. Some window obstacles such as metal window blinds may affect performance. If it is found that window blinds affect performance, raise blinds or keep blinds open to achieve best performance.

Antenna Polarization

Antenna polarization must be the same at both ends of the link. The antenna can be mounted to provide either vertical or horizontal polarization. To verify polarization of the outdoor antenna, refer to the mounting instructions in Appendix B.

NOTE

Verify that you use the correct polarization according to the results of the spectrum analysis survey.

Antenna Seal

The antenna connectors as well as other outdoors RF connections must be sealed against rain.

Lightning Protection

Lightning protection is designed to protect people, property and equipment by providing a path to ground for the lightning's energy. The lightning arrestor diverts the strike energy to the ground along a deliberate and controlled path instead of allowing it to choose a random path. Lightning protection for a building is more forgiving than protection of electronic devices. A building can withstand up to 100,000 volts, but electronic equipment may be damaged by just a few volts.

Lightning protection entails connecting an antenna discharge unit (also called an arrestor) to each cable as close as possible to the point where it enters the building. It also entails proper grounding of the arrestors and of the antenna mast (if the antenna is connected to one).

The lightning arrestor should be installed and grounded at the point where the cable enters the building. The arrestor is connected to the unit at one end and to the antenna at the other end.

The professional installer you choose must be knowledgeable about lightning protection. The installer must install the lightning protector in a way that maximizes lightning protection.

A Lightning and Grounding installation kit is available from Alvarion.

Refer to Alvarion web site (www.alvarion-usa.com) for recommendations regarding grounding and lightning protection.

WARNING

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 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.

Installing SU-I Units

Connectors and LEDs

The unit provides the following interfaces:

- An Ethernet connector (marked ETH) on the rear panel for connecting the unit to a PC.
- A DC-IN 5V connector on the side panel for the power transformer.
- A Monitor connector on the side panel for connecting an ASCII terminal with terminal emulation software for configuration and maintenance purposes.
- An RF connector (marked 2) on the side panel for connecting to an antenna.

The unit provides the following LED indicators on its front panel:

Table 2-5: Subscriber Unit's LEDs

Name	Description	Functionality	
POWER	Power Supply	On - After successful power up Off - Power off	
WLNK	Wireless Link Activity	Blinking - Receiving packets from the wireless link Off - no reception of packets from the wireless link	
ETHERNET	Ethernet Activity	Blinking - Reception of data from Ethernet LAN Off - No reception of data from Ethernet LAN	
SIGNAL QUALITY	Received Signal Quality		Very low quality reception or not synchronized with Access Unit
			Low quality reception (usually enabling 1Mbps traffic)
			Medium quality reception (usually enabling 2 Mbps traffic)
			High quality reception (usually enabling 3 Mbps traffic)

Wall Mounting the Unit

Use the supplied brackets for wall mounting to install the unit on a wall or a ceiling.

To mount the unit on a wall:

1. Turn the unit so the rear panel is facing you.
2. Unscrew the two screws located at the antennas end of the unit (the top screws).
3. Align the Unit Mounting Slots (see Figure 2-11) with the slots you have just unscrewed.

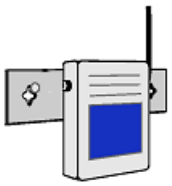


Figure 2-11: Wall Mounting the SU-I

4. Using the longer screws supplied with the wall mounts, screw the wall mount to the unit.
5. Align the Convenience Mounting Slots (see Figure 2-12) with the nails, push the wall mount against the wall and let it slide down until it rests on the nails.

Special slots have been added to the wall mounts to allow for unobtrusive cable installation. These slots should be used to fasten cables coming out of the unit to the wall mounts, eliminating loose or tangled cable installations.

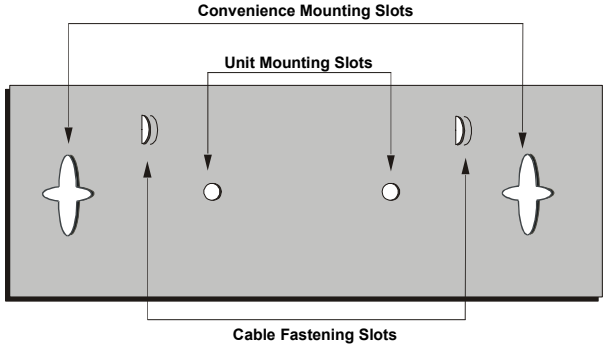


Figure 2-12: Wall Mounting Plate

Installing the Outdoor Antenna and Lightning Protection

To install the outdoor antenna and lightning protection:

1. The antenna can be mounted on a 1”-4” pole. The mounting on a 1”-2.5” pole differs from mounting on a 2.5”-4” pole. You may use the Wall/Roof Mount Arm available from Alvarion (P/N 872442). Refer to Appendix A - Mounting the 10dBi Antenna for instructions on installing the antenna.

NOTE

Vertical polarization: The POLARIZATION arrow should point upward or downward.
Horizontal polarization: The POLARIZATION arrow should be parallel to ground.

2. Install the DC grounding block or optional lighning arrestor near the point where the antenna cable enters the building and perform all the required RF and grounding connections according to the instructions provided in Appendix B - Lightning and Grounding Instructions.

NOTE

All RF cables connections must be adequately sealed against water.

Window Mounting the Indoor Antenna

To install the indoor antenna on a window:

1. Clean glass area where antenna will be mounted. Ensure that no substance such as grease or oil will affect making a permanent mount.

2. Assemble window bracket to the antenna in chosen mount (vertical or horizontal) position by removing the two applicable screws at both ends of the antenna. Be sure that the window bracket is mounted on the correct face of the antenna: The front face of the antenna that should point towards the AU is clear. The back face of the antenna has the polarization (V/H) label.

NOTE

Vertical polarization: The arrow marked V on the back of the antenna should point upward or downward.

Horizontal polarization: The arrow marked H on the back of the antenna should point upward or downward.

3. There are 3 Suction-cups located at the ends of the window mounting bracket to provide attachment to the window. Mount the antenna by placing the 3 Suction-cups to the window, with the ends of the mounting bracket pointing upward and downward. Ensure that each cup is pressed down firmly.

NOTE

The suction cup mount is installed on the radiating side of the antenna so when attached to the glass it is radiating out towards the base station.

4. The window bracket is attached to the antenna at a rotating junction to provide +/- 30 degree horizontal articulation. Always optimize the indoor antenna signal strength by making a series of slow horizontal movements, recording the RSSI level of the attached SU-I subscriber unit for each horizontal location.

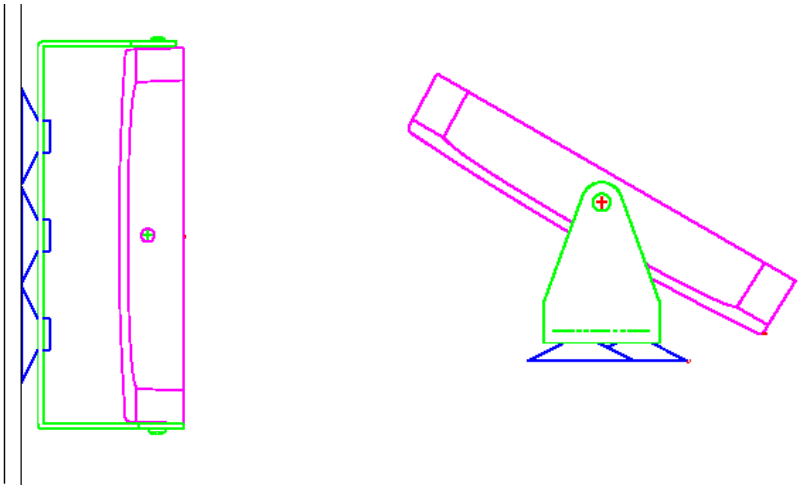


Figure 2-13: Window Mounting the Indoor Antenna

Wall Mounting the Indoor Antenna

To install the indoor antenna on a wall:

1. Assemble wall bracket to the antenna in chosen mount (vertical or horizontal) position by removing the two applicable screws at both ends of the antenna. Be sure that the wall bracket is mounted on the correct face of the antenna: The front face of the antenna that should point towards the AU is clear. The back face of the antenna has the polarization (V/H) label.

NOTE

Vertical polarization: The arrow marked V on the back of the antenna should point upward or downward.

Horizontal polarization: The arrow marked H on the back of the antenna should point upward or downward,

2. There are 2 white anchors and 2 screws provided with the antenna. Use the anchors when mounting on a wall that will not support normal screw insertion such as a drywall. In using the anchors, drill a 3/16 " (4mm) pilot hole into the drywall, insert the anchor into the hole so the exposed end of the anchor is flush with the wall. Mount the antenna by placing the 2 screws into the wall, ensuring each screw is firm and secure making a permanent mount.

3. The wall bracket is attached to the antenna at a rotating junction to provide +/- 30 degree horizontal articulation. Always optimize the indoor antenna signal strength by making a series of slow horizontal movements, recording the RSSI level of the attached SU-I subscriber unit for each horizontal location.

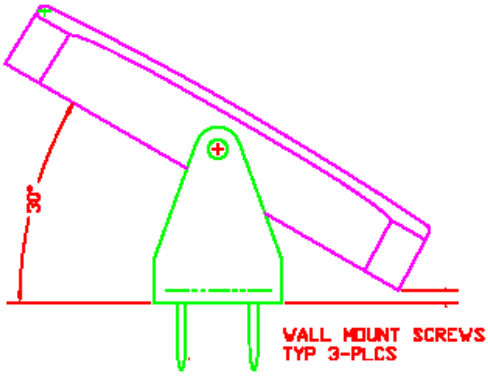


Figure 2-14: Wall Mounting the Indoor Antenna

Connecting the Antenna to the Unit

To connect the antenna to the unit:

1. Connect the cable to the connector marked 2 on the side of the unit.

NOTE

Do not remove the runner cover of the connector marked 1, and do not attempt to connect the antenna to this connector.

2. Use the torque key included in the package to tighten the cable to the connector. The key is designed to prevent over tightening of the screws and protects the connectors from damage. If excessive pressure is applied to tighten the screws, the torque key will break.

NOTE

The use of improper tools for tightening antenna connection cables to BreezeACCESS units may result in damage to the cable connectors.

Connecting the Unit to the CPE and Power Outlet

The unit operates on a power input of 5VDC, supplied by the power transformer included with the unit.

To connect the unit to the CPE and Power Outlet:

1. Plug the output jack of the power transformer into the DC input jack (marked DC IN 5V) located on the side of the unit.
2. Connect the power transformer to a power outlet - 110/ 220VAC.
3. Use a straight Ethernet 10Base-T cable to connect a PC to the Ethernet port located on the rear panel of the unit.

3

Chapter 3 - Commissioning

About this Chapter

Set-up and Initialization

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

NOTE

The decision on hopping frequencies to be used, based on the results of the Spectrum Analysis survey, must be made prior to starting the process of configuring basic parameters.

Accessing the Monitor Program

NOTE

The BS-GU does not have an external Monitor port and it should be configured via the Ethernet port using Telnet.

To access the Monitor Program using the Monitor cable:

Use the Monitor cable to connect the Ethernet connector of the unit to the COM port of a PC running a terminal emulation program. The COM port connector on the Monitor cable is a 9-pin D-type plug.

1. Run a terminal emulation program, such as HyperTerminal™.
2. Set the communication parameters as shown in Table 3-1.
3. Press Enter. 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.
5. Enter your password and press Enter. The Main Menu is displayed.

Table 3-1: Monitor Port Communication Parameters

Parameter	Value
Baud Rate	9600
Data Bits	8
Stop Bits	1
Parity	None
Flow Control	Xon/Xoff
Connector	Connected COM port

NOTE

Following three unsuccessful login attempts (using incorrect passwords) from either the Monitor port or via Telnet, 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.

To access the Monitor Program locally using Telnet:

1. Connect a PC to the Ethernet port using a crossover cable when connecting to the AU and a straight cable when connecting to the GU or to the SU-I.
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.
5. Enter your password and press Enter. The Main Menu is displayed.

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.

Configuring Basic Parameters

The Basic Configuration menu includes all the parameters necessary for the initial installation and operation of the BreezeACCESS 900 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 Tables 3-2 (AU), 3-3 (SU) and 3-4 (GU). Once the basic parameters are configured, the unit must be reset in order to activate the new configuration.

Refer to Chapter 4 - Operation and Administration for detailed information on the applicable parameters.

Basic Parameters in AU

Table 3-2: Basic Parameters in the AU

Parameter	Default Value	Comment
IP Address	10.0.0.1	
Subnet Mask	255.0.0.0	
Default Gateway Address	0.0.0.0	
DHCP Options	Disable	
Access to DHCP	From Ethernet Only	
ESSID	ESSID1	
Operator ESSID Option	Enable	
Operator ESSID	ESSID1	
HDM Mode	Disable	
Flexible Hopping Definition	915	According to the spectrum analysis survey
Scrambling Mode	Enhanced	
Manual Sequence Definition		Applicable only when Scrambling Mode is configured to Manual Scrambling
Spanning Factor	1	Applicable only for Enhanced Scrambling with 7 or more frequencies

Table 3-2: Basic Parameters in the AU

Parameter	Default Value	Comment
Hopping Sequence (Shift) (AU-BS)	0	
Hopping Sync (AU-BS)	Idle	
Transmit Power Control	0	See Note below
VLAN Link Type	Hybrid	
VLAN ID-Management	65535	
Authentication Algorithm	Open System	Can be changed to Shared Key only after configuring at least one WEP Key
WEP Key 1-4	0000000000 (none)	
Encryption Seed	7	
Encryption Polynom Index	0	

NOTE

For compliance with FCC rules, the power input to the 900 MHz antenna of the AU should not exceed 23dBm. The Transmit Power Control should be set to 1 (delivering 24.5dBm power output) only when using a longer RF cable with an attenuation of 1.5dB at least, or when using an external Band-pass filter to compensate for the power loss in the filter. Such a filter may be required if the equipment is located near a very strong transmitter using frequencies that are close to the frequencies used by the BreezeACCESS equipment.

NOTE

Once the basic parameters are configured, the unit must be reset in order to activate the new configuration.

Basic Parameters in SU-I

Table 3-3: Basic Parameters in the SU-I

Parameter	Default Value	Comment
IP Address	10.0.0.1	
Subnet Mask	255.0.0.0	
Default Gateway Address	0.0.0.0	
DHCP Options	Disable	
Access to DHCP	From Wlan Only	
ESSID	ESSID1	
Flexible Hopping Definition	915	According to the spectrum analysis survey. Not applicable when the Scan Entire Band is enabled.
Scrambling Mode	Enhanced	Not applicable when HDM Mode in the AU is enabled.
Manual Sequence Definition		Applicable only when Scrambling Mode is configured to Manual Scrambling and HDM Mode in the AU is disabled.
Scan Entire Band	Enable	
Transmit Antenna	Antenna 2	Must remain Antenna 2
Transmit Level	23 dBm	
Best AU Support	Disable	
Preferred AU MAC Address	00-00-00-00-00-00 (none)	Applicable only when Best AU Support is enabled
Scanning Mode	Active	
VLAN Link Type	Hybrid	
VLAN ID-Management	65535	
Authentication Algorithm	Open System	Can be changed to Shared Key only after configuring the WEP Key and the applicable Default Key ID

Table 3-3: Basic Parameters in the SU-I		
Parameter	**Default Value**	**Comment**
Default Key ID	1	
WEP Key 1-4	0000000000 (none)	
Encryption Seed	7	
Encryption Polynom Index	0	

NOTE

Once the basic parameters are configured, the unit must be reset in order to activate the new configuration.

Basic Parameters in GU

Table 3-4: Basic Parameters in the GU		
Parameter	**Default Value**	**Comment**
IP Address	10.0.0.1	
Subnet Mask	255.0.0.0	
Default Gateway Address	0.0.0.0	
DHCP Options	Disable	
Number of Hopping Frequencies		According to the Number of Hopping Frequencies in the AUs
Automatic Recovery Option	Enable	Applicable to “Master” GU only
Automatic Recovery Interval	15 minutes	Applicable to “Master” GU only
VLAN ID-Management	65535	

NOTE

Once the basic parameters are configured, the unit must be reset in order to activate the new configuration.

GU Connections

Connecting External Alarm devices

Open-ended cables are available from the company for connecting to the module external alarm inputs through the AL IN connector and/or activating external devices through the AL OUT connector. See the tables that follow for descriptions of the connectors' pins functionality. For details on defining and using the alarm inputs and output, refer to THe Operation and Administration section in BreezeACCESS II System Manual.

WARNING

The load of the Alarm Out (AL OUT) connector should not exceed 24 V@1 A max.

Alarm In Cable

Table 3-5: GU Alarm In Cable

9-pin Micro D-Type AL IN Connector	Description	Color Code
1	Alarm Input 1	Brown
2	Alarm Input 2	White
3	Alarm Input 3	Green
4	Alarm Input 4	Red
5	Not Connected	Black
6	GND	Purple
7	GND	Yellow
8	GND	Orange
9	GND	Blue

The other side of the cable is supplied open-ended.

The cable shield is connected to the body of the connector.

Alarm Out Cable

Table 3-6: GU Alarm Out Cable		
9-pin Micro D-Type AL OUT Connector	**Description**	**Color Code**
1	Relay 1 Common	Brown
2	Relay 1 Normally Closed	White
3	Relay 2 Common	Green
4	Relay 3 Common	Red
5	Relay 3 Normally Closed	Black
6	Relay 1 Normally Open	Purple
7	Relay 2 Normally Closed	Yellow
8	Relay 2 Normally Open	Orange
9	Relay 3 Normally Open	Blue

The other side of the cable is supplied open-ended.

The cable shield is connected to the body of the connector.

GPS Cable

Cable Type: EIA RS-422 3X2X25AWG +1X2X24 AWG FTP Shielded cable.

Table 3-7: GU GPS Cable

9-pin Micro D-Type SYNC IN Connector	Description*	Color Code	12-pin round connector
1	GPS_TX+	Yellow	5
2	GPS_TX-	Green	4
3	GPS_RX+	Red	3
4	GPS_RX-	Orange	2
5	1PPS+	Brown	11
6	1PPS-	Black	12
7	DC_GPS+	Blue (thick)**	1
8	DC_GPS-	Brown (thick)**	9
9	Not Connected		6, 7, 8, 10

* Descriptions are with respect to the BS-GU SYNC IN connector side.

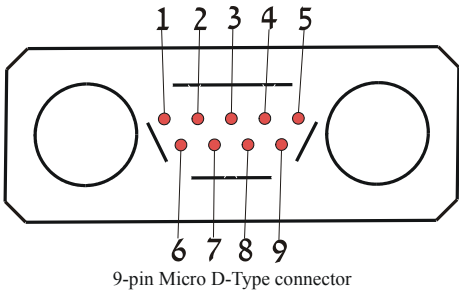


Figure 3-1: 9 Pin Micro-D Type Connector Schematic (Cable Side)

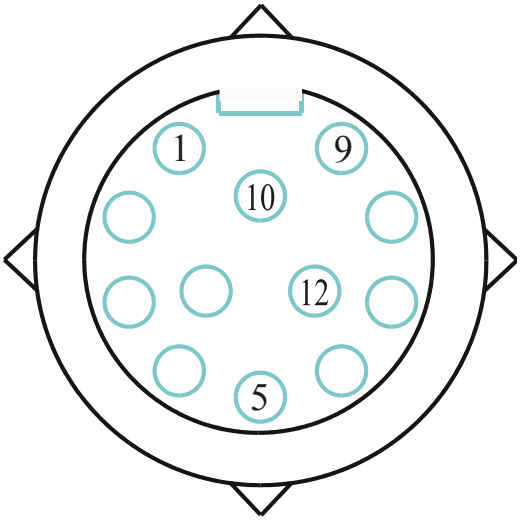


Figure 3-2: 12 Pin Round Connector Schematic

SYNC Cable

Cable Type: EIA RS-422 3X2X25AWG +1X2X24 AWG FTP Shielded cable.

Table 3-8: GU GPS Cable

9-pin Micro D-Type SYNC OUT Connector	Description*	Color Code	9-pin Micro D-Type SYNC-IN Connector
1	GPS TX+/SYNC D+	Black	1
2	GPS TX-/SYNC D-	Brown	2
5	1PPS+/SYNC S+	Red	5
6	1PPS-/SYNC S-	Orange	6
8	DC GPS	Green	8
9	Slave	Yellow	9
3, 4, 7	Not Connected		3, 4, 7

* Descriptions are with respect to the BS-GU SYNC IN connector side.

The SYNC cables shield is connected to the body of the micro D-Type connectors.

Aligning the Subscriber Unit's Antenna

For antenna alignment, you can use either the 3 Signal Quality LED indicators on the front panel of the SU-I or view the Received Signal Strength Indication in the Site Survey menu. Typically, alignment using the Signal Quality LEDs is sufficient. This section describes how to align the SU-RA antenna using the Signal Quality LEDs.

NOTE

Antenna alignment using the Signal Quality LEDs is possible only after the SU is associated with an AU. The AU must be operational and the basic SU's parameters must be correctly configured. If not, the unit will not be able to synchronize with the AU. As the SNR measurement is performed on received frames, its results are meaningless unless the SU is associated with an AU.

To align the antenna of the SU:

1. Align the antenna by pointing it in the general direction of the Access Unit.
2. Verify that the power indication of the unit is **On**.
3. Verify that the WLNK LED of the unit is **On**, indicating that the unit is associated with an Access Unit. If the WLNK LED is **Off**, check that the basic parameters are correctly configured. 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. Check the SIGNAL QUALITY L, M and H LEDs. The higher the number of LEDs that are on, the better the quality of the link. Rotate the antenna left and/or right until you reach the point of highest signal quality reading on the SIGNAL QUALITY LEDs. For proper operation, at least one (L) LED should be on. If this is not possible, improve the link quality by placing the antenna at a higher point or in an alternate location.
5. For an outdoor antenna installation, secure the antenna firmly to the pole.

Verifying Proper Operation

The following sections describe how to verify the correct functioning of the various unit, Ethernet connections and data connectivity.

LED Indicators

To verify the correct operation of the units, examine the LED indicators of the units. The following tables list the provided LEDs and their associated indications.

Table 3-9: SU-I LEDs

Name	Description	Functionality	
POWER	Power Supply	On - After successful power up Off - Power off	
WLNK	Wireless Link Activity	Blinking - Receiving packets from the wireless link Off - no reception of packets from the wireless link	
ETHERNET	Ethernet Activity	Blinking - Reception of data from Ethernet LAN Off - No reception of data from Ethernet LAN	
SIGNAL QUALITY	Received Signal Quality		Very low quality reception or not synchronized with Access Unit
			Low quality reception (usually enabling 1Mbps traffic)
			Medium quality reception (usually enabling 2 Mbps traffic)
			High quality reception (usually enabling 3 Mbps traffic)

Table 3-10: AU-RE-900 LEDs

Name	Description	Functionality
ETH	Ethernet activity indication	Off – No traffic activity detected on the Ethernet port Blinking – Data received from or transmitted to the Ethernet port
12V IN	12 VDC Power Supply Indication	On –12 VDC power is supplied to the unit Off – 12 VDC power is not available
ALARM	Alarm Indication	On – A problem with the power amplifier or in the locking process of any of the synthesizers Off – Normal operation

Table 3-11: AU-NI LEDs

Name	Description	Functionality
PWR	Power Supply	On – After successful power up, indicating that 12 VDC is supplied to the outdoor unit. Off – Power off or failure to supply 12 VDC to the outdoor unit.
WLNK	Wireless Link Activity Indictor	Blinking – Packets received from the wireless link Off – No reception of packets from the wireless link

Table 3-12: BS-AU LEDs

Name	Description	Functionality
PWR	Power supply 12 VDC	■ On – After successful power up, indicating that 12 VDC is supplied to the outdoor unit. ■ Off – Power off or DC/DC converter failure (12 VDC not supplied to the outdoor unit)
WLNK	Wireless link activity	■ Blinking – Receiving packets from the wireless media ■ Off – No reception of packets from the wireless media
ALRM	Alarm	On – Loss of hopping synchronization (in Slave mode)
MASTER	Master unit	On – The unit is configured as Master

Table 3-13: BS-PS DC Power Supply LEDs

Name	Description
ON	-48 VDC is available and Power Supply is ON
5V	The 5V power supply module is OK and power is consumed (at least one BS-AU module is inserted)
12V	The 12V power supply module is OK and power is consumed (at least one AU-RA/RE unit is connected)

Table 3-14: BS-PS-AC AC Power Supply LEDs	
Name	**Functionality**
3.3V	On – the 3.3 V power supply module is OK (3.3V power supply is not used by current BreezeACCESS modules)
5V	On – the 5V power supply module is OK
12V	On – the 12V power supply module is OK
OVERTEMP	On – an Over Temperature condition in the power supply module

NOTE

If the OVERTEMP indication stays on for more than 10 seconds, the power supply module will shut itself off automatically to prevent damage.

Table 3-15: BS-GU LEDs	
Name	**Functionality**
PWR (green)	■ On – Power supply functioning properly. ■ Off – Power supply not functioning properly.
OK (green)	■ On – Proper signals are being received from the GPS antenna. ■ Off – The GPS antenna is not connected or it is not functioning properly.
A1 (red)	On – Alarm In 1 (external) is activated.
A2 (red)	On – Alarm In 2 (external) is activated.
A3 (red)	On – Alarm In 3 (external) is activated.
A4 (red)	On – Alarm In 4 (external) is activated.
A5, A6 (red)	Reserved for future use.

Verifying the Ethernet Connection

Once you have connected the unit to a PC (SU-I) or to the network (AU), verify that the Ethernet Integrity indicator (the yellow LED embedded in the Ethernet connector) is on, indicating that the unit is connected to an Ethernet segment. The Ethernet Activity indicator (the green embedded LED) should blink whenever the unit receives or transmits traffic on the Ethernet port.

Verifying Data Connectivity (SU-I)

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

Verifying Proper Operation of the GU-A-BS GPS Unit

When the unit is operating properly, the PWR and OK green LEDS should be on, indicating that the BS-GU module is supplying power to the GU-RA GPS antenna and that the GPS antenna is functioning properly.

NOTE

It may take up to 10 minutes from the time the GU-RA GPS antenna is powered up until it is fully synchronized with the GPS satellite system.

If the OK LED is not on, check the functionality of the GPS antenna as follows:

1. From the Main Menu, select Info Screens. The Info Screens menu opens.
2. From the Info Screen menu, select Show Unit Status and view the Unit Status display. You should see one of the following messages:

- UTC is available; date..; time..: This message indicates that the GPS antenna has synchronized with the satellite system and that the BS-GU is functioning properly. The message may include an incorrect time and date, such as a date in 1999: this indicates that the GPS antenna has not yet synchronized with the GPS satellite system.

–Or–

- UTC time is not available: This message indicates that the BS_GU is not getting timing signals from the GPS antenna. If the antenna is functioning and properly connected to the module, a probable reason might be that the antenna has not yet synchronized with the GPS satellite system

4

Chapter 4 - Operation and Administration

In this Chapter

Working with the Monitor Program

The Local Terminal Management program can be accessed either via the MON port of the unit or using Telnet.

NOTE

It is impossible to access the Local Terminal Management from both the MON port and Telnet simultaneously.

Accessing the Monitor Program Using the MON Port

1. Use the Monitor cable to connect the MON connector of the unit to the COM port of your ASCII ANSI terminal or PC. The COM port connector on the Monitor cable is a 9_pin D_type plug.
2. Run a terminal emulation program, such as HyperTerminal™.
3. Set the communication parameters as shown in the following table:

Table 4-1: MON Port Communication Parameters

Parameter	Value
Baud Rate	9600
Data Bits	8
Stop Bits	1
Parity	None
Flow Control	Xon/Xoff
Connector	Connected COM port

4. Click Enter. The Select Access Level menu is displayed.
5. Select the required access level, depending on your specific access rights. A password entry request is displayed. Table 4-2 lists the default passwords for each of the access levels.

6. Enter your password and click 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.

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 4-2 lists the default passwords for each of the access levels.

Table 4-2: Default Passwords

Access Rights	Password
Read-Only	public
Installer	user
Administrator	private

NOTE

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

5. Enter your password and click 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/SU
Official Release Version - 4.5.4
Release Date: Tue Dec 23 18:44:18 2003
Main Menu
==========
1 -  Info Screens
2 - Unit Control
3 -  Basic Configuration
4 - Site Survey
5 - Advanced Configuration
>>>
```

Figure 4-1: Main Menu (Administrator Level)

NOTE

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

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

- For users with read only access rights, only the Info Screens option is displayed. Users with this access level are not able to access the Unit Control, Basic Configuration, Site Survey and Advanced Configuration menus.
- For users with Installer access rights, the first four menu items, Info Screens, Unit Control, Basic Configuration and Site Survey, are displayed. Users with this access level are not able to access the Advanced Configuration menu.
- For users with Administrator access rights, the full Main Menu is displayed. These users can access all the menu items.

Common Operations

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

- Type an option number to open or activate the option. In certain cases you may need to click Enter.
- Click Esc to exit a menu or option.

NOTE

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

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

Menus

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

- **Info Screens:** Provides a read only display of current parameter values. The Info screens menu is available at all access levels.
- **Unit Control:** Enables you to access general operations, such as resetting the unit, reverting to factory default parameters, changing passwords and switching between software versions. The Unit Control menu is available at the Installer and Administrator access levels.
- **Basic Configuration:** Enables you to access the set of parameters that are configured during the installation process. These parameters are also available in the Advanced Configuration menu. The Basic Configuration menu is available at the Installer and Administrator access levels.
- **Site Survey:** Enables you to activate certain tests and view various system counters. The Sit Survey menu is available at the Installer and Administrator access levels.
- **Advanced Configuration:** Enables you to access all system parameters, including the Basic Configuration parameters. The Advanced Configuration menu is available only at the Administrator access level.

Info Screens Menu

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

Show Unit Status

The Show Unit Status menu displays the current values of the following parameters:

- **Unit Type:** Identifies the unit's type: Access Unit, Subscriber Unit or GPS and Alarms Module.
- **Unit MAC Address:** The unit's unique IEEE MAC address.
- **Unit Ethernet Port Operational Status:** The current operational status of the Ethernet port: Up (Ethernet link identified on Ethernet Port), Down (No link identified on Ethernet Port) or Testing (a temporary status).
- **Unit Hardware Version**: The hardware version of the unit (In IF based products the HW version of the indoor unit is displayed).
- **Flash Type:** The type and size of the Flash memory.
- **Flash Versions:**
  - **Current Version** – The software version that is currently active.
  - **Shadow Version** – The software version currently defined as the shadow (backup) version.
  - **Version After Reset** – The software version that will be used after the next reset.
- **Console Speed:** The speed defined in the unit for the connected terminal, used for running the terminal emulation program.
- **Number of Associations Since Last Reset:** In SUs - the total number of associations with any AU since the last reset, including duplicate associations with the same AU.
  In AUs - the number of SUs that have associated with the AU since the last reset, including duplicate associations with the same SU.

The following parameters appear for Subscriber Units only:

- **Unit Status:** 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:** 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.

The following parameter appear for Access Units only:

- **Current Number of Associations:** The total number of SUs associated with this AU. This number may include units that are not currently active since 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. A SNAP frame is received from another AU indicating that the SU is now associated with the other AU.

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

The following parameter appear for GPS module only:

- **Unit Status:** The status of the GPS antenna. Either one of the following messages may be displayed:
  - UTC is available; date..; time..: This message indicates that the GPS antenna has synchronized with the satellite system and that the BS-GU is functioning properly. The message may include an incorrect time and date, such as a date in 1999. This indicates that the GPS antenna has not yet synchronized with the GPS satellites system.
  - UTC time is not available: This message indicates that the BS-GU is not getting timing signals from the GPS antenna. If the antenna is functioning and properly connected to the module, this may be because the antenna has not yet synchronized with the GPS satellite system.
- **Master/Slave Operation Mode**: A message indicating the operation mode of the unit: “Unit is working as Master” or “Unit is working as Slave”.

Show Basic Configuration

The Show Basic Configuration menu displays the current values of the parameters included in the Basic Configuration menu. When using Read-Only or Installer access rights several security related parameters are not displayed. The display includes some additional useful read-only information such as the Number of Hopping Frequencies in SU and AU.

Show Advanced Configuration

The Show Advanced Configuration menu enables you to access the read only sub menus that display the current values of the parameters included in the applicable sub menus of the Advanced Configuration menu. When using Read-Only or Installer access rights several security related parameters are not displayed. The display includes some additional useful read-only information such as the Number of Hopping Frequencies in SU and AU.

Show All Parameters

The Show All Parameters menu is a read only menu that displays the current values of all status and configuration parameters. When using Read-Only or Installer access rights several security related parameters are not displayed. The display includes some additional useful read-only information such as the Number of Hopping Frequencies in SU and AU.

Unit Control Menu

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

Reset Unit

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

Default Settings

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

The available options are:

Set Defaults:

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

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

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

   The complete Operator Defaults Configuration file can be downloaded/uploaded using TFTP with the SNMP Write community string. The procedure is the same as for downloading/uploading configuration files (for more information refer to Appendix E), except that the extension used for the file name is .cmr.

   Examples (using the default SNMP Write community string):

   To upload the configuration file using DOS based TFTP Client to an SU whose IP address is 206.25.63.65:
   tftp 206.25.63.65 put Suconf private.cmr.

   To download the configuration file from the same unit:
   tftp 206.25.63.65 get private.cmr Suconf

The available options in the Set Defaults submenu are:

- **Set Complete Factory Defaults:** Available only with Administrator access rights. Resets the unit to the set of Alvarion's standard default values. These are the default values as defined in this manual for each of the parameters. After the next reset all parameters will revert to their Factory Defaults value, except for the parameters that are marked in the "Complete" column of Table 4-3 on page 4-10.

NOTE

Activating Set Complete Factory Defaults will result in loss of connectivity. If the unit is managed remotely, you may lose the ability to communicate with it.

- **Set Partial Factory defaults:** Reverts all parameters to the values of the Factory Defaults configuration after the next reset, except for parameters that are necessary to maintain connectivity and to enable management of the unit and some other sensitive parameters. The exact list of parameters that are not changed depends on the access rights of the user. Referring to Table 4-3, the parameters that are not changed after activating Set Partial Factory Defaults using Administrator access rights are marked in the "Partial-Admin" Column. The parameters that are not changed after activating Set Partial Factory Defaults using Installer access rights are marked in the "Partial-Installer" Column.

Table 4-3: Parameters not changed after Set Complete/Partial Defaults

Parameter	Complete	Partial – Admin	Partial - Installer
Unit Control Parameters			
Passwords	√	√	√
Event Log Policy			√
Auto Configuration Option			√
IP Parameters			
IP Address		√	√
Subnet Mask		√	√
Default Gateway Address		√	√

Table 4-3: Parameters not changed after Set Complete/Partial Defaults

Parameter	Complete	Partial – Admin	Partial - Installer
DHCP Option		√	√
Access to DHCP		√	√
Air Interface Parameters			
ESSID		√	√
Operator ESSID Option		√	√
Operator ESSID		√	√
Best AU Support		√	√
Preferred AU MAC Address		√	√
Dwell Time		√	√
Hopping Sequence (Shift)		√	√
HDM Mode	√	√	√
Defined Sub Band	√	√	√
Scrambling Mode	√	√	√
Manual Sequence	√	√	√
Spanning Factor	√	√	√
Acknowledge Delay Limit		√	√
MAC Address Black List		√	√
Bridge Parameters			
VLAN Link Type		√	√
VLAN ID – Data		√	√
VLAN ID – Management		√	√
VLAN Forwarding Support		√	√
Forwarding VLAN IDs		√	√

Table 4-3: Parameters not changed after Set Complete/Partial Defaults

Parameter	Complete	Partial – Admin	Partial - Installer
VLAN Relaying Support		√	√
Relaying VLAN IDs		√	√
VLAN Priority – Data		√	√
VLAN Priority – Management		√	√
VLAN Priority Threshold		√	√
Ethernet Port Control		√	√
Security Parameters			
Authentication Algorithm		√	√
Default Key ID		√	√
WEP Key 1 to 4		√	√
Encryption Seed		√	√
Encryption Polynom Index		√	√
Network Management Parameters			
Access To Network Management			√
Network Management Filtering			√
Network Management IP Addresses			√
Send SNMP Traps			√
Per Trap Control (all Send Trap Parameters)			√
SNMP Traps IP destination			√
SNMP Traps Community			√
RADIUS Parameters			
RADIUS User Name			√
RADIUS User Password			√
RADIUS Shared Secret			√

Table 4-3: Parameters not changed after Set Complete/Partial Defaults

Parameter	Complete	Partial – Admin	Partial - Installer
Authentication Option			√
RADIUS Server Authentication IP address			√
RADIUS Server Authentication Port			√
Accounting Option			√
RADIUS Server Accounting IP address			√
RADIUS Server Accounting Port			√
Accounting Interval			√

- **Set Complete Operator Defaults:** Available only with Administrator access rights. Set the unit to its' Operator Defaults configuration. After the next reset, all parameters will revert to their Operator Defaults values, except for the parameters that are marked in the "Complete" column of Table 4-3. Operator Defaults configuration can be defined by the Administrator (see Save Current Configuration As Operator Defaults below). It may also be defined at the factory according to customer's definition. The default Operators Defaults configuration is the Factory Defaults configuration.

NOTE

Activating Set Complete Operator Defaults will result in loss of connectivity. If the unit is managed remotely, you may lose the ability to communicate with it.

- **Set Partial Operator defaults:** Reverts all parameters to the values of the Operator Defaults configuration after the next reset, except for parameters that are necessary to maintain connectivity and to enable management of the unit and some other sensitive parameters. The exact list of parameters that are not changed depends on the access rights of the user. Referring to Table 4-3, the parameters that are not changed after activating Set Partial Operation Defaults using Administrator access rights are marked in the "Partial-Admin" Column. The parameters that are not changed after activating Set Partial Operator Defaults using Installer access rights are marked in the "Partial-Installer" Column.

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. This option is only available with Administrator access rights.

Change Unit Name

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

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

The default unit name is an empty string.

Change Password

The Change Password submenu enables changing the access password(s). 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 Table 4-2, on page 4-3 for a list of the default passwords for each of the access levels.

Flash Memory Control

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

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

Console Speed

The Console Speed parameter defines the speed at which the unit communicates with the terminal running the terminal emulation program. This parameter must be changed prior to changing the speed of the terminal connected to it.

The allowed speeds are: 9600, 19200, 38400, 57600 and 115200 baud.

The default value is 9600 baud.

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.

Event Log Menu

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

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

The Event Log Menu includes the following options:

Event Log Policy

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

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

The default selection is Fatal (FTL) Level severity.

Display Event Log

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

Erase Event Log

The Erase Event Log option enables clearing the event log.

Auto Configuration Parameters

The Auto Configuration sub-menu contains the parameters related to using the Auto Configuration mechanism. The Auto Configuration mechanism is intended to simplify the configuration process through automatic loading of a configuration file from a TFTP server. The Auto Configuration process is based on getting from a DHCP server the address of the TFTP server and the name of the configuration file to be loaded. This information is used by the unit to initiate a session with the TFTP server, requesting transfer of the applicable configuration file. Upon completing the process of loading the new configuration file, the unit will reset automatically so that the new configuration will take effect.

The following conditions must be met to enable the use of the Auto Configuration process:

- The DHCP Option (see page 2-37) in the unit must be configured to either DHCP Only or Automatic mode to enable communication with the DHCP server.
- The unit must be able to communicate with the DHCP server, according to the configured option of the Access to DHCP parameter.
- The address of the TFTP server and the proper name of the configuration file must be configured in the DHCP server:

- The Server Address should be specified in the 'sname' field of the DHCP header. The code for this option is 66, and the minimum length is 1. It must include a legal IP address, with a maximum length of 64 characters (maximum length includes spaces. Extra characters will be ignored).
- The Configuration File Name should be specified in the 'file' field of the DHCP header. The code for this option is 67, and the minimum length is 1. The maximum length is 128 characters (maximum length includes spaces. Extra characters will be ignored).

The unit shall initiate a request for a configuration file in the following cases (provided the DHCP Option is enabled):

- After power-up reset (HW reset), provided the Auto Configuration Option is enabled.
- Upon enabling the Auto Configuration Option.
- Upon a user initiated request.

NOTE

If the response messages from the DHCP server after the requests for TFTP Server Name and Boot File Name do not include these options, or if invalid values have been received, this DHCP server will not be used for automatic IP parameters assignment.

The Auto Configuration Parameters sub-menu includes the following options:

Auto Configuration Option

Select this option to disable or enable the Auto Configuration mechanism.

The default is Disable.

Request Auto Configuration

Select this option to initiate an Auto Configuration process.

NOTE

Upon completion of the Auto Configuration process the unit will reset automatically.

Show Auto Configuration Parameters

Select this option to view the status of the Auto Configuration Option and the Auto Configuration Received Status (Received/Not Received), indicating whether an Auto Configuration File has been received.

SNMP Read ESSID (AU, SU)

The SNMP Read ESSID parameter is available only under Administrator access rights. For security reasons, the values of some parameters, including ESSID and Run Time ESSID, can be viewed (get) using SNMP only with the Write Community string, and are not available with the Read Community string. When this parameter is enabled, it allows viewing (get) the values of ESSID and Run Time ESSID with the Read Community string as well.

The default is Disable.

Basic Configuration Menu

The Basic Configuration menu includes all the parameters that are necessary for the initial installation and operation of the unit. Once the unit is properly installed and operational, other parameters can be configured either locally using the monitor program or remotely using Telnet, SNMP management or TFTP for loading to the unit a pre-prepared configuration file.

For more information about the initial configuration of BreezeACCESS units, see Book 3: Commissioning.

The Basic Configuration menu includes the following submenu parameters:

- IP Address (see page 2-36)
- Subnet Mask (see page 2-36)
- Default Gateway Address (see page 2-36)
- DHCP Client (see page 2-37)
- Maximum Data Rate (SU) (see page 2-60)
- ESSID (see page 2-53)
- Operator ESSID Parameters (AU) (see page 2-53)
- Hopping Sequence (Shift) (AU-BS) (see page 2-37)
- Hopping Sync (AU-BS) (see page 2-52)
- Hybrid Digital Modulation Parameters
- Transmit Power Control (AU) (see page 2-57)
- Power Level (SU) (see page 2-45)
- Best AU Parameters (SU) (see page 2-55)
- VLAN Support
- Security Parameters
- Scanning Mode (SU) (see page 2-64)

NOTE

All parameters in the Basic Configuration menu are also available in the appropriate submenus of the Advanced Configuration menu.

Site Survey Menu

The Site Survey menu provides various tests and counters for verifying the quality of the wireless link and the proper operation of the unit. These tests can be used to help determine where to position the units for optimal coverage, to align antennas and to assist in troubleshooting.

Traffic Statistics (AU and SU)

The traffic statistics can be used to monitor, interpret and analyze the wired and wireless links performance. The traffic statistics counters display statistics concerning wireless link and Ethernet frames. The menu includes the following options:

- **Display Counters:** Select this option to display the current value of the Ethernet and Wireless Link Counters.
- **Reset Counters:** Select this option to reset all the counters.

Ethernet Counters

The unit receives Ethernet frames from its Ethernet port and forwards them to its internal bridge, which decides whether the frame should be transmitted to the wireless media. Frames that were discarded by the unit's hardware filter are not counted by the Ethernet counters.

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

The Ethernet Counters include the following statistics:

- **Total received frames via Ethernet:** The total number of frames received from the Ethernet port.
- **Transmitted wireless to Ethernet:** The number of frames transmitted by the unit to the Ethernet port. These are usually frames that have been received from the wireless side, but also frames generated by the unit itself.

Wireless Link Counters

The unit transmits data frames received from the Ethernet port, as well as self-generated control and wireless management frames, to the wireless media. After transmission of a unicast frame, 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 that are sent to more than one unit are not acknowledged. If an ACK is not received after a predefined time (determined by the Acknowledge Delay Limit parameter), the unit will retransmit the frame until it receives an ACK. If an ACK is not received before the number of retransmissions has reached a maximum predefined number (Number of Retransmissions parameter), it stops retransmitting and drops the frames.

- **Total transmitted frames to wireless**: The number of frames transmitted to the wireless media. The total includes one count for each data that was transmitted successfully (excluding retransmissions) as well as the number of transmitted control and wireless management frames.
- **Total transmitted unicast frames to wireless:** The number of unicast frames successfully transmitted to the wireless media, excluding retransmissions. This count is useful for calculating the rates of retransmissions or dropped frame, since only unicast frames are retransmitted if not acknowledged.
- **Total submitted frames (bridge)**: The total number of data and RTP frames submitted to the bridge for transmission to the wireless media. The count does not include control frames, wireless management frames, and retransmissions.
  In addition to the total count, there are also separate counts for frames according to the priority queue to which they were routed (Low, Mid, or High).
- **Frames dropped (too many retries):** The number of dropped frames. The frames that were retransmitted to the extent of the maximum allowed number of retransmissions without being acknowledged.
- **Total retransmitted frames:** The total number of retransmissions of frames (counts all unsuccessful transmissions/retransmissions).

- **Total Tx errors:** The number of transmit errors that have occurred. The total number of Tx errors includes transmissions that were not acknowledged properly, transmissions that were aborted and transmissions that were delayed for various reasons (e.g. not enough time until the end of the current dwell period).

  In addition, the following special counters are displayed to indicate the reason for the error:

  - H/W: An internal hardware problem in the modem.
  - ABR: The transmission was aborted before completion because of internal problems in the DSP.
  - CSL: The transmission was cancelled because the modem was busy in receiving data.
  - ACKTOUT (Acknowledge Timeout): The frame was not acknowledged within the time defined by the Acknowledge Delay Limit parameter.
  - FAIL: There was an internal timeout in the modem.
  - ACKCRC: There was a CRC error in the ACK message.
  - RTSC: The RTS was sent but no CTS was received (RTS collision).
  - EOD (End of Dwell): There was not enough time left to transmit the message

- **Total received frames from wireless:** The total number of frames that were received from the wireless media. The count includes data, control and wireless management frames, including beacons received from the AU. The count does not include frames that were discarded internally, bad frames and duplicate frames.
- **Total received data frames:** The total number of data frames received from the wireless media, including duplicate frames (see Duplicate frames discarded, below). In addition to the total count, there are also separate counts for data frames according to the receive priority queue to which they were routed (Low or High).
- **Bad fragments received:** The number of frames received from the wireless media with errors (CRC errors).

- **Duplicate frames discarded:** The number of frames discarded due to receiving multiple copies. If an acknowledge message was not received by the originating unit, the same data frame can be properly received twice (or more). Although duplicate frames are included in all counters that count 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 allowed information rate.

Per Hop Statistics (AU and SU)

The Per Hop Statistics provide information on performance of the wireless signal at different hopping frequencies. The Per Hop Statistics menu includes the following options:

- **Display Counters:** Select this option to display the continuously updated statistics.
- **Reset Counters:** Select this option to reset the Per Hop Statistics counters.

The Display Counters option displays various statistics for each of the hopping frequencies. In addition, it displays some general wireless link performance statistics:

- **Num:** The number of the information row, assigned automatically and sequentially by the program.
- **Freq:** The hopping frequency, according to the hopping sequence.
- **Rx:** The accumulated number of frames received at the specified frequency since last reset.
- **Tx:** The accumulated number of frames transmitted successfully at the specified frequency since last reset.
- **RTx:** The accumulated number of frames re-transmitted at the specified frequency since last reset.
- **avrDBM (avrRSSI**): The average RSSI (Received Signal Strength Indication) in dBm or RSSI units (according to the selected RSSI Display Option) of all the frames received at the specified frequency since the last reset. If no frames have been received, the value is NA (Not Available).

The Rx, Tx and RTx per hop counters accumulate the number of applicable frames since last reset. The counters can also be reset using the Reset Counters option in either the Per Hop Statistics menu or in the Traffic Counters menu.

The general rate (Frames per second) statistics is the average rate during the last 64 hops.

The display is continuously updated. Press any key to exit.

Ping Test (AU, SU and GU)

The Ping Test enables pinging another device in the network. The Ping Test menu includes the following options:

- **Destination IP Address**: The IP address of the destination unit for pinging.

  The default IP address is 192.0.0.1.

- **No. of Pings:** The number of ping attempts per session.

  The allowed range is from 0 to 9999. Select 0 for continuous pinging.

  The default value is 1.

- **Ping Frame Length:** The ping packet size.

  The allowed 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) to wait between ping attempts.

  The allowed range is from 200 to 60000 ms, in increments of 200 milliseconds (200, 400, 600,……60000).

  The default value is 200 ms.

- **Start Sending:** Select this option to start transmission of ping frames.

- **Stop Sending:** Select this option to stop the transmission of ping frames. The test will end automatically once the number of pings that were sent 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 was selected.

- **Show Ping Test Values:** Select this option to display the current values of the ping test parameters, the transmission status (sending or not), the number of pings sent, and the number of pings received (acknowledged frames).

Continuous Link Quality Display (SU)

The Continuous Link Quality Display option displays continuously updated entries that include information on the quality of the link between the SU and the AU. Press any key to abort the test.

Each line includes the number of Beacon frames that were received by the SU since the last measurement (total Rx), the average RSSI in dBm or RSSI units (according to the RSSI Display Option) for these frames (avrDBM/avrRSSI) and the Error rate (number of frames retransmitted by the SU in the last 100 transmitted frames).

The Error rate is meaningful only when there is traffic from the SU to the AU. For testing purposes it is recommended to use the Ping Test with a Ping Frame Length of 1472 bytes.

MAC Address Database

The MAC Address Database option in the AU displays information regarding the Subscriber Units associated with the AU as well as bridging (forwarding) information. 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 SW version of the SU is also displayed.
- **Sp (Special):** 5 addresses that are always present, which include:
  - The MAC address of the AU, which appears twice as it is learned from both the Ethernet and wireless ports.
  - 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 terminals) and the Vp (Virtual ports) entries. For Association Info 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. A SNAP frame is received from another AU indicating that the SU is now associated with the other AU.

b. The SU failed to respond to a certain number of 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 1019 (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.

Display Association Info

The Display Associations Info option 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

- The value configured for the Maximum Modulation Level parameter of the Subscriber Unit
- The Status of the Subscriber Unit. There are three options:

  A. **Associated**

  B. **Authenticated**

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

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

Table 4-4: Authentication and Association Process

Message	Direction	Status in AU
SU Status: Scanning*		
Probe Request (including ESSID) - Scanning	SU → AU	
Probe Response (only if correct ESSID in Probe Request)	AU → SU	-
SU Status: Synchronized		
Authentication Request	SU → AU	Not authenticated
Challenge Text**	AU → SU	Not authenticated
Challenge Text Encrypted**	AU → SU	Not authenticated
Authentication Successful	AU → SU	Authenticated
SU Status: Authenticated		
Association Request	SU → AU	Authenticated
Association Successful	AU → SU	Associated
SU Status: Associated		
ACK	SU → AU	Associated
Data Traffic	SU ↔ AU	Associated

* When passive scanning is used, the Scanning Phase is comprised of searching for a Beacon frame with the correct ESSID.

** Challenge text is used only if Authentication Algorithm is set to Shared Key.

- The average level of RF signals received from the Subscriber Unit.
- The SW version of the SU.

In addition, a summary table displays information about the Association Database (Association 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. A SNAP frame is received from another AU indicating that the SU is now associated with the other AU.

B. The SU failed to respond to a certain number of 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

The Show MIR/CIR Database option displays information on the MIR/CIR parameters of the associated Subscriber Units.

Each entry includes the following information:

- The MAC address of the associated Subscriber Unit.
- The SW version of the SU.
- 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.

Per-rate Counters (AU and SU)

The per-rate counters display the number of frames (excluding retransmissions) transmitted since the last reset at each of the rates (1 Mbps, 2 Mbps, 3 Mbps) and the total number of frames that were retransmitted at each of the rates. In the AU the information is provided for each of the associated SUs, identified by their MAC address. The counters in the AU are reset when there is a new association with an SU (including re-associations).

RSSI Display Option (AU and SU)

In BreezeACCESS units running SW versions 3.X and below, all measurements of received RF signal levels are displayed using arbitrary RSSI units. From version 4.0 onward, the conventional dBm measurement units can be used. However, to support users that prefer to continue using RSSI units, the RSSI Display option enables selecting the measurement units to be used for displaying received signal level values.

Refer to Appendix D - RSSI to dBm Conversion for details on converting RSSI to dBm and vice versa.

Available selections: dBm, RSSI.

Default selection: RSSI.

AU Alarms (AU)

The AU Alarms feature enables to identify and alert upon the detection of a potential problem in the outdoor unit of the AU, or another problem that causes significant degradation in the performance of the wireless link.

When the AU Alarms Option is enabled, three types of tests are performed: Traffic Statistics tests, Power tests and Associations test. Information is gathered continuously and various calculations used for decision making are performed each test cycle period that is defined by the configurable Test Cycle parameter. Alarms can be generated only after a sufficient time, defined by the configurable Learning Period parameter, has elapsed since the last reset (or since the AU Alarm Option was enabled).

Traffic Statistics Tests

The AU gathers traffic information that is used to calculate various traffic statistics. The calculated statistics are used for estimating the performance of the wireless link. The following traffic statistics rates are calculated for each test cycle period:

- **Current Retransmission Rate** - Defined as Nr/(Nt+ Nr), Where:

  Nr - Number of retransmissions during the last test cycle period.

Nt - Number of successfully transmitted unicast frames during the last test cycle. The minimum value of Nt+ Nr for a meaningful test is 50 (otherwise the result is NA).

- **Current Dropped Frames Rate** - Defined as Nd/Nt, where Nd is the number of dropped frames during the last test cycle period. Dropped frames are frames that were drooped because they were retransmitted to the extent of the maximum allowed number of retransmissions without being acknowledged. The minimum value of Nt for a meaningful test is 50 (otherwise the result is NA).

- **Current CRC Error Rate** - Defined as Ncrc/(Nrx+Ncrc), where:

  Ncrc - Number of frames received with a CRC error during the last test cycle period.

Nrx - Number of successfully received frames during the last test cycle period.

  The minimum value of Nrx+Ncrc for a meaningful test is 50 (otherwise the result is NA).

- **Current Duplicate Frames Rate** - Defined as Ndup/Nrx, where Ndup is the number of dropped frames during the last test cycle period. The minimum value of Nrx for a meaningful test is 50 (otherwise the result is NA).

In addition, the Average Rate is also calculated for each of the above traffic statistics rates, using the formula Ra(t)=[Rc*1 +Ra(t-1)*5]/6, where:

Rc - Current Rate

Ra(t) - The new value of the Average Rate for the applicable rate.

Ra(t-1) - the previous Average Rate of the applicable rate.

For the first test cycle after reset (or after enabling the AU Alarms Option), Ra= Rc.

For each traffic statistics type, three values can be configured:

- **Minor Alarm Threshold** - The threshold for decision on a minor severity alarm for the applicable traffic statistics type.
- **Major Alarm Threshold** - The threshold for decision on a major severity alarm for the applicable traffic statistics type.
- **Minimum Minor Alarm Delta** - serves in the minor alarm decision process, as described below.

A minor severity alarm is generated if both of the following conditions are met:

- The Current Rate of the applicable rate exceeds the Minor Alarm Threshold for this traffic statistics type.
- The Current Rate is higher than the Average Rate by at least the value of the Minimum Minor Alarm Delta, indicating a rapid decrease in performance.

A minor severity alarm will also be generated if the Current Rate dropped below the applicable Major Alarm Threshold but is still higher than the applicable Minor Alarm Threshold. (Alarm status changed from major to minor).

A major severity alarm is generated if the Current Rate has increased above the Major Alarm Threshold for the applicable traffic statistics type.

Power Tests

Each test cycle, the AU transmits a multicast SNAP (Sub Network Access Protocol) polling message to its associated SUs. The SUs must respond to this message within a given time frame. The response message includes the last RSSI level at which the SU receives transmissions from the AU.

Based on the RSSI information responses from the SUs, the AU performs a calculation of the SU Rx Power Average Delta, defined as the average difference for all SUs between the last RSSI at the SU and the previous (one before last) RSSI. The average is calculated only for SUs that responded to both of the last two polling message. The average is calculated as: $Sn=\Sigma_{n=1-N}$ [SURSSIn(t) - SURSSIn(t-1)]/N, where:

SURSSIn(t) - The last RSSI value received from responding SU number n.

SURSSIn(t-1) - The previous RSSI value received from responding SU number n.

N - The number of SUs that responded to both last and previous polling requests.

A Tx Power Level Decrease major severity alarm is generated if the decrease in the SU Rx Power Average Delta is higher than the value of the configurable SU Rx Power Decrease Threshold parameter:
-(SU Rx Power Average Delta) > SU Rx Power Decrease Threshold.

The alarm is generated only if the number of SUs used in calculating the SU Rx Power Average Delta (responded to both of the last two polling messages) is at least 5.

The AU also gathers for all responding SUs the RSSI level at which each SU was received by the AU. Based on these measurements, the AU performs a calculation of the AU Rx Power Average Delta, defined as the average difference for all responding SUs between the last RSSI at he AU and the previous (one before last) RSSI:

$Sn=\Sigma_{n=1-N}$ [AURSSIn(t) - AURSSIn(t-1)]/N, where:

AURSSIn(t) - The last RSSI value at which the responding SU number n was received by the AU.

AURSSIn(t-1) - The previous RSSI value at which the responding SU number n was received by the AU.

An Rx Signal Strength Decrease major severity alarm is generated if the decrease in the AU Rx Power Average Delta is higher than the value of the configurable AU Rx Power Decrease Threshold parameter:
-(AU Rx Power Average Delta) > AU Rx Power Decrease Threshold.

The alarm is generated only if the number of responding SUs used in calculating the AU Rx Power Average Delta (responded to both of the last two polling messages) is at least 5.

Association Tests

If the AU was reset 3 times because no SU became associated with it, a No Associations critical alarm will be generated, provided that previously the AU was associated with at least Minimum Number Of SUs.

An All Associations Lost major alarm is generated if no response was received by the AU to the last three polling messages, provided that prior to that, the average number of responding SUs was not lower than the Minimum Number Of SUs.

AU Alarms Summary

A prerequisite for all alarms except the No Associations alarm is that the elapsed time since last power-up (or since the AU Alarms Option was enabled) is not lower than the Learning Period.

The AU Alarms are summarized below.

No Associations Alarm

- **Severity:** Critical
- **On Conditions:** Three consecutive resets due to no response from any SU, and prior to that the AU was associated with at least Minimum Number Of SUs.
- **Off Conditions:**
  - At lease one SU became associated with the AU

    -OR-
  - All alarms were cleared

    -OR-
  - AU Alarms Option was disabled
- **Possible Problem:** Unlocked synthesizer, very low Tx power or another major HW problem.

All Associations Lost Alarm

- **Severity:** Major
- **On Conditions:** No response from any SU to the last 3 polling messages, and prior to that the average number of responding SUs was not lower than the Minimum Number Of SUs.
- **Off Conditions:**
  - At lease one SU became associated with the AU

    -OR-
  - All alarms were cleared

    -OR-
  - AU Alarms Option was disabled
- **Possible Problem:** Unlocked synthesizer, very low Tx power or another major HW problem.

Tx Power Level Decrease Alarm

- **Severity:** Major
- **On Conditions:** The inverse (minus) of SU Rx Power Average Delta is higher than SU Rx Power Decrease Threshold, and the number of SUs that responded to the last two polling messages is at least 5.
- **Off Conditions:**
  - All alarms were cleared

    -OR-
  - AU Alarms Option was disabled
- **Possible Problem:** A transmitter fault resulting in a significant decline of the Tx power level.

Rx Signal Strength Decrease Alarm

- **Severity:** Major
- **On Conditions:** The inverse (minus) of AU Rx Power Average Delta is higher than AU Rx Power Decrease Threshold, and the number of SUs that responded to the last two polling messages is at least 5.
- **Off Conditions:**
  - All alarms were cleared

    -OR-
  - AU Alarms Option was disabled
- **Possible Problem:** A receiver fault.

High Retransmissions Rate Alarm

- **Severity:** Minor, Major
- **Minor Severity Alarm On Conditions**:
  - The Retransmissions Current Rate exceeds the Retransmissions Minor Alarm Threshold, and is higher than the Retransmissions Average Rate by at least Retransmissions Minor Alarm Minimum Delta

    -OR-
  - The Retransmissions Current Rate has dropped below the Retransmissions Major Alarm Threshold but is still higher than the Retransmissions Minor Alarm Threshold.

- **Major Severity Alarm On Conditions:** The Retransmissions Current Rate is higher than the Retransmissions Major Alarm Threshold.
- **Off Conditions**:
  - The Retransmissions Current Rate has dropped below the Retransmissions Minor/Major Alarm Threshold

    -OR-
  - All alarms were cleared

    -OR-
  - AU Alarms Option was disabled
- **Possible Problem:**
  - Transmitter or receiver fault
  - Poor link conditions, strong interference, or an overloaded network.

High Dropped Frames Rate Alarm

- **Severity:** Minor, Major
- **Minor Severity Alarm On Conditions**:
  - The Dropped Frames Current Rate exceeds the Dropped Frames Minor Alarm Threshold, and is higher than the Dropped Frames Average Rate by at least Dropped Frames Minor Alarm Minimum Delta

    -OR-
  - The Dropped Frames Current Rate has dropped below the Dropped Frames Major Alarm Threshold, but is still higher than the Dropped Frames Minor Alarm Threshold.
- **Major Severity Alarm On Conditions**: The Dropped Frames Current Rate is higher than the Dropped Frames Major Alarm Threshold.
- **Off Conditions**:
  - The Dropped Frames Current Rate has dropped below the Dropped Frames Minor/Major Alarm Threshold

    -OR-
  - All alarms were cleared

-OR-

- AU Alarms Option was disabled

- **Possible Problem**:
  - Transmitter or receiver fault
  - A severe case of poor link conditions, strong interference, or an overloaded network.

High CRC Error Rate Alarm

- **Severity:** Minor, Major
- **Minor Severity Alarm On Conditions**:
  - The CRC Error Current Rate exceeds the CRC Error Minor Alarm Threshold, and is higher than the CRC Error Average Rate by at least CRC Error Minor Alarm Minimum Delta

    -OR-

  - The CRC Error Current Rate has dropped below the CRC Error Major Alarm Threshold but is still higher than the CRC Error Minor Alarm Threshold.
- **Major Severity Alarm On Conditions**: The CRC Error Current Rate is higher than the CRC Error Major Alarm Threshold.
- **Off Conditions**:
  - The CRC Error Current Rate has dropped below the CRC Error Minor/Major Alarm Threshold

    -OR-

  - All alarms were cleared

    -OR-

  - AU Alarms Option was disabled
- **Possible Problem**:
  - Receiver fault
  - Strong interference

High Duplicate Frames Rate Alarm

- Severity: Minor, Major
- **Minor Severity Alarm On Conditions**:

- The Duplicate Frames Current Rate exceeds the Duplicate Frames Minor Alarm Threshold, and is higher than the Duplicate Frames Average Rate by at least Duplicate Frames Minor Alarm Minimum Delta

  -OR-

- The Duplicate Frames Current Rate has dropped below the Duplicate Frames Major Alarm Threshold but is still higher than the Duplicate Frames Minor Alarm Threshold.

■ **Major Severity Alarm On Conditions**: The Duplicate Frames Current Rate is higher than the Duplicate Frames Major Alarm Threshold.

■ **Off Conditions**:

- The Duplicate Frames Current Rate has dropped below the Duplicate Frames Minor/Major Alarm Threshold

  -OR-

- All alarms were cleared

  -OR-

- AU Alarms Option was disabled

■ **Possible Problem**:

- Transmitter fault
- Strong interference, preventing the SU from receiving the AU's ACKs.

The AU Alarms Menu

The AU Alarms menu enables to configure relevant parameters and to view current statistics. The AU Alarms menu is available only with Administrator access rights, except for Show All AU Alarms Parameters and Data that is available also with Installer access rights.

AU Alarms Option

The AU Alarms Option parameter is used to enable or disable the AU Alarms feature.

The default is Disable.

Learning Period

The Learning Period parameter defines the period dedicated to accumulating information without generating alarms (except for the No Association Alarm).

Valid values: 1 to 1440 (minutes)

Default: 30 (minutes)

Test Cycle

The Test Cycle parameter defines the time between two consecutive transmissions of a polling message and for calculating the current averages for the various traffic statistics.

Valid values: 1 to 1440 (minutes)

Default: 10 (minutes)

Traffic Statistics

The Traffic Statistics sub menu includes the following options:

- Retransmissions Rate Parameters
- Dropped Frames Rate Parameters
- CRC Error Rate Parameters
- Duplicate Frames Rate Parameters

For each of these traffic statistics types, a sub menu enables to configure three parameters:

Minor Alarm Minimum Delta

The Minor Alarm Minimum Delta is the minimum difference between the Current Rate and the previous Average Rate, for activating a minor severity alarm, for the relevant statistics type. Another prerequisite for activating the alarm is that the relevant Current Rate exceeds the applicable Minor Alarm Threshold.

Valid range: 0 to 100 (%)

Minor Alarm Threshold

The Minor Alarm Threshold is the threshold for activating a minor severity alarm for the relevant traffic statistics type. Another prerequisite for activating the alarm is that the difference between the applicable Current Rate and the previous Average Rate exceeds the Minor Alarm Minimum Delta.

Valid range: 1 to 100 (%)

Major Alarm Threshold

The Major Alarm Threshold is the threshold for activating a major severity alarm for the relevant statistics type.

Valid range: 1 to 100 (%)

The default values for these thresholds are as follows:

Table 4-5: Default Alarm Thresholds

Parameter	Default (%)
Retransmission Minor Alarm Minimum Delta	20
Retransmission Minor Alarm Threshold	30
Retransmission Major Alarm Threshold	60
Dropped Frames Minor Alarm Minimum Delta	10
Dropped Frames Minor Alarm Threshold	10
Dropped Frames Major Alarm Threshold	20
CRC Error Minor Alarm Minimum Delta	20
CRC Error Minor Alarm Threshold	40
CRC Error Major Alarm Threshold	70
Duplicate Frames Minor Alarm Minimum Delta	5
Duplicate Frames Minor Alarm Threshold	5
Duplicate Frames Major Alarm Threshold	15

NOTE

The value of the Major Alarm Threshold must be higher than the applicable Minor Alarm Threshold. The system will not accept a Major Alarm Threshold that is lower than the current Minor Alarm Threshold, and vice versa.

Show Traffic Statistics Parameters and Data

Select this option to display for each statistics type the configured parameters as well as the applicable Current and Average Rates.

SU Rx Power Test

The SU Rx Power Test sub menu includes the following options:

SU Rx Power Decrease Threshold

The SU Rx Power Decrease Threshold is the minimum inverse (negative) value of the SU Rx Power Average Delta that will trigger an alarm.

Valid values: 1 to 99 (dBm).

Default value: 15 (dBm).

Show SU Rx Power Test Parameters and Data

Select this option to display the value of the SU Rx Power Decrease Threshold and the current SU Rx Power Average Delta.

AU Rx Power Test

The AU Rx Power Test sub menu includes the following options:

AU Rx Power Decrease Threshold

The AU Rx Power Decrease Threshold is the minimum inverse (negative) value of the AU Rx Power Average Delta that will trigger an alarm.

Valid values: 1 to 99 (dBm).

Default value: 15 (dBm).

Show AU Rx Power Test Parameters and Data

Select this option to display the value of the AU Rx Power Decrease Threshold and the current AU Rx Power Average Delta.

Responding SUs

The Responding SUs sub menu includes the following options:

Minimum Average Number Of SUs

The Minimum Average Number Of SUs parameter defines the minimum average number of SUs required for association tests.

Valid values: 1 to 254 (SUs)

Default value: 5 (SUs)

Show Responding SUs Parameters and Data

Select this option to display the value of the Minimum Average Number Of Responding SUs and the Current and Average Number Of Responding SUs.

Alarms Status

The Alarms Status sub menu includes the following options:

Clear All alarms

Select this option to clear (set off) all the AU Alarms.

Show Turned On Alarms

Select this option to display a list of all the alarms that are turned on and the severity of each of these alarms.

Show All AU Alarms Parameters and Data

Select this option to display the values of all AU Alarms parameters as well as all the current results available in Show Traffic Statistics Parameters and Data, Show SU Rx Power Test Parameters and Data, Show AU Rx Power Test Parameters and Data and Show Turned On Alarms.

Advanced Configuration Menu

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

The Advanced Configuration menu provides access to the following menus:

- IP Parameters (AU, SU and GU)
- Air Interface Parameters (AU and SU)
- Network Management Parameters (AU, SU and GU)
- Bridge Parameters (AU and SU)
- VLAN Parameters (GU)
- Performance Parameters (AU and SU)
- Service Parameters (AU and SU)
- RADIUS Parameters (SU)
- Security Parameters (AU and SU)
- Hopping Parameters (GU)
- Alarm Parameters (GU)

IP Parameters (AU, SU & GU)

The IP Parameters sub-menu allows configuration of the following parameters:

IP Address

The IP Address parameter displays the current IP address of the unit and allows the entry of a new IP address.

The default IP Address is 10.0.0.1.

Subnet Mask

The Subnet Mask parameter displays the current subnet mask of the unit and allows entry of a new subnet mask.

The default mask is 255.0.0.0.

Default Gateway Address

The Default Gateway Address parameter displays the current address of the default gateway of the unit and allows entry of a new default gateway address.

The default is 0.0.0.0.

DHCP Client

The DHCP Client sub-menu includes parameters related to acquisition of IP parameters using DHCP (Dynamic Host Configuration Protocol). It includes the following parameters:

DHCP Options

The DHCP Option parameter defines the method for acquisition of IP parameters. The available options are:

- Disable – Use manual procedure for configuring the IP parameters.
- DHCP Only – Search for a DHCP Server and obtain the IP parameters from it (IP Address, Subnet Mask and Default Gateway Address).

- Automatic – Search for a DHCP Server for configuration of the IP parameters. If a DHCP Server is not found within approximately 40 seconds, use the currently configured IP parameters.

The default is Disable.

Access to DHCP

The Access to DHCP parameter defines the port through which the unit is allowed to communicate with a DHCP server. The options are:

- From Wlan Only
- From Ethernet Only
- From Both Ethernet & WLAN

The default for an Access Unit is From Ethernet Only. The default for a Subscriber Unit is From Wlan Only.

NOTE

The Access to DHCP option is not available in the GU, as this module does not have a wireless link interface.

Show IP Parameters

Select this option to display the current values of the IP Parameters.

Air Interface Parameters (AU & SU)

Configuring Hopping Parameters

The parameters that define the hopping frequencies are:

- Hybrid Digital Modulation parameters
- Hopping Sequence (Shift)
- Hopping Sync

This section describes the functionality of these parameters and provides guidelines on how to use them for setting the hopping frequencies and applicable operation modes.

General

The process of setting the operation mode and hopping sequence includes the following steps:

1. Decide whether to enable Hybrid Digital Modulation (HDM) mode of operation. When enabled, the SU learns from the AU all the parameters that define the hopping sequence. When disabled, the same set of parameters that define the hopping sequence should be configured in the AU and in all SUs served by it.
2. Select the frequencies to be used.
3. Define the method of generating the basic hopping sequence based on the set of selected frequencies, using the Scrambling Definition sub-menu. The method of generating the basic sequence and the number of hopping frequencies also define the hopping shift mechanism for generating different actual hopping sequences.
4. If two or more non-synchronized AUs (and/or CXs) are co-located and Enhanced Scrambling is used for generating the basic sequence, configure the Spanning Factor parameter to define a different hopping sequence for each AU in order to minimize interference between adjacent AUs.
5. In a modular base station, it is recommended to synchronize the hopping mechanisms of all BS-AUs using the Hopping Sync parameter. In this case, configure the Hopping Shift parameter to define a different hopping sequence for each AU in order to minimize interference between adjacent AUs.

The HDM/Flexible Hopping Parameters menu enables defining the hopping frequencies and the method of scrambling the selected frequencies for generating the basic hopping sequence. It also enables to view the selected hopping frequencies and the current hopping sequence (based on the previous selections made before the last reset). The new selections will come into effect only after the next reset.

The default selection (including the case where all frequencies were deleted) is a single frequency, 915 MHz.

NOTE

When HDM mode is disabled, the CX/AU and all SU that that will be associated to the CX/AU must be configured to the same hopping parameters. In this mode the SU does not learn the hopping channels from the AU.

Refer to the technical bulletin, "BreezeACCESS 900 Co-location Installation Guidelines", for specific instructions on how to properly install and configure the CX and AU units for operation in environments where more than one unit will be operating.

Frequencies Selection and Basic Sequence Generation Using the HDM/Flexible Hopping Parameters Menu

The HDM/Flexible Hopping Parameters menu includes the following options:

HDM Mode (AU only)

The HDM Mode option, configurable only in AU (and CX) allows enabling or disabling Hybrid Digital Modulation mode of operation for the entire cell. When enabled, the SU learns from the AU all the parameters that define the hopping sequence. When disabled, the same set of parameters that define the hopping sequence should be configured in the AU and in all SUs served by it.

The default HDM Mode is Disable.

Define Sub-Bands

The Define Sub-Bands option enables defining a new list of sub-bands and/or discrete frequencies. Enter a list of the required sub-bands and/or frequencies, using either sub-bands (f1-f2) or discrete frequencies, e.g. 904-910,915,919-925. Use a comma to separate between entries, do not use spaces.

The usable center frequencies are from 904 to 926, using a 1 MHz resolution (904, 905, 906,...926). However, the channel spacing, which is the minimum distance between two consecutive frequencies, is 2 MHz. Thus, for example, the sequence 904,905 is not a valid entry because the distance between frequencies is less than 2 MHz, and it will be rejected.

When entering discrete frequencies, the actual center frequencies are defined. When entering a sub-ban, a guard band of 1 MHz on both sides is included, which means that the sub-band entries can start at 903 and end at 927. Defining for example the sub-band 903-909 will result in selecting the frequencies 904, 906, 908. The same set of frequencies (904, 906, 908) will be selected also if the defined sub band is 903-910. Defining the sequence 904-910,915,919-927 will result in selecting the frequencies 905, 907, 909, 915, 920, 922, 924 and 926.

The new selected set of frequencies (frequencies to be used) will become effective only after the next reset.

The default selection (including the case where all frequencies were deleted) is a single frequency, 915 MHz.

Scrambling Definitions

The Scrambling Definitions menu enables defining the method of organizing the selected frequencies to form the actual hopping sequence to be used. Proper organization of the hopping sequence is essential to guarantee minimal cross interference among several neighboring cells that use the same sequence with different Hopping Shift values.

Scrambling Mode

Defines the scrambling mode. The following options are available:

Standard Scrambling

This mode is not recommended for sequences with 7 or more channels. The scrambled basic sequences for 3 to 6 frequencies when using Standard Scrambling are:

Table 4-6: Basic Sequences using Standard Scrambling

N (number of channels)	Scrambled Basic Sequence (channel indexes)
3	1, 3, 2
4	1, 3, 2, 4
5	1, 3, 5, 2, 4
6	1, 3, 5, 2, 6, 4

Frequency 1 (index=1) is the lowest frequency in the list of frequencies to be used, frequency 2 is the next frequency and so on.

Manual Scrambling

For customized definition of the hopping sequence, using the Manual Sequence Definition option (see below).

Enhanced Scrambling

Automatically generates hopping sequences using an enhanced algorithm. If the Enhanced Scrambling Mode is selected, the Spanning Factor parameter (see below) must be configured in the AU.

The Enhanced Mode is not suitable for sequences with 6 or less frequencies. If Enhanced Scrambling is selected with sequences that have 6 or less frequencies, than Standard Scrambling is used by default.

For seven or more frequencies, the scrambled sequence is generated according to the following rules:

1. The first channel in the basic scrambled sequence is frequency 1 (Frequency 1 (index=1) is the lowest frequency in the list of frequencies to be used, frequency 2 is the next frequency and so on.)
2. The index of each of the other channels is calculated by adding the Spanning Factor to the index of the previous channel. Note that the sequence is cyclic, meaning that adding 1 to the highest index in the sequence (Index=N where N is the number of channels in the sequence) will result in the first channel (Index=1).

The scrambled basic sequence can also be calculated using the formula: P_x (j)= {[(j-1)*X]mod(N)}+1

Where:
X is the Spanning Factor
N is the number of channels in the sequence (modulus)
J is the sequence index

Example: N=8, X=3

$P_1(5)=\{[(1-1)*3\}mod8\}+1=1$

$P_2(5)=\{[(2-1)*3\}mod8\}+1=6$

$P_3(5)=\{[(3-1)*3\}mod8\}+1=3$

$P_4(5)=\{[(4-1)*3\}mod8\}+1=8$

$P_5(5)=\{[(5-1)*3\}mod8\}+1=5$

$P_6(5)=\{[(6-1)*3\}mod8\}+1=2$

$P_7(5)=\{[(7-1)*3\}mod8\}+1=7$

$P_8(5)=\{[(8-1)*3\}mod8\}+1=4$

And the basic scrambled sequence is: 1, 4, 7, 2, 5, 8, 3, 6.

Manual Sequence Definition

Manually defines the hopping sequence, using numbered channel indexes (from 1 to "Number of Hopping Frequencies"). The sequence length must be equal to "Number of Hopping Frequencies" (all the defined frequencies must be used).

Erase Manual Sequence

Erases the manually defined hopping sequence.

Spanning Factor (AU only)

Defines the Spanning Factor to be used by the Enhanced Scrambling mechanism when seven or more frequencies are used. The Spanning Factor should be chosen so that the GCD (Greater Common Divisor) of the Spanning Factor and the Number of Hopping Frequencies would be 1 (e.g. for 8 frequencies possible values for the Spanning Factor are 1, 3, 5 and 7). The SU learns the value of the Spanning Factor from the AU during the association process.

Use of different spanning factors by non-synchronized neighboring AUs and/or CXs reduces the probability of interference between adjacent sectors.

Valid values: 1 to Number of Hopping Frequencies minus 1, provided it meets the GCD requirement as described above.

It is not recommended to use spanning factors of 1 and N-1, as they result in hopping on consecutive channel (assuming that the available channels are consecutive). In these cases the advantage of using frequency hopping is not fully utilized, since narrow band interference may affect several consecutive hops. Spanning factors of 2 and N-2 also result in a relatively poor spread of the hopping frequencies over the available frequency band.

Default Value: 1

NOTE

During the association process, the SU learns the Scrambling Mode (and the Spanning Factor if applicable) of the AU. If the Scrambling Mode of the AU is different from the one configured for the SU, than after completing the association process the SU will use the Scrambling Mode of the AU.

Table C-2 displays the available spanning factors and corresponding hopping sequences for 7 to 12 channels. The recommended spanning factors are highlighted (shaded background).

Table 4-7: Spanning Factors and Hopping Sequences for Sequences with 7 to 12 Channels

Number of Channels	Spanning Factor	Hopping Sequence
7	1	1, 2, 3, 4, 5, 6, 7
	2	1, 3, 5, 7, 2, 4, 6
	3	1, 4, 7, 3, 6, 2, 5
	4	1, 5, 2, 6, 3, 7, 4
	5	1, 6, 4, 2, 7, 5, 3
	6	1, 7, 6, 5, 4, 3, 2,
8	1	1, 2, 3, 4, 5, 6, 7, 8
	3	1, 4, 7, 2, 5, 8, 3, 6
	5	1, 6, 3, 8, 5, 2, 7, 4
	7	1, 8, 7, 6, 5, 4, 3, 2,

Table 4-7: Spanning Factors and Hopping Sequences for Sequences with 7 to 12 Channels

Number of Channels	Spanning Factor	Hopping Sequence
9	1	1, 2, 3, 4, 5, 6, 7, 8, 9
	2	1, 3, 5, 7, 9, 2, 4, 6, 8
	4	1, 5, 9, 4, 8, 3, 7, 2, 6
	5	1, 6, 2, 7, 3, 8, 4, 9, 5
	7	1, 8, 6, 4, 2, 9, 7, 5, 3
	8	1, 9, 8, 7, 6, 5, 4, 3, 2
10	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10
	3	1, 4, 7, 10, 3, 6, 9, 2, 5, 8
	7	1, 8, 5, 2, 9, 6, 3, 10, 7, 4
	9	1, 10, 9, 8, 7, 6, 5, 4, 3, 2
11	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11
	2	1, 3, 5, 7, 9, 11, 2, 4, 6, 8, 10
	3	1, 4, 7, 10, 2, 5, 8, 11, 3, 6, 9
	4	1, 5, 9, 2, 6, 10, 3, 7, 11, 4, 8
	5	1, 6, 11, 5, 10, 4, 9, 3, 8, 2, 7
	6	1, 7, 2, 8, 3, 9, 4, 10, 5, 11, 6
	7	1, 8, 4, 11, 7, 3, 10, 6, 2, 9, 5
	8	1, 9, 6, 3, 11, 8, 5, 2, 10, 7, 4
	9	1, 10, 8, 6, 4, 2, 11, 9, 7, 5, 3
	10	1, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2
12	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12
	5	1, 6, 11, 4, 9, 2, 7, 12, 5, 10, 3, 8
	7	1, 8, 3, 10, 5, 12, 7, 2, 9, 4, 11, 6
	11	1, 12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2

Scan Entire Band (SU only)

When the Scan Entire Band option is enabled, the SU will scan the entire band (904 – 926 MHz) when searching for an AU. When it is disabled, only the frequencies defined by the Define Sub-Bands option will be used.

The default Scan Entire Band is Enable.

Show HDM/Flexible Hopping Parameters

Displays the following information:

- HDM Mode status (enabled or disabled)
- An updated list of the defined sub-bands and discrete frequencies to become effective after the next reset. A sub-band is defined by the first and last hopping frequency in a series of consecutive frequencies, with 2MHz separation between frequencies.
- An updated list of all the hopping frequencies to be used after the next reset.
- Scrambling Mode
- Manual Sequence Definition (if applicable)
- Spanning Factor (if applicable. In the SU it will be shown only when operating in the Enhanced Scrambling mode with 7 or more frequencies)
- The current sequence of operational hopping frequencies

Operational Hopping Sequence Definition Using the Hopping Shift Parameter

The Hopping Shift parameter is used to provide different operational hopping sequences when several co-located Access Units use the same set of hopping frequencies and the same scrambling method (and hence the same basic hopping sequence). Correct selection of different hopping shift values for adjacent AUs will minimize the cross interference among these AUs and will allow for better spectrum utilization. The Hopping Shift parameter is available only in AU-BSs. All the associated SUs learn the value of the Hopping Shift parameter from the AU during the association process.

When setting this parameter, consider the following relationship:

Max. Hopping Shift (channels) = Number of hopping frequencies-1.

The actual hopping sequences depend on the method used for defining the basic hopping sequence: Standard Scrambling, Enhanced Scrambling or Manual Sequence Definition. In Enhanced Scrambling mode it depends also on the number of frequencies.

Enhanced Scrambling mode, 7 or more frequencies:

In this mode the shift operation is performed on the channel indexes. The actual hopping channel is calculated by increasing the indexes of the basic hopping sequence by the value of the Hopping Shift. Note that the sequence is cyclic, meaning that adding 1 to the highest index in the sequence (Index=N where N is the number of channels in the sequence) will result in the first channel (Index=1).

Example: Enhanced Scrambling, N=8, Spanning Factor=3:

Table 4-8: Hopping Shift Implementation, Enhanced Scrambling (N=8, Spanning Factor=3)

Hopping Shift)	Actual Sequence Indexes
0 (basic sequence)	1, 4, 7, 2, 5, 8, 3, 6
1	2, 5, 8, 3, 6, 1, 4, 7
2	3, 6, 1, 4, 7, 2, 5, 8
3	4, 7, 2, 5, 8, 3, 6, 1
4	5, 8, 3, 6, 1, 4, 7, 2
5	6, 1, 4, 7, 2, 5, 8, 3
6	7, 2, 5, 8, 3, 6, 1, 4
7	8, 3, 6, 1, 4, 7, 2, 5

If for example the defined hopping frequencies are 904, 906, 908, 910, 912, 914, 916 and, 918, then the frequencies of the actual hopping sequences are:

Table 4-9: Actual Hopping sequences, Enhanced Scrambling (N=8, Spanning Factor=3)

Hopping Shift	Hop #1	Hop #2	Hop #3	Hop #4	Hop #5	Hop #6	Hop #7	Hop #8
0	904	910	916	906	912	918	908	914
1	906	912	918	908	914	904	910	916
2	908	914	904	910	916	906	912	918
3	910	916	906	912	918	908	914	904
4	912	918	908	914	904	910	916	906
5	914	904	910	916	906	912	918	908
6	916	906	912	918	908	914	904	910
7	918	908	914	904	910	916	906	912

The following formula can be used for calculating the actual hopping sequence:

$P_S(j)=\{[P_0(j)+S-1]\bmod(N)\}+1$

Where:

S=Hopping Shift

N=number of channels in the sequence (modulus)

$P_0(j)$=Channel no. j in the basic sequence (shift=0)

$P_S(j)$=Channel no. j in the actual sequence with hopping shift S

Example: The basic hopping sequence is 1, 4, 7, 2, 5, 8, 3, 6 (Enhanced Scrambling, N=8, Spanning Factor=3).

The actual hopping sequence for a hopping shift of 3 is:

$P_3(1)=[1+3-1]\bmod8+1=4$

$P_3(2)=[4+3-1]\bmod8+1=7$

$P_3(3)=[7+3-1]\bmod8+1=2$

$P_3(4)=[2+3-1]\bmod8+1=5$

$P_3(5)=[5+3-1]\bmod8+1=8$

$P_3(6)=[8+3-1]\bmod8+1=3$

$P_3(7)=[3+3-1]\text{mod}8+1=6$

$P_3(8)=[6+3-1]\text{mod}8+1=1$

The actual hopping sequence indexes are: 4, 7, 2, 5, 8, 3, 6, 1.

Standard and Manual Scrambling:

In these modes the shift operation is performed on the sequence elements. The basic sequence is shifted cyclically according to the value of the Hopping Shift parameter, so that element no. i in the actual sequence equals element number i+s in the basic sequence, where s is the hopping shift. Thus, if the basic sequence is a, b, c, d, e, f then a shift of 1 will result in the sequence b, c, d, e, f, a; a shift of 2 will result in the sequence c, d, e, f, a, b; and so forth.

Example: Standard Scrambling, 6 frequencies (N=6):

Table 4-10: Hopping Shift Implementation, Standard Scrambling (N=6)

Hopping Shift)	Actual Sequence Indexes
0 (basic sequence)	1, 3, 5, 2, 6, 4
1	3, 5, 2, 6, 4, 1
2	5, 2, 6, 4, 1, 3
3	2, 6, 4, 1, 3, 5
4	6, 4, 1, 3, 5, 2
5	4, 1, 3, 5, 2, 6

If the defined frequencies are 910, 912, 914, 916, 918, 920, then the frequencies of the actual hopping sequences are:

Table 4-11: Actual Hopping sequences, Standard Scrambling (N=6)

Hopping Shift	Hop #1	Hop #2	Hop #3	Hop #4	Hop #5	Hop #6
0	910	914	918	912	920	916
1	914	918	912	920	916	910
2	918	912	920	916	910	914
3	912	920	916	910	914	918
4	920	916	910	914	918	912
5	916	910	914	918	912	920

The following formula can be used to calculate the actual hopping sequence:

$P_S(i)=P_0[(i+s-1)\mathrm{mod}(N)+1]$

Where:

S is the hopping shift

N=number of channels in the sequence (modulus)

$P_S(i)$ is element number i in the actual sequence with hopping shift s

$P_0(i)$ is element number in the basic hopping sequence (s=0).

For example, in the basic sequence with N=6:

$P_0(1)=1$

$P_0(2)=3$

$P_0(3)=5$

$P_0(4)=2$

$P_0(5)=6$

$P_0(6)=4$

For a shift of 3, the actual sequence is:

$P_3(1)=P_0[(1+3-1)\mathrm{mod}6+1]=P_0(4)=2$

$P_3(2) = P_0[(2+3-1) \bmod 6+1] = P_0(5) = 6$

$P_3(3) = P_0[(3+3-1) \bmod 6+1] = P_0(6) = 4$

$P_3(4) = P_0[(4+3-1) \bmod 6+1] = P_0(1) = 1$

$P_3(5) = P_0[(5+3-1) \bmod 6+1] = P_0(2) = 3$

$P_3(6) = P_0[(6+3-1) \bmod 6+1] = P_0(3) = 5$

And the actual hopping sequence is 2, 6, 4, 1, 3, 5.

Hopping Shift Range and Default Value

The allowed range for the Hopping shift parameter is from 0 to N-1, where N is the number of hopping frequencies.

The default is 0.

Hopping Sync (BS-AU only)

The Hopping Sync parameter defines the AUs synchronization mode. When several AUs that use the same basic hopping sequence and different hopping shifts are co-located, their operation should be synchronized in terms of hopping sequence initialization and timing. If a BS-GU GPS module is not used for synchronization, then one AU must be specified as a Master unit and all other units must be specified as Slave units. When a GPS module is used, all AUs must be configured to Slave mode. Available options are:

- Idle – No synchronization (stand-alone operation)
- Master – The AU that serves as a Master unit providing synchronization signals to the Slave units
- Slave – The AU operates as a Slave, receiving synchronization signals from the master AU or from a GPS module.

The default is Idle.

ESSID Parameters

The ESSID (Extended Service Set ID) is a string used to identify a wireless network and to prevent the unintentional merging of two wireless network or two sectors in the same network. Typically, a different ESSID is defined for each 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 it 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. Once the SU has become associated with a specific AU, its ESSID can be reconfigured to the value of the ESSID of the AU.

The following ESSID parameters are available:

ESSID

The ESSID parameter defines the ESSID of the unit.

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

The default value is ESSID1.

NOTE

The ESSID string is case sensitive.

Operator ESSID Parameters (AU only)

The Operator ESSID Parameters submenu includes the following parameters:

Operator ESSID Option

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

The default is Enable.

Operator ESSID

The Operator ESSID parameter defines the Operator ESSID.

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

The default value is ESSID1.

NOTE

The Operator ESSID string is case sensitive.

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 or other factors such as number of SUs serviced by each AU. The same limitation also exists if only one AU in the neighborhood has an ESSID identical to the one used by the SU, since 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 a 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 it can communicate with. 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 done 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:

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.

Number Of Scanning Attempts

When the Best AU option is enabled, the SU gathers information on neighboring AUs for approximately 0.019 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: 20.

NOTE

When Best AU support is enabled, it is recommended to use Active Scanning. If passive scanning is used, the SU may not hear the best AU (or the preferred AU). The higher the number of hopping channels, the higher the probability that the SU will not hear the best (or preferred) AU when passive scanning is used.

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 whom 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.

Show Best AU Parameters and Data

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

- **Neighboring AU Data table**

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

  - MAC Address
  - Received signal strength (RSSI or dBm)
  - 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)
- **Run Time ESSID** (the ESSID of the selected AU).

Scanning Mode (SU only)

The Scanning Mode parameter defines whether to use Active or Passive scanning. In active scanning, the SU transmits a Probe Request upon power-up. In passive scanning, the SU searches for a Beacon message from an AU prior to starting the authentication/association process.

The default is Active

Transmit Power (SU)

The Transmit Power parameter enables to optimize the performance of the system through controlling the transmitted power level of Subscriber Units. In a Subscriber Unit that is relatively close to the Access Unit the transmitted power level of the unit should be decreased from the maximum level that is supported by the unit. The use of a lower transmit power level minimizes the interference to signals received by the AU from other subscriber units as well as interference to neighboring cells.

The range is 3-24dBm in 1dB steps.

The default is the maximum supported level, 24dBm.

Transmit Power Control (AU)

The Transmit Power Control parameter control the transmit power level in an AU.

The available options are:

- 0 (the default, 23dBm output power at the antenna port)
- 1 (24.5dBm output power at the antenna port).

NOTE

For compliance with FCC rules, the power input to the 900 MHz antenna of the AU should not exceed 23dBm. The Transmit Power Control should be set to 1 (delivering 24.5dBm power output) only when using a longer RF cable with an attenuation of 1.5dB at least, or when using an external Band-pass filter to compensate for the power loss in the filter. Such a filter may be required if the equipment is located near a very strong transmitter using frequencies that are close to the frequencies used by the BreezeACCESS equipment.

Maximum Data Rate

BreezeACCESS units operate at data rates of 3 Mbps, 2 Mbps, and 1 Mbps. Under certain conditions (compatibility reasons or range/speed trade-off), you may decide to limit the use of higher rates. If the quality of the link is not good enough, it is recommended to decrease the value of this parameter (the higher the data rate, the higher the error rate). Otherwise, there is a high probability that the unit will have to retransmit many frames several times (defined by the Number of Retransmissions to Decrease Rate parameter) before temporarily reducing the data rate. A high number of retransmissions reduces the overall throughput for the selected SU as well as for all the other SUs served by the same AU. It is recommended to also configure the Maximum Data Rate parameter when the Multi-Rate mechanism is enabled, to avoid unnecessary trials to transmit at higher rates when the probability of successful transmissions at these rates is low.

In the SU, the link quality can be estimated based on the RSSI measurement, using the assumption that the link is more or less symmetrical and that this value is a good indication to the level at which the SU is received by the AU. If the measured RSSI is less than a certain threshold, it is recommended to decrease the Maximum Data Rate of the SU in accordance with Table 4-12. The recommended threshold values in this table are based on the sensitivity for different data rates, taking into account a 3 dB safety margin. For best results it is recommended to acquire the RSSI results from the AU, indicating the level at which the AU receives transmissions from the specific SU (uplink RSSI), and to use this value for reaching a decision on the recommended Maximum Data Rate.

Allowed values are 1, 2, 3 Mbps.

The default value is 3 Mbps.

Table 4-12: Recommended Maximum Data Rate

3 Mbps	2 Mbps	1 Mbps
RSSI>-74dBm	-81dBm<RSSI<-74dBm	RSSI<-81dBm

AU Transmission Rate Control (SU only)

The AU Transmission Rate Control parameter defines whether the value of the Maximum Data Rate parameter in the SU influences the maximum rate of transmissions from the AU to this particular SU. In symmetrical links where it was determined that the Maximum Data Rate of the SU must be set to a value lower than 3 Mbps, it is recommended to also limit the maximum rate of transmissions from the AU by enabling this parameter.

The default is Disable.

Acknowledge Delay Limit

The Acknowledge Delay Limit parameter enables the user to increase the range of the system through increasing the time that the unit can wait for a response message. This includes several scenarios where the unit expects a response message, such as handshaking during association process, an acknowledgement after transmitting a data frame and CTS after RTS. Increasing the range, however, may decrease the overall performance and achievable network throughput. It should be increased only to support SUs located at distances of over 10 km from the AU. The value of the parameter for the AU must be the highest value configured for any of the SUs it serves.

Valid values are: Low (up to 10 km), Medium (up to 20 km) and High (more than 20 km).

The default setting is Low (up to 10 km).

Transmit Antenna (SU)

Antenna Diversity is not supported. The Transmit Antenna parameter must always be configured to Antenna 2.

Maximum Number of Associations

The Maximum Number of Associations parameter defines the upper limit for the number of Subscriber Units that can be associated with the AU, in order to guarantee the required quality of service to the customers.

Valid values: 0-512.

Default value: 512.

NOTE

There is no aging time for SUs. An SU will be removed from the list of associated SUs only upon occurrence of any of the following:
(1) The AU received from another AU a SNAP frame with the SU MAC address indicating that the SU has become associated with the other AU, or
(2) The AU has decided that the SU aged out following its failure to acknowledge a certain number of consecutive frames transmitted to it.
Thus, the database of associated SUs may include units that are no longer associated with the AU. If the number of associated SUs has reached the value of the Maximum Number of Associations parameter, additional SUs can not be served by this AU. To view the current number of associated SUs, use the Display Association Info option in the MAC Address Database menu. To delete entries of SUs that are no longer active, the AU must be reset.

MAC Address Black List (AU only)

The MAC Address Black List feature 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 black 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 black list can include up to 100 MAC Addresses.

The MAC Address Black List sub-menu includes the following options:

- Add MAC Address to Black List - To add a MAC Address to the Black List.
- Remove MAC Address from Black List - To remove a MAC Address from the Black List.
- Show MAC Address Black List - To display the current list of MAC Addresses included in the black list.

Wireless Trap Threshold

The Wireless Trap Threshold parameter defines the threshold for the wireless quality traps: The brzaccAUWirelessQualityTRAP or the brzaccSUWirelessQualityTRAP. These traps indicate that the quality of the wireless link has gone below or above the specified threshold.

For AU the threshold is in percents of retransmissions. For SU the threshold indicates the level of the received signal and is in RSSI units, indicating the quality of the received signal. Refer to Appendix D - RSSI to dBm Conversion for details on converting RSSI to dBm and vice versa.

Default values:

AU: 30 (%)

SU-I: 45 (RSSI units), which is equivalent to –87dBm.

Send Roaming SNAP (SU only)

The Send Roaming SNAP feature is applicable primarily to mobile units that can roam among AUs. The feature enables fast distribution of the new location for all clients that are behind the SU.

When enabled, the SU will send multicast SNAP messages via the wireless link each time it associates with an AU, except to 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 selection is Disable.

Network Management Parameters (AU, SU & GU)

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

The Network Management Parameters menu includes the following options:

Access to Network Management (AU & SU)

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

- From WlanOnly
- From Ethernet Only
- From Both Ethernet & Wlan

The default selection is From Both Ethernet & Wlan.

NOTE

The Access to Network Management option is not available in the GU, as this module does not have a wireless link interface.

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.

Network Management Filtering

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

- **Disable:** No IP address based filtering is configured.
- **Activate Management 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 Management IP Filter on Wlan 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 Management IP filter on Both Ethernet & Wlan 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.

NOTE

In the GU only the Disable and Activate Management IP Filtering on Ethernet Port options are available.

Set Network Management IP Address

The Set Network Management IP Address option enables defining up to 3 IP addresses of devices that can manage the unit if the Network Management Filtering option is enabled.

The default Network Management IP Address is 0.0.0.0 (all 3 addresses)

Delete a Network Management IP Address

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

Delete All Network Management IP Addresses

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

SNMP Traps

The SNMP Traps submenu enables to control the transmission of all or selected traps. It also enables to define up to 3 destination addresses and SNMP communities for the traps.

The SNMP Traps sub-menu includes the following options:

Traps Control

The Traps Control sub-menu enables to control the transmission of traps. It includes the following options:

Send SNMP Traps

The Send SNMP Traps option enables to control whether the unit will send traps or not. The available options are:

- Enable Traps Sending - enables sending of SNMP traps. The traps that will be sent can be defined by the Per Trap Control menu. The addresses to which these traps will be sent and the SNMP Communities associated with these traps are defined by the SNMP Traps IP Destination and the SNMP Traps Community options.

- Disable Traps Sending - no SNMP traps will be sent by the unit.

The default selection is Disable Traps Sending.

Per Trap Control

When SNMP Traps Sending is enabled, the Per Trap Control sub-menu allows defining for each individual trap whether it will be transmitted or not. The traps that can be controlled and the default option for each Trap are detailed in the following table:

Table 4-13: Per Trap Control Parameters

Parameter	Unit Type	Default
Send SU Associated AU Trap	AU	Enable Trap Sending
Send Disassociated Trap	AU	Enable Trap Sending
Send AU Aging Trap	AU	Enable Trap Sending
Send AU Wireless Quality Trap	AU	Enable Trap Sending
Send SU Associated Trap	SU	Enable Trap Sending
Send SU Wireless Quality Trap	SU	Enable Trap Sending
Send Parameter Changed Trap	AU, SU	Enable Trap Sending
Send GPS Alarm In Trap	GU	Enable Trap Sending
Send GPS Alarm Out Trap	GU	Enable Trap Sending
Send UTC Status Trap	GU	Enable Trap Sending
Send Power Up From Reset Trap	All	AU, GU: Enable Trap Sending SU: Disable Trap Sending
Send Monitor Status Trap	All	Enable Trap Sending
Send Cold \ Warm Start Trap	All	AU, GU: Enable Trap Sending SU: Disable Trap Sending
Send AU Loss Of Sync Trap	BS-AU in slave mode	Enable Trap Sending
Send AU Alarms Traps	AU	Enable Traps Sending (all AU Alarms Traps)
Send Ethernet Broadcast Limiter Trap	AU, SU	Disable Trap Sending

SNMP Traps Destination IP Addresses

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

The default of all 3 SNMP Traps IP destinations is 0.0.0.0.

SNMP Traps Community

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

Valid strings: Up to 14 ASCII characters.

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

Delete One Trap Address

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

Delete All Trap Addresses

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

Bridge Parameters (AU, SU & GU)

The Bridge Parameters menu provides a series of parameters that enables configuring features such as VLAN support, control and filtering options, forwarding and relaying policies, and Type of Service prioritization.

VLAN Support

The VLAN Support menu enables defining the parameters related to the IEEE 802.1Q compliant VLAN aware (Virtual LAN aware) feature of the BreezeACCESS 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 units supports frame routing by port information, whereby each port is connected to only one VLAN.

The VLAN Support menu enables configuring the following parameters:

VLAN ID-Data (SU only)

The VLAN ID-Data is applicable for Access Links only. It enables defining the VLAN ID for data frames, which identifies the VLAN to which the unit belongs.

Valid values range from 1 to 4094.

Default value: 1.

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

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

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

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

VLAN ID-Management (AU, SU & GU)

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, RADIUS 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 4-14: VLAN Management Port Functionality

Action	Management Port - Internal
Receive from Ethernet	Tagged frames, matching VID-M Untagged frames when VID-M=65535
Receive from Wireless	Tagged frames, matching VID-M Untagged frames when VID-M=65535
Transmit	Insert VID-M, PID-M

Table Legend:

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

VLAN Link Type (AU, SU & GU)

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.

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 4-15 summarizes the functionality of the data port for an Access link.

Table 4-15: 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

Trunk Link

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

CAUTION

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

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

NOTE

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

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 4-16 summarizes the functionality of the data port for a Trunk link.

Table 4-16: 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

Hybrid Link

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

Table 4-17 summarizes the functionality of the data port for a Hybrid link.

Table 4-17: 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

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:

VLAN Forwarding Support

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

Available selections are Disable and Enable.

The default selection is Disable.

Add Forwarding VLAN ID

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

Valid values are 1 to 4094.

Remove Forwarding VLAN ID

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

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

Show VLAN ID Forwarding List

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

NOTE

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

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

VLAN 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:

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.

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.

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.

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.

VLAN Traffic Priority

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

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

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

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

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

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

Any frame coming from the Ethernet port, which is meant to reach another BreezeACCESS unit via the wireless port, is sent to the High queue, regardless of the priority configuration.

The VLAN Traffic Priority menu provides the following parameters:

VLAN Priority - Data (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 that other VLAN aware devices handle the packet.

Valid values range from 0 to 7.

The default value is 0.

NOTE

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

VLAN Priority - Management (AU, SU & GU)

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

Valid values range from 0 to 7.

The default value is 0.

VLAN Priority Threshold (AU & SU)

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

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

- The precedence in the ToS field is higher than the value of the ToS Precedence Threshold parameter. This is applicable to both tagged and untagged frames.
- The VLAN Priority field in a tagged frame is higher than the value of the VLAN Priority Threshold parameter.

Valid values range from 0 to 7.

The default value is 4.

Show VLAN Parameters

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

ToS Parameters

ToS Precedence Threshold (AU & SU)

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

- The precedence in the ToS field is higher than the value of the ToS Precedence Threshold parameter. This is applicable to both tagged and untagged frames.
- The VLAN Priority field in a tagged frame (Hybrid or Trunk Link) is higher than the value of the VLAN Priority Threshold parameter.

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

Valid values are 0 to 7.

The default value is 3.

NOTE

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

Ethernet Broadcast Filtering

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

The 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 media 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. In case that the Ethernet filters of the SU are disabled, the limiter will be applied to all relevant packets received.

When the Ethernet Broadcast Limiter is enabled and the 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 Broadcasting Filtering menu allows viewing and setting the following parameters:

Filter Options (SU)

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

- **Disable**, which means no Ethernet Broadcast Filtering.
- **From Ethernet Only**, which filters broadcast messages received from the Ethernet port.
- **From WlanOnly**, which filters broadcast messages received from the wireless link port.
- **Both from Ethernet & Wlan**, which filters broadcast messages received from both the Ethernet and wireless link ports.

The default selection is Disable.

DHCP Broadcast Override Filter (SU)

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

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

The default selection is Disable.

PPPoE Broadcast Override Filter (SU)

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

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

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

The default selection is Disable.

ARP Broadcast Override Filter (SU)

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

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

The default selection is Enable.

Ethernet Broadcast/Multicast Limiter Option (AU & SU)

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.

Ethernet Broadcast Limiter Threshold (AU & SU)

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

The range is from 0 to 20480 (packets/second).

The default is 20480.

LAN to Wireless Link Bridging Mode (AU)

The LAN to Wireless Link Bridging Mode option controls the flow of information from the Ethernet backbone to the wireless media. The options are:

- **Reject Unknown** – Allows transmission of packets only to addresses that the AU knows to exist in the wireless link.
- **Forward Unknown** – Allows transmission of all packets, except those sent to addresses that the AU recognizes as being on its wired Ethernet side.

The default selection is Forward Unknown.

Bridge Aging Time (AU & SU)

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

The available range is 100 to 2000 seconds.

The default value is 300 seconds for AU and 1800 seconds for SU.

Broadcast Relaying (AU)

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.

Unicast Relaying (AU)

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.

Ports Control (SU)

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

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 may still be managed via the Ethernet port even when it is disabled for data traffic.

The default selection is Enable.

Performance Parameters (AU & SU)

The Performance Parameters menu includes parameters that control the method by which traffic is transmitted through the BreezeACCESS wireless access network. It includes the following parameters:

RTS Threshold

The RTS Threshold defines the minimal packet size to require RTS/CTS (Request To Send/Clear To Send) handshake. Packets with a size below 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 will prevent the RTS/CTS handshake for packets transmitted by this unit.

The allowed range is from 20 to 1600.

The default value is 60 bytes for SUs and 1600 for AUs. Using a value of 1600 for the AU ensures that it will never use the RTS/CTS mechanism.

Number of Retransmissions

The Number of Retransmissions parameter defines the maximum number of times that a packet that was not acknowledged will be retransmitted.

Valid values are from 0 (no retransmissions) to 100.

The default value is 1.

Number of Dwells to Retransmit

The Number of Dwells to Retransmit parameter defines the minimum number of dwell periods during which a packets can be retransmitted. The Number of Dwells to Retransmit parameter is used together with the Number of Retransmissions parameter (see above) to spread the retransmissions in both the time and frequency domains.

Valid values are from 0 to 9.

The default value is 2.

Number of Retransmissions to Decrease Rate

The Number of Retransmissions to Decrease Rate parameter defines number of unsuccessful retransmissions that will cause an automatic decrease in the data rate before the next retransmission (the lower the data rate, the higher the probability that the packet will be properly received and acknowledged). The count is reset each time the rate is reduced, meaning that at each rate the maximum number of transmission attempts equals the value of this parameter plus 1.

Valid values are from 0 to 10.

The default value is 0, meaning that the rate will be decreased immediately following an unsuccessful transmission attempt at the each rate.

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 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 media resulting from attempts of more than one unit to transmit at the same time.

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 after reaching a decision that the medium has become free.

The system uses an exponential back-off algorithm to resolve contention between several units that want to access the wireless media. 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 media. The unit will attempt to access the media only after a certain minimum time (DIFS) plus N time slots, always checking if a different unit has accessed the media before. Each time the unit tried to transmit and a collision happened; the maximum number C used for the random number selection will be increased to the next available value. The available values for C 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 Valid values are from 7 to 255.

The default value is 31.

Maximum Multicast Rate (AU)

The Maximum Multicast Rate parameter defines the maximum rate of multicast and broadcast transmissions. Multicast and broadcast transmissions are not acknowledged; therefore there is a chance that such transmissions will not be properly received without the possibility of using the acknowledgement mechanism for retransmission. Therefore, it is recommended to use a lower rate for transmission of broadcast, multicast and control frames, to increase the probability that they will be received without errors.

The available selections are 1, 2, and 3 Mbps.

The default is the minimum possible rate, 1Mbps.

Multi-Rate

Link quality dynamically changes, due to various environmental conditions. Dynamically switching between the possible transmission rates increases the probability of using the maximum rate for the current radio link quality at any given moment. Decreasing the rate one step improves the receiver sensitivity by 6-8dB. When enabled, the transmission rate decisions are made separately for each unit. This algorithm, which control the rate for the first transmission trial of each packet, is completely separated from the retransmission mechanism defined by Number of Retransmission and Number of Dwells to Retransmit parameters. The algorithm provides Access Units with simultaneous, adaptive support for multiple Subscriber Units at different rates.

The decision on the rate of each transmission (first attempt) is based on counting transmissions, retransmissions and successful windows. A window is defined as N consecutive transmission or retransmission attempts, defined by the Multi-Rate Decision Window Size parameter. A successful window is a window in which the number of failed transmissions is not higher than a defined threshold. A transmission is defined as failed if an ACK was not received after the first transmission of a frame. If the current rate is lower than the maximum available rate, the transmission rate will be increased to the next available rate following a number of successful windows. In order to minimize fluctuations, the number of successful windows at a certain rate required to reach a decision to increase the rate depends on previous rate of unsuccessful windows at the higher rate. The higher the rate of previous unsuccessful windows at a specific rate, the higher is the number of required consecutive successful windows at the lower rate prior to increasing the rate. If the current rate is higher than the minimum available rate (1 Mbps), the transmission rate will be decreased to the next available rate following a failed window.

The Multi-Rate menu includes the following parameters:

Multi-Rate Support

The Multi-Rate Support option enables or disables the Multi-Rate decision algorithm. When enabled, the algorithm supports increase/decrease of transmission rates in the range from 1 Mbps to the current value of the Maximum Data Rate parameter. (enabling the algorithm has no effect if the Maximum Data Rate is 1 Mbps).

The default selection is Enable.

Multi-Rate Decision Window Size

The Multi-Rate Decision Window Size parameter sets the size of the decision window. The size of a window is measured as the number of consecutive transmission or retransmission attempts. Increasing the size of the window will increase the probability that it will be a successful window, thus slowing down the decision to degrade to a lower rate and accelerating the decision to upgrade to a higher rate.

Valid values are from 1 to 50.

The default value is 12.

Number of Failures in Multi-Rate Decision Window

The Number of Failures in Multi-Rate Decision Window parameter sets the maximum number of failures allowed in a decision window. A window is defined as successful only if the number of failures is not higher than this number. A transmission attempt is defined as a failure if an ACK was not received upon the first transmission attempt. Increasing the value of this parameter will increase the probability that it will be a successful window, thus slowing down the decision to degrade to a lower rate and accelerating the decision to upgrade to a higher rate.

Valid value: 1 to Multi-Rate Decision Window Size.

Default value: 8.

Dwell Time (AU)

Dwell Time is the time spent on a radio channel before hopping to the next channel according to the operational hopping sequence.

The allowed selections are 32, 64 and 128 Kilo-microseconds (1 Kilo-microseconds=1024 microseconds).

The default value is 128 Kilo-microseconds.

Interference Avoidance Parameters

The Interference Avoidance parameters include the following parameters:

- Noise Floor
- Carrier to Interference Difference Level
- Carrier Sense Level

■ Adaptive Thresholds Parameters

These parameters enable to define the interference avoidance algorithm. The algorithm is designed to minimize the probability of the modem identifying interference as a possible desired signal. Such an occurrence should be avoided, as locking on the interfering signal may disable the modem from timely identifying the appearance of a desired signal.

Setting a certain level as a threshold below which signal are considered as interference is not sufficient, since the energy in the relevant spectrum of interfering signals may temporarily be well above the threshold level. On the other hand, setting the threshold at a higher level to overcome the effect of temporary occurrences of high-level interferences is not a good solution, as it may cause the unit to reject desired signals. The solution is a dynamic decision algorithm that will follow temporary high-level interferences and adjust the decision threshold accordingly.

The algorithm for identifying transmissions of messages initiated by another unit includes two settable parameters: Noise Floor and Carrier to Interference Difference Level.

The Noise Floor parameter represents the equivalent noise level in the neighborhood of the unit, including both the thermal noise and average level of interference in the relevant spectrum.

Carrier to Interference Difference Level is the minimal difference between the level that is defined as the Current Noise Level and the level of a “good” signal (a signal that the unit should treat as a possibly desired signal).

The modem of the unit continuously estimates the level of the received energy at the relevant spectrum. The Current Noise Floor is defined as follows:

If the last estimated energy level was lower than or equal to the Noise Floor, then the Current Noise Floor is equal to the Noise Floor.

If the last estimated level was above the Noise Floor, it can be either interference or a possibly “good” signal. If it is lower than the last Current Noise Floor, or if the difference from the last Current Noise Floor is less than the Carrier to Interference Difference Level, it shall be considered as interference and it becomes the updated Current Noise Floor.

Carrier to Interference Difference Level is the minimal difference between the Current Noise Floor and the level of a signal that will be defined as a “good” one. This means that the actual threshold to be used for decision on the existence of a valid signal is the higher of the two following:

a. Carrier Sense Level

b. “Current Noise Floor” + Carrier to Interference Difference Level.

This algorithm allows the unit to identify and track temporary high level interference and to adjust the decision threshold accordingly.

Noise Floor

The Noise Floor parameter defines the equivalent noise level that is affected by the thermal noise and the average interference level.

Available values: -115 to –50 (dBm).

The default values are -112dBm for AU and -105dBm for SU.

Carrier to Interference Difference Level

The Carrier to Interference Difference Level parameter defines the minimal difference between the Current Noise Floor and a “good” signal. In environment where there is a high probability that the level of interfering signals may temporarily increase significantly above the average level, this parameter should be set to a higher value.

Valid values: 6 to 60 (dB)

The default values are 8dB for AU and 9dB for SU.

Carrier Sense Level

The Carrier Sense Level parameter defines the threshold level that is used prior to initiating a transmission by the unit to determine the existence of transmission from another unit. As long as the level of a received signal is above this threshold, the unit will assume that another unit is transmitting and will refrain from trying to transmit in order to prevent collisions.

The actual level used by the SU as a threshold for decision on the existence of a “good” signal (Runtime Carrier Sense Level) may differ from the configured Carrier Sense Level, as described in the Adaptive Thresholds section below.

Available values: -100 to -40 (dBm)

The default values are –90dBm for AU and –85dBm for SU.

Adaptive Thresholds Parameters (SU only)

The interference avoidance algorithm described above adjusts dynamically the "Current Noise Level" to adapt to relatively fast changes in the environment. The adaptive thresholds algorithm enables improved rejection of interference in the SU units, in varied noisy environments. On receiving, it reduces the number of erroneously detected packets that are actually just noise ("bad packets"). On transmitting, it provides a more accurate carrier sense, therefore lowering erroneous collision detection. The algorithm changes the actual level that is used as the Noise Floor, by adapting to actual levels of received "good" signals. When the Adaptive Threshold algorithm is enabled, then the Runtime Noise Floor is the higher of the following two values:

a. The configured Noise Floor.

b. Calculated Noise Floor: Average RSSI[dBm] – Delta - Fading Factor – 2dB.

Where Delta is a hard coded value that may differ among product types. Fading Factor is a configurable parameter as described below.

The Runtime Carrier Sense Level, will be the higher of:

a. Carrier Sense Level

b. Calculated Noise Floor as defined above (Average RSSI[dBm] – Delta - Fading Factor – 2dB) + Carrier to Interference Difference Level.

The Adaptive Thresholds menu includes the following parameters:

Adaptive Thresholds Option

The Adaptive Thresholds Option is used to enable or disable the adaptive thresholds algorithm.

The default is Disable

Adaptive Thresholds Period

The Adaptive Thresholds Period parameter defines the interval between consecutive updates of the runtime values when the adaptive threshold algorithm is enabled.

Valid values: 1-60 seconds

The default is 15 seconds

Adaptive Thresholds Fading Factor

The Adaptive Thresholds Fading Factor parameter defines the Fading Factor to be used in the formula for calculating the Runtime Noise Floor. The higher the expected variance in levels of received signal, the higher this value should be.

Valid values: 0-70 dB

The default is 10 dB

Service Parameters (AU & SU)

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

The Service Parameters menu includes the following parameters:

User Filtering Parameters (SU only)

The User Filtering Parameters sub-menu defines IP addresses of user's devices that are authorized to access the wireless media, serving for security and/or control purposes. It can also be used to enable transmission/reception of specific protocol frames only. These filtering functions do not affect management frames that are sent to or generated by the unit or.

The User Filtering Parameters sub-menu includes the following parameters and options:

User Filtering Option

The User Filtering Option is used to disable or enable the User Filtering feature. The available options are:

- **Disable** (No filtering).
- **IP Only** (only IP Protocol packets pass).
- **User Defined Addresses Only** (only IP messages from/to IP addresses included in the User Filter Addresses list pass).
- **PPPoE Protocol Only** (only PPPoE frames pass - Ethernet type 0x8863 and 0x8864).

The default selection is Disable.

Set User Filter Address

The Set User Filter Address option enables defining up to 8 IP addresses to be used if the User Defined Addresses Only option was selected in the User Filtering Option above.

The default for all addresses is 0.0.0.0.

Set User Filter Mask

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

The default for all subnet masks is 255.0.0.0.

Set User Filter Range

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

Valid values: 0 – 255.

The default value is 0 (not used).

NOTE

You may use either Mask or Range (but not both) to define a group of user filter addresses. If the range is other than 0, than the mask is ignored.

If IP broadcast packets should reach the devices connected behind the SU unit, the Broadcast IP address should be included in the configured User Filter Address entries.

Delete a User Filtering Entry

The Delete a User Filtering Entry option displays the current list of IP addresses, subnet masks and ranges. Enter the list number (from 0 to 7) to delete the entry from the list (the list number will be replaced by the default values).

Delete All User Filtering Entries

Select this option to delete all User Filtering entries (and replaces them with the default values).

MIR and CIR Parameters

The CIR (Committed Information Rate) value specifies the minimum data rate guaranteed to the applicable 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) will be between the applicable CIR and MIR values: IR=CIR+K(MIR-CIR), where K is between 0 to 1 and is determined dynamically by the AU according to overall demand in the cell and the prevailing conditions that may influence the performance of the wireless link. In some situations the minimum rate (CIR) cannot be provided. This may occur as a result of high demand and poor wireless link conditions and/or high demand in cells with over subscription (total CIR higher than 1600Kbps). When this happens, actual information rate will be lower than CIR. The simple solution for managing information rate in such cases results in an unfair allocation of resources, as subscribers with higher CIR can actually get an IR lower than that given to subscribers with lower CIR. A special algorithm for graceful degradation has been incorporated into the AU, ensuring that the degradation of performance for each individual subscriber will be proportional to its CIR.

The MIR/CIR algorithm uses buffers to control the flow of data. To average the performance over time, a special Burst Duration algorithm is employed to enable higher transmission rates after a period of inactivity. If no data was 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 an inactivity time of 0.5 second, a unit with CIR = 64 Kbps can transmit up to 64 Kbits x 0.5 = 32 Kbits without any delay.

The MIR and CIR Parameters sub-menu includes the following parameters and options:

MIR/CIR Option

The MIR/CIR Option enables or disables the CIR/MIR support feature. The MIR/CIR Option in the AU controls the operation of the whole cell. The MIR/CIR Option in the SU is thus meaningless, as the setting of the option in the AU will override possible conflicting setting in any of the served SUs. The option is available in the SUs only for compatibility with previous versions.

Default selection is Disable.

MIR: AU to SU (SU only)

The MIR: AU to SU parameter sets the Maximum Information Rate of the down-link from the AU to the SU. The MIR value cannot be lower than the corresponding CIR value.

Valid values are from 32 to 2200 Kbps.

The default value is 128 Kbps.

MIR: SU to AU (SU only)

The MIR: AU to SU parameter 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.

Valid values are from 32 to 2200Kbps.

The default value is 128Kbps.

CIR: AU to SU (SU only)

The CIR: AU to SU parameter sets the Committed Information Rate of the down-link from the AU to the SU. The CIR value cannot be higher than the corresponding MIR value.

Valid values are from 0 to 2200Kbps.

The default value is 64Kbps.

CIR: SU to AU (SU only)

The CIR: AU to SU parameter sets the Committed Information Rate of the up-link from the SU to the AU. The CIR value cannot be higher than the corresponding MIR value.

Valid values are from 0 to 2200Kbps.

The default value is 64Kbps.

NOTE

The value of the MIR must be higher than the value of the applicable CIR. The system will not accept a MIR value that is lower than the current CIR value, and vice versa.

Maximum Burst Duration (SU & AU)

The Maximum Burst Duration parameter sets the maximum time for accumulating burst transmission rights according to the Burst Duration algorithm.

Valid values: 0 – 2000 (milliseconds).

Default value: 5 (milliseconds), allowing a maximum burst of (0.005 X CIR) Kbps, after an inactivity period of 5 milliseconds or more.

Maximum Delay (SU only)

The Maximum Delay parameter sets the maximum permitted delay in the buffers system. Some applications are very sensitive to delay. If relatively high delays are permitted, such applications may suffer from poor performance due to accumulation in the buffers of data from other applications (e.g. FTP). The Maximum Delay parameter limits the number of available buffers. Data that is delayed more than the permitted maximum delay will be discarded. If the SU should support applications that are very sensitive to delay, the value of the Maximum Delay should be decreased.

Valid values: 300 – 10000 (milliseconds).

Default value: 5000 (milliseconds).

Graceful Degradation Limit (AU only)

The Graceful Degradation Limit parameter sets the limit on using the graceful degradation algorithm. In cases of over demand, the performance of all SUs will be degraded proportionally to their CIR (IR=(100%-k%) x CIR). The graceful degradation algorithm will be used as long as k £ K, where K is the Graceful Degradation Limit. Beyond this point the simple “brute force” algorithm will be used. The higher is the expected over demand in a cell, the higher should be 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 that do not enable proper communication with the AU at the highest data rate.

Valid values: 0 – 70 (%).

Default value: 70 (%).

Mir Only Option (AU only)

The Mir Only Option enables or disables the feature of forcing 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 demand conditions, based on the configured CIR and MIR values. When the Mir Only Option is enabled, the MIR/CIR algorithm is overridden and is forced to operate with MIR values only (e.g. 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 Disable.

RADIUS Parameters (SU only)

Managing a large number of users creates the need for significant administrative support together with careful attention to security, authorization and accounting. The use of RADIUS (Remote Authentication Dial In User Service) enables operators to manage a single "database" of users, supporting authentication (verifying user name and password) as well as configuration information detailing the type of service to deliver to the user and the traffic that the user transmitted and received, for billing proposes.

The RADIUS is a protocol for carrying authentication, authorization, and configuration information between a Network Access Server, which desires to authenticate its links and a shared Authentication server. A Network Access Server (NAS) operates as a client of RADIUS. The client is responsible for passing user information to designated RADIUS servers, and then acting on the response. RADIUS servers are responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver service to the user.

Transactions between the client and RADIUS server are authenticated through the use of a shared secret, which is never sent over the network. In addition, any user passwords are sent encrypted between the client and RADIUS server, using a method based on the RSA Message Digest Algorithm MD5.

The Access-Request is submitted to the RADIUS server via the network. If no response is returned within a length of time, the request is re-sent a number of times. Once the RADIUS server receives the request, it validates the sending client. A request from a client for which the RADIUS server does not have a shared secret must be silently discarded. If the client is valid, the RADIUS server consults a database of users to find the user whose name matches the request. The user entry in the database contains a list of requirements that must be met to allow access for the user. This always includes verification of the password, but can also specify the client(s) or port(s) to which the user is allowed access.

In the BreezeACCESS system there is a RADIUS NAS (Network Access Server) implemented in each Subscriber Unit. The RADIUS server can be used for authentication purposes only, for accounting purposes only, or for both authentication and accounting purposes.

The RADIUS Parameters menu includes three sub-menus:

a. General RADIUS Parameters – intended for all users of RADIUS.

b. Authentication Parameters.

c. Accounting Parameters.

NOTE

Different servers may be used for authentication and for accounting.

General RADIUS Parameters Menu

The General RADIUS Parameters menu is used to define general RADIUS parameters that must be configured by all SUs to be served by a RADIUS server, either for authentication only, for accounting only, or for both authentication and accounting.

User Name

The User Name defines the user name that will be used by the RADIUS server to identify the SU.

Valid values: A string of up to 64 printable ASCII characters, case sensitive.

Default value: The unit's MAC Address

User Password

The User Password defines the password to be used by the RADIUS server to confirm the identity of the SU.

Valid values: A string of up to 64 printable ASCII characters, case sensitive.

Default value: RadiusPassword1.

Shared Secret

The Shared Secret defines the key that will be used for encrypting the User Password for increased security. The algorithm used for encrypting the User Password is MD5.

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

Default value: RadiusSecret1234.

Authentication Parameters Menu

The implementation is based on RFC 2865. The mechanism allows an SU to synchronize and associate to its AU, then request authentication from the RADIUS server. Only if the authentication is successful the user will receive services (data and voice). It is then possible to download from a remote server the full unit services configuration (CIR/MIR, Telephone number etc.). If the authentication is not successful, the data and voice ports of the SU will be blocked.

Authentication Option

The Authentication Option enables or disables the use of RADIUS for authentication. When this option is enabled and the RADIUS Server Authentication IP Address is configured to an address other than 0.0.0.0, the SU enables the RADIUS authentication feature.

Default selection: Disable

RADIUS Server Authentication IP Address

The RADIUS Server Authentication IP Address parameter defines the IP address of the RADIUS server to be used for authentication.

The default address is 0.0.0.0 (none).

RADIUS Server Authentication Port

The RADIUS Server Authentication Port parameter specifies the UDP port number used by the Radius server for authenticating the clients.

Valid values: 1000 to 65535.

The default value is 1812 (RFC requirement).

Show Authentication Parameters and Status

Select this option to display the Authentication parameters and the current status. The status can be Idle, Sending Request, Waiting For Response, Sending Challenge, Authenticated or Rejected.

Accounting Parameters Menu

If the Accounting Option is enabled, then every period defined by the service provider (Accounting Interval) the NAS (SU) will update the Radius Accounting Server with the traffic passed through it during the period. From the Radius Server point of view this period is a session in accordance with the RFC 2866 definitions. The information is sent to the Radius Server using the standard Radius attributes. The record structure is described in RADIUS Record Structure, page 2-93.

The Accounting Parameters menu allows enabling the RADIUS client embedded in the Subscriber Unit and configuring the parameters that control the transmission of accounting records to a RADIUS billing server. The Accounting Parameters menu includes the following parameters:

Accounting Option

The Accounting Option enables or disables the accounting records transmission feature. When this option is enabled and the RADIUS Server Accounting IP Address is configured to an address other than 0.0.0.0., the SU enables the RADIUS accounting client.

The default is Disable.

RADIUS Server Accounting IP Address

The RADIUS Server Accounting IP Address parameter defines the IP address of the RADIUS server to be used for accounting.

The default address is 0.0.0.0 (none).

RADIUS Server Accounting Port

The RADIUS Server Accounting Port parameter specifies the UDP port number used by the Radius server for accounting.

Valid values are 1000 to 65535.

The default value is 1813 (RFC requirement).

Accounting Interval

The Accounting Interval defines the interval in seconds between two consecutive transmissions of accounting records.

Valid values are from 60 to 6000 seconds (1 to 100 minutes).

The default value is 90 seconds.

Show Accounting Parameters

Select this option to displays the current values of the Accounting parameters.

RADIUS Record Structure

Each RADIUS Accounting message includes a Session ID and up to 11 Ethernet Specific records. A space is used to separate fields from each other.

Table 4-18: Session ID Record Structure

Field	Format	Description
Unit Name	16 ASCII characters (no nulls).	The Unit name
Unit MAC Address	xx-xx-xx-xx-xx-xx (hex format)	The IEEE MAC address of the SU.
Message ID	4 hex digits	The Message ID
Reset Counters	2 hex digits (0-99)	The number of resets since power-up of the unit.

Table 4-19: Ethernet Vendor Specific Record Structure (Vendor Specific ID is 710)

Field	Format	Description
Traffic Type	1 hexadecimal digit	Data (0)/Management (1)/Voice (2)
VLAN ID	3 hexadecimal digits	VLAN ID
Layer 3 Protoco	4 hexadecimal digits	Third layer protocol type (IP, ARP..)
Remote IP Address	xxx.xxx.xxx.xxx (decimal format)	The remote IP Address
IP Type Of Service	2 hexadecimal digits	Precedence/ Delay/ Throughput/ Reliability
VLAN Priority	1 hexadecimal digit	VLAN Priority

Table 4-19: Ethernet Vendor Specific Record Structure (Vendor Specific ID is 710)

Field	Format	Description
ETH Output Octets	8 hexadecimal characters	Number of octets successfully transmitted to Ethernet
ETH Input Octets	8 hexadecimal characters	Number of octets received from Ethernet
ETH Output Packets	8 hexadecimal characters	Number of packets successfully transmitted to Ethernet
ETH Input Packets	8 hexadecimal characters	Number of packets received from Ethernet
WLAN Output Octets	8 hexadecimal characters	Number of octets successfully transmitted to Wireless
WLAN Input Octets	8 hexadecimal characters	Number of octets received from Wireless.
WLAN Output Packets	8 hexadecimal characters	Number of packets successfully transmitted to Wireless
WLAN Input Packets	8 hexadecimal characters	Number of packets received from Wireless

Security Parameters (AU & SU)

Preventing Unauthorized Access

Unauthorized wireless connection is prevented by using the Wired Equivalent Privacy (WEP) algorithm defined in the IEEE 802.11 Wireless LAN standard. The WEP is based on RSA's RC4 encryption algorithm. The following parameters are available in the Security Parameters menu:

Authentication Algorithm

The Authentication Algorithm parameter defines the operation mode of the unit. The available options are:

- **Open System**: An SU configured to Open System can be authenticated only by an AU that is also configured to Open System. The WEP algorithm is not used.
- **Shared Key**: Authentication enabled. The authentication messages are encrypted. An SU configured to use Shared Key can be authenticated only by an AU configured to use Shared Key, provided they both use the same WEP Key. Both the WEP Key number and the WEP Key should be identical at both sides of the link.
- **Support All** (AU only): The AU authenticates all SUs, regardless of the Authentication Algorithm and WEP Key configured in the SU. This is intended primarily for installations with possible "stolen" SUs. In such cases, initial authentication will be in this mode, and the mode will be changed to Shared Key only after configuring appropriate WEP Keys in the AU as well as in all associated SUs, excluding known "stolen" SUs that belong to the Black List.

The applicable key(s) must be defined prior to enabling the Shared Key option. If the required algorithm is Shared Key, do the following:

1. Define at least one of the four WEP Keys by selecting one of them from the Security Parameters menu and entering the required key.
2. In an SU, select Default Key ID from the Security Parameters menu and enter the number of a defined WEP key.
3. Select Authentication Algorithm from the Security Parameters menu. The Authentication Algorithm menu opens.
4. Select the Shared Key option.

NOTE

The Shared Key option cannot be selected until at least one WEP Key is configured. In the SU the appropriate Default Key ID must also be configured.

The default is Open System.

Default Key ID (SU Only)

The Default Key ID defines the ID of the key to be used for encryption of transmitted authentication messages and decryption of received authentication messages.

Valid values are from 1 to 4.

The default is WEP KEY # 1.

WEP KEY # 1 through WEP KEY # 4

A WEP Key defines an encryption key to be used for initialization of the pseudo-random number generator used in the RC4 encryption process. At least one WEP Key must be configured before the Shared Key authentication mode can be used. The Subscriber Unit must use the same WEP Key that is used by the Access Unit.

The WEP Key is a string of 10 hexadecimal numbers.

The default for all 4 keys is a string of 10 zeros (no key).

Wireless Media Security

Wireless media security is provided by preventing the ability to perform data sniffing on the air. Encryption functionality is achieved by using the modem scrambler. The scrambling algorithm is based on two parameters - a polynom and a seed. In order to be able to extract wireless data the receiver must have the same polynom and seed as the transmitter. The wireless media security feature enables changing the polynom and the seed used for the scrambling operation, thus insuring that only units with the same polynom and seed may interact with each other. Enhanced security is achieved by using 16-bit length seeds and up to 16-bit polynoms.

The available parameters are:

Encryption Seed

The Encryption Seed parameter defines the index of the 16-bit encryption seed to be used for wireless media security.

Valid values are from 1 to 127.

The default is 7.

Encryption Polynom Index

The Encryption Polynom Index parameter defines the index of the up to 16-bit encryption polynom to be used for wireless media security.

Valid values are from 0 to 9.

The default is 0.

NOTE

To ensure security, the values of the WEP Keys, Encryption Seed and Encryption Polynom Index may be entered using Installer access rights but can be viewed only with Administrator access rights.

Hopping Parameters (GU)

The Hopping Parameters Menu allows configuration of the hopping mechanism. The GPS modules deliver signals to the Access Units that insure that their hopping patterns are fully synchronized. This includes synchronizing the time each unit starts a new hop and ensuring that units start the hopping sequence simultaneously.

Number of Hopping Frequencies

Configures the Number of Hopping Frequencies parameter to guarantee that all the Access Units managed by the GPS module will start their hopping sequence simultaneously.

To determine the correct number of hopping frequencies, access the monitor program in one of the AU units, select Show Basic Configuration in the Info Screens menu and view the Number of Hopping Frequencies value displayed.

Dwell Time

The Dwell Time parameter in the GU must be set to the value configured for the Dwell Time in the AU(s)

GPS Antenna Recovery

Under normal operating conditions, the BS-GU module uses the time signals it receives from the GPS antenna to generate the synchronization signals for the AUs. When two or more BS-GU modules are daisy-chained, the signals from the GPS antenna are transferred to all "slave" BS-GU modules via the SYNC OUT - SYNC IN cable, and all BS-GUs use these signals to generate synchronization signals for their AUs.

The BS-GU can detect whether a daisy-chaining cable is connected to its' SYNC IN port; If a daisy-chaining cable is connected to the SYNC IN port, the unit is a "slave" unit. If a daisy-chaining cable is not connected to the SYNC IN port, the unit will behave like a "master".

The BS-GU continuously checks whether it receives proper PPS (Pulse Per Second) signals from the GPS antenna. Proper PPS signals are exactly one second apart. When a BS-GU detects that it does not receive proper timing signals from the GPS antenna, it will behave as follows:

a. If the BS-GU is a "master", it will start generating synchronization signals using its internal clock. The synchronization signals will also be transferred to the SYNC OUT port.

b. If a BS-GU is a "slave", it will use the synchronization signals it receives from the "master" via the SYNC IN port. It will also transfer these signals to its SYNC OUT port for use by the next slave module if applicable.

A slave module continuously monitors the lines from the GPS antenna in its SYNC IN port. If it determines that proper PPS signals are received (at least three consecutive PPS signals one second apart), it will automatically revert to the regular operating mode, using the PPS signals for generating its synchronization signals.

A master BS-GU must enter a special antenna recovery mode to check the validity of the signals it receives from the GPS antenna.

NOTE

During Antenna Recovery mode the master BS-GU module stops generating synchronization signals for several seconds. Therefore, the rate of entering this mode should be minimal.

The antenna recovery mode can be activated either manually or automatically, using the GPS Antenna Recovery menu:

Manual Recovery Mode

The Manual Recovery Mode option enables to initiate a single antenna recovery process during which the unit checks the signals it receives from the GPS antenna. The manual recovery mode is completely independent of the automatic recovery mode, meaning that a manual recovery process can be initiated by the user regardless of the selected option in Automatic Recovery Option. Typically, manual recovery will be initiated after connecting/re-connecting or fixing a problem in the GPS antenna.

Automatic Recovery Mode

The Automatic Recovery Mode sub-menu enables to control an automatic recovery process. It includes the following option and parameter:

Automatic Recovery Option

The Automatic Recovery Option enables or disables automatic initiation of antenna recovery process. If a GPS antenna is not used, the Automatic Recovery Option should be disabled.

The default selection is Enable.

Automatic Recovery Interval

The Automatic Recovery Interval parameter defines the time interval between two consecutive initiations of automatic antenna recovery processes.

Valid values: 5 to 1440 (minutes)

Default value: 15 (minutes)

NOTE

The GPS Antenna Recovery menu is applicable only to a "master" BS-GU module.

Alarm Parameters (GU)

The GU module serves also as the alarms control unit for the BreezeACCESS system and auxiliary equipment. It has dry contact connections to 4 external alarm inputs (Alarm In 1 through Alarm In 4), that turn on upon contact closure. It also receives alarm indications from BreezeACCESS power supply module (Alarm In 7 through Alarm In 10), that turn on to indicate a power failure or over temperature problem in any of the two optional power supplies. PS1 alarms refer to a power supply module inserted in the left-most slot of the chassis. PS2 alarms refer to a power supply module inserted in the right-most slot of the chassis. Alarm In 5 (GPS Antenna Status) is generated internally in the GU module, and it is turned on to indicate that proper PPS (pulse per second) timing signals are received from the GPS antenna.

NOTE

Over Temperature alarm indication is only supported by the AC power supply module. In installations with a single power supply module, the GU module doesn't function (and therefore will not provide an alarm indication) upon total failure of the power supply or upon failure of the 5 V module.

The GU module can also control 3 Alarm Out relay, where each relay has a common contact, a normally open (NO) contact and a normally closed (NC) contact.

The Alarm Parameters menu allows access to the following sub-menus:

- Alarms In Names.
- Alarms Out Names.
- Automatic Alarms Out Definition.
- Alarms Out Control.
- Show Alarm Parameters.

Alarms In Names

The Alarms In Names menu enables defining names for each of the four external alarm indications that can be connected to the AL IN connector. These names can reflect the specific environment in which the module is being used (e.g. "Smoke Detector 1" or "Main Door").

Each Alarms In Name can contain up to 31 printable ASCII characters (case sensitive).

The default names are Alarm In 1 through Alarm In 4.

Alarms Out Names

The Alarms Out Names menu enables defining names for each of the three external devices that can be connected to the AL OUT connector. These names can reflect the specific environment in which the module is being used (e.g. “Alarm Light 1”).

Each Alarms Out Name can contain up to 31 printable ASCII characters (case sensitive).

The default names are Alarm Out 1 through Alarm Out 3.

Automatic Alarms Out Definition

The Automatic Alarms Out Definition menu allows you to define the conditions under which each of the 3 Alarms Outs is to be activated (when operating in Automatic mode). The available options for each of the three Alarms Out are:

- 1 – Activate if Alarm In 1 turns ON.
- 2 – Activate if Alarm In 2 turns ON.
- 3 – Activate if Alarm In 3 turns ON.
- 4 – Activate if Alarm In 4 turns ON.
- 5 - Activate if Alarm In 5 (GPS Antenna Status) turns ON
- 6 - Not Applicable (Alarm In 6 is not defined)
- 7 - Activate if Alarm In 7 (PS1Over Temperature) turns ON
- 8 - Activate if Alarm In 8 (PS2 Over Temperature) turns ON
- 9 - Activate if Alarm In 9 (PS1 Power) turns ON
- 10 - Activate if Alarm In 10 (PS2 Power) turns ON
- N – None (never activate this Alarm Out).
- A - Activate if ANY of the Alarms In turns ON.

The default for all three Alarms Out is 0 (None – never activate the alarm).

Alarms Out Control

The Alarms Out Control menu allows the functionality of the Alarms Out control mechanism to be defined. Its main purpose is to support "manual" activation/deactivation of each of the Alarms Out either locally or remotely using Telnet or SNMP. For each of the three Alarms Out, the following control options are available:

- 0 – Turn Alarm OFF (even if it should be ON according to the definition in the Automatic Alarms Out Definition Menu).
- 1 – Turn Alarm ON (even if it should be OFF according to the definition in the Automatic Alarms Out Definition Menu).
- 2 – Automatic (activate/deactivate according to the definition in the Automatic Alarms Out Definition Menu).

The default for all three Alarms Out is 2 (Automatic).

Show Alarm Parameters

Shows the current values of the Alarms In and Alarms Out parameters as well as their current status. It includes the following items:

Alarms In Names And Status

Displays the names and current status (ON or OFF) for all Alarm In indications, including "internal" alarms, as follows:

- Alarm In 1 through Alarm In 4: Name according to the name defined in the Alarms In Names Menu.
- Alarm In 5: GPS Antenna Status.
- Alarm In 6: NA (reserved for future use).
- Alarm In 7: PS1 Over Temperature (over temperature indication for BS-PS Power Supply module 1, which is the module inserted in the left-most slot of the chassis).
- Alarm In 8: PS2 Over Temperature (over temperature indication for BS-PS Power Supply module 2, which is the module inserted in the right-most slot of the chassis).
- Alarm In 9: PS1 Power (power fail indication for BS-PS Power Supply module 1, which is the module inserted in the left-most slot of the chassis).

- Alarm In 10: PS2 Power (power fail indication for BS-PS Power Supply module 2, which is the module inserted in the right-most slot of the chassis).

NOTE

In some installations only one Power Supply module (either PS1 or PS2) may be used.

Alarms Out Names, Definitions, Control and Status

Displays the following information for each of the three Alarms Out:

- Name: Name according to the name defined in the Alarms In Names Menu.
- Definition: NONE, Alarm In # or ANY, according to the configuration in the Automatic Alarms Out Definition Menu.
- Control: OFF, ON or AUTO, according to the configuration in the Alarms Out Control Menu.
- Status: ON or OFF.

This page left intentionally blank.

A

Appendix A - Mounting the 10 dBi Flat Panel Subscriber Antenna

This antenna is provided with the subscriber unit. It may also be purchased separately for use with either the AU or CX units.

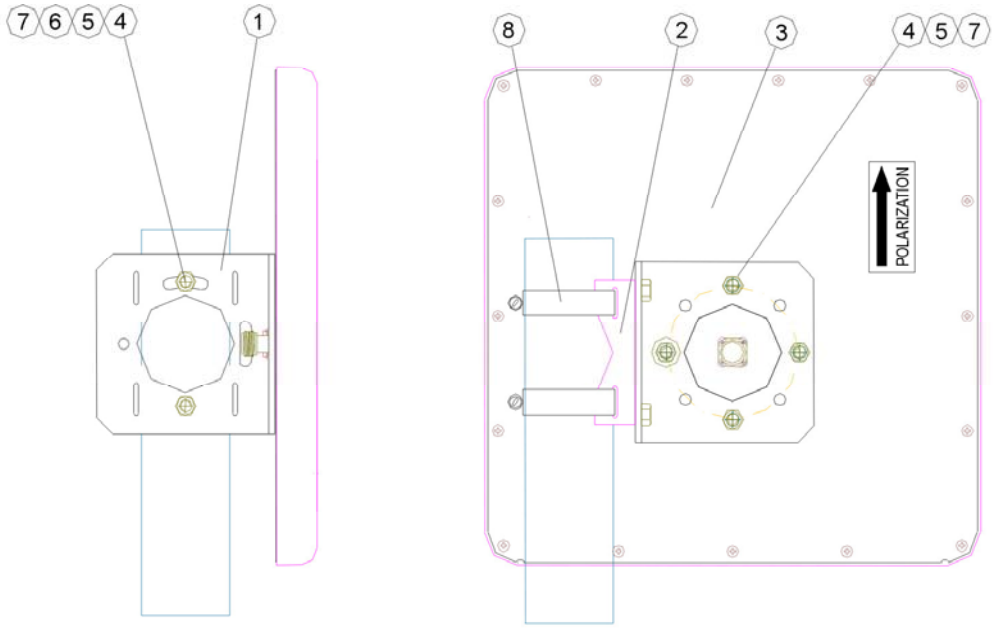
Vertical polarization: The POLARIZATION arrow should point upward or downward.

Horizontal polarization: The POLARIZATION arrow should be parallel to ground.

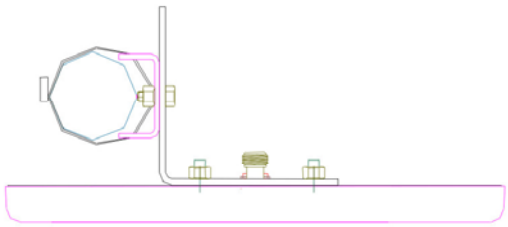
CAUTION

Do not install antennas near power lines. Contact with high voltage lines is dangerous and can cause death or serious injury.

Mounting on a 1”-2.5” Pole



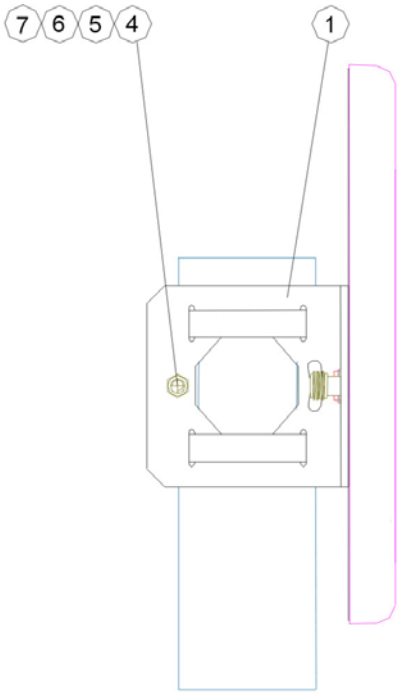
ITEM No.	DESCRIPTION	QTY.
1	GRIP 1	1
2	GRIP 3	1
3	ANT. ASSY	1
4	NUT NC 1/4-20"	6
5	SPRING WASHER #1/4	6
6	FLAT WASHER #1/4	6
7	SCREW NC 1/4 - 20 X 5/8"	2
8	S.S BAND 75-110 & S.S SCREW	2

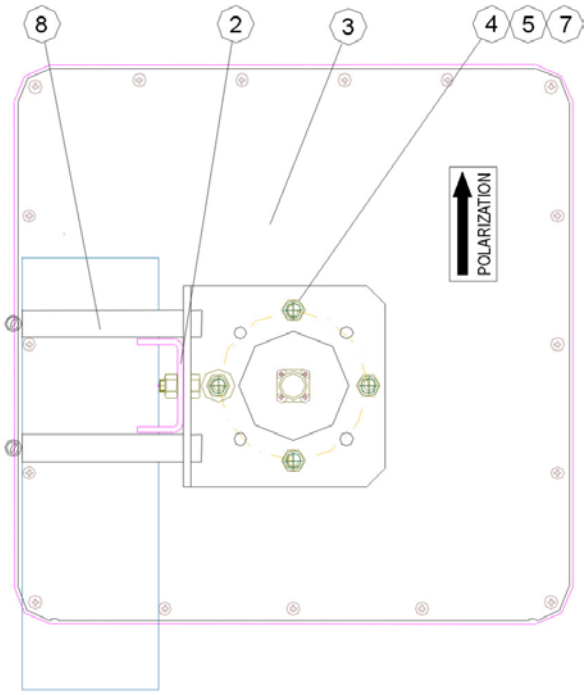


Mounting instructions - Azimuth and Elevation Tilt

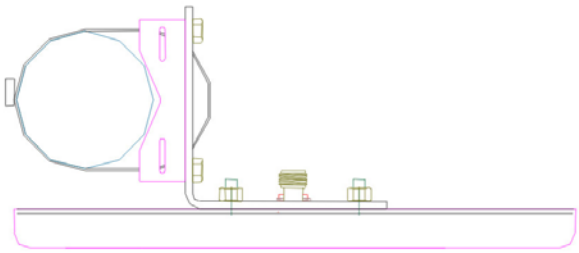
1. Place item No. 1 on the antenna, as illustrated in the drawing. Align with the screw holes.
2. Connect item No. 1 to the antenna with spring washers (5), flat washers (6) and nuts (4).
3. Tighten the nuts at a torque of 30 In*Lbs.
4. Connect item No. 2 to item No. 1 as illustrated, with items 4,5,6,7. Leave screws slightly loose.
5. Connect item No. 2 to the pole with the hose clamps (8) and tighten to the pole with a torque of 30 In*Lbs.
6. Adjust the desired angle, and fully tighten the loose screws (paragraph 4).

Mounting on a 2.5”-4” Pole





ITEM No.	DESCRIPTION	QTY.
1	GRIP 1	1
2	GRIP 3	1
3	ANT. ASSY	1
4	NUT NC 1/4-20"	6
5	SPRING WASHER #1/4	6
6	FLAT WASHER #1/4	6
7	SCREW NC 1/4-20 X 5/8"	2
8	S.S BAND 75-110 & S.S SCREW	2



Mounting instructions - Azimuth and Elevation Tilt

1. Place item No. 1 on the antenna, as illustrated in the drawing. Align with the screw holes.
2. Connect item No. 1 to the antenna with spring washers (5), flat washers (6) and nuts (4).
3. Tighten the nuts at a torque of 30 In*Lbs.
4. Connect item No. 2 to item No. 1 as illustrated, with items 4,5,6,7.
5. Connect item No. 1 to the pole with the hose clamps (8) and tighten to the pole with a torque of 30 In*Lbs.
6. Adjust the desired angle, and fully tighten the loose screws.

This page left intentionally blank.

B

Appendix B - SU-I Lightning and Grounding Installation

SU-I Lightning and Grounding Installation

Extra Items Needed

An N-Type DC grounding block can be used to provide an Eearth ground connection for the SU-I-1D-900. To complete the grounding installation you will need these items:

- 50ft. Grounding wire and clamps.
- Mounting screws, anchors, and coax cable clips.
- 2 Coax seal patches.
- A grounding block or connection to an Earth ground
- (Optional) 900 MHz Lightning arrestor for use in place of the grounding block in lightning prone areas where the antenna is placed at the building high point. Available from Alvarion, model number LA-900.

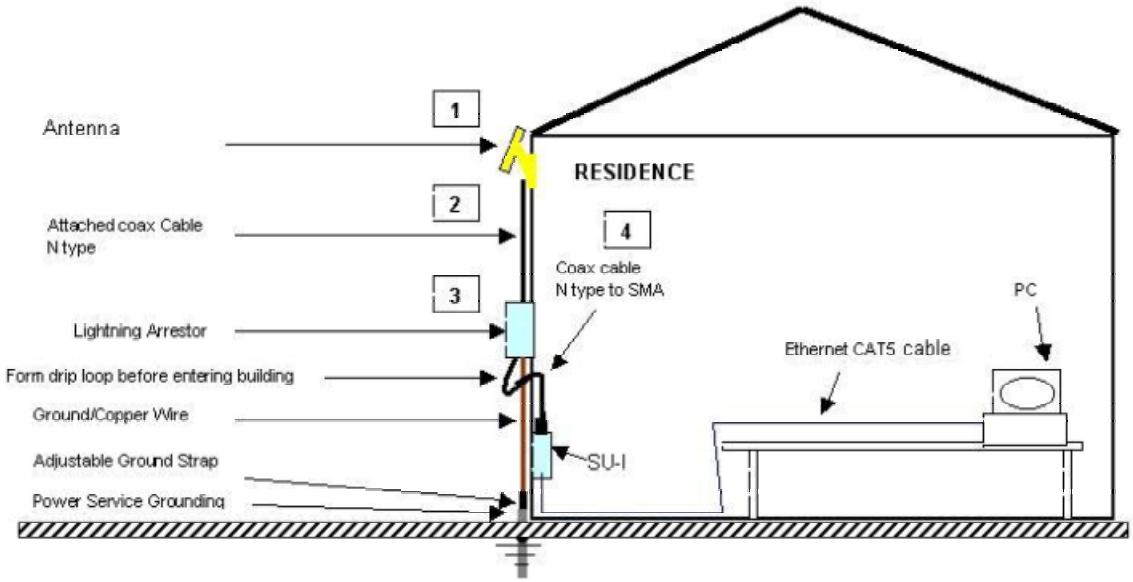


Figure B-1: Connections Diagram

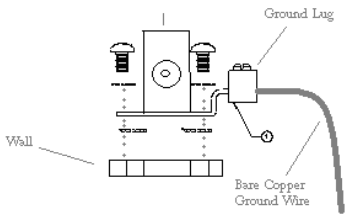


Figure B-2: Installing the Grounding Block or Lightning arrestor

C

Appendix C - Parameters Summary

In this Appendix:

The tables in this appendix provide an at a glance summary of the configurable parameters, value ranges, and default values. In addition, each parameter entry also includes an indication as to whether the parameter is updated in run-time or whether the unit must be reset before the modification takes effect.

Parameters Summary

Unit Control Parameters

Table C-1: Unit Control Parameters

Parameter	Unit	Range	Default	Run-Time
Change Unit Name	All	Up to 32 printable ASCII characters	None	Yes
Change Read Only Password	All	Up to 8 printable ASCII characters	public	No
Change Installer Password	All	Up to 8 printable ASCII characters	user	No
Change Administrator Password	All	Up to 8 printable ASCII characters	private	No
Console Speed	All	■ 9600 ■ 19200 ■ 38400 ■ 57600 ■ 115200	9600	No
Event Log Policy	All	■ Log All (TRC) ■ Message (MSG) ■ Warning (WRN) ■ Error (ERR) ■ Fatal (FTL) ■ Log None	Fatal (FTL)	Yes
Log Out Timer	All	1-999 minutes	5	Yes
Auto Configuration Option	All	■ Disable ■ Enable	Disable	Yes
SNMP Read ESSID	AU, SU	■ Disable ■ Enable	Disable	No

Site Survey Parameters

Table C-2: Site Survey Parameters

Parameter	Unit	Range	Default	Run-Time
Ping Test Destination IP address	All	IP address	192.0.0.1	Yes
No. of Pings	All	0-9999 (o is for continuous pinging	1	Yes
Ping Frame Length	All	60 – 1472 bytes	64	Yes
Ping Frame Timeout	All	200 to 60000 ms, in increments of 200 ms (200, 400, 600,……60000)	200	Yes
RSSI Display Option	AU, SU	■ RSSI ■ dBm	RSSI	Yes
AU alarm Option	AU	■ Disable ■ Enable	Disable	Yes
Learning Period	AU	1 – 1440 (minutes)	30 (minutes)	Yes
Test Cycle	AU	1 – 1440 (minutes)	10 (minutes)	Yes
Retransmissions Minor Alarm Minimum Delta	AU	0 – 100 (%)	20 (%)	Yes
Retransmissions Minor Alarm Threshold	AU	1 – 100 (%)	30 (%)	Yes
Retransmissions Major Alarm Threshold	AU	1 – 100 (%)	60 (%)	Yes
Dropped Frames Minor Alarm Minimum Delta	AU	0 – 100 (%)	10 (%)	Yes
Dropped Frames Minor Alarm Threshold	AU	1 – 100 (%)	10 (%)	Yes
Dropped Frames Major alarm Threshold	AU	1 – 100 (%)	20 (%)	Yes
CRC Error Minor Alarm Minimum Delta	AU	0 – 100 (%)	20 (%)	Yes
CRC Error Minor Alarm Threshold	AU	1 – 100 (%)	40 (%)	Yes
CRC Error Major Alarm Threshold	AU	1 – 100 (%)	70 (%)	Yes
Duplicate Frames Minor Alarm Minimum Delta	AU	0 – 100 (%)	5 (%)	Yes

Table C-2: Site Survey Parameters

Parameter	Unit	Range	Default	Run-Time
Duplicate Frames Minor Alarm Threshold	AU	1 – 100 (%)	5 (%)	Yes
Duplicate Frames Major alarm Threshold	AU	1 – 100 (%)	15 (%)	Yes
SU Rx Power Decrease Threshold	AU	1 – 99 (dBm)	15 (dBm)	Yes
AU Rx Power Decrease Threshold	AU	1 – 99 (dBm)	15 (dBm)	Yes
Minimum Number Of SUs	AU	1 – 254 (SUs)	5 (SUs)	Yes

IP Parameters

Table C-3: IP Parameters

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

Air Interface Parameters

Table C-4: Air Interface Parameters

Parameter	Unit	Range	Default	Run-Time
HDM Mode	AU	■ Disable ■ Enable	Disable	No
Define Sub-Bands	AU, SU	904-926 MHz	915 MHz	No
Scrambling Mode	AU, SU	■ Standard ■ Enhanced ■ Manual	Enhanced	No
Spanning Factor	AU	1 to number of frequencies minus 1	1	No
Scan Entire Band	SU	■ Disable ■ Enable	Enable	No
Hopping Sequence (Shift)	AU	0 to number of frequencies minus 1	0	No
Hopping Sync	AU	■ Idle ■ Master ■ Slave	Idle	No
ESSID	AU, SU	Up to 31 printable ASCII characters	ESSID1	No
Operator ESSID Option	AU	■ Disable ■ Enable	Enable	No
Operator ESSID	AU	Up to 31 printable ASCII characters	ESSID1	No
Best AU Support	SU	■ Disable ■ Enable	Disable	No
Number of Scanning Attempts	SU	1 – 255	20	No
Preferred AU MAC Address	SU	MAC Address	00-00-00-00-00-00 (no preferred AU)	Yes
Scanning Mode	SU	■ Passive ■ Active	Active	No
Transmit Power	SU	3023 (dBm)	23 (dBm)	No
Transmit Power Control	AU	■ 0 (23 dBm) ■ 1 (24.5 dBm) ■ Manual	0 (23 dBm)	No

Table C-4: Air Interface Parameters

Parameter	Unit	Range	Default	Run-Time
Maximum Data Rate	AU, SU	■ 1 Mbps ■ 2 Mbps ■ 3 Mbps	3 Mbps	No
AU Transmission Rate Control	SU	■ Disable ■ Enable	Disable	No
Acknowledge Delay Limit	AU, SU	■ Low (<10 km) ■ Medium (<20 km) ■ High (>20 km)	Low	No
Wireless Trap Threshold	AU, SU	AU: 1-100 (%) SU: 0-255 (RSSI units)	AU: 30 (%) SU: 45 (RSSI)	Yes
Maximum Number of Associations	AU	1 – 512	512	Yes
MAC Address Black List	AU	Up to 100 MAC addresses	None (empty list)	Yes
Send Roaming SNAP	SU	■ Disable ■ Enable	Disable	No

Network Management Parameters

Table C-5: Network Management Parameters

Parameter	Unit	Range	Default	Run-Time
Access to Network Management	AU, SU	■ From Wlan Only ■ From Ethernet Only ■ From Both Ethernet & Wlan	From Both Ethernet & Wlan	No
Network Management Filtering	All	■ Disable ■ Activate Management IP Filter On Ethernet Port ■ Activate Management IP Filter On Wlan Port (not available in GU) ■ Activate Management IP Filter On Both Ethernet & Wlan Ports (not available in GU)	Disable	No
Set Network Management IP Address	All	IP address	0.0.0.0 (all 3 entries)	No
Send SNMP Traps	All	■ Disable ■ Enable	Disable	Yes
SNPM Traps IP Destination	All	IP address	0.0.0.0 (all 3 entries)	No
SNMP Traps Community	All	Up to 14 printable ASCII characters	public (all 3 entries)	No
Send SU Associated AU Trap	AU	■ Disable ■ Enable	Enable	Yes
Send AU Disassociated Trap	AU	■ Disable ■ Enable	Enable	Yes
Send AU Aging Trap	AU	■ Disable ■ Enable	Enable	Yes
Send AU Wireless Quality Trap	AU	■ Disable ■ Enable	Enable	Yes
Send SU Associated Trap	SU	■ Disable ■ Enable	Enable	Yes

Table C-5: Network Management Parameters

Parameter	Unit	Range	Default	Run-Time
Send SU Wireless Quality Trap	SU	■ Disable ■ Enable	Enable	Yes
Send Parameter Changed Trap	AU, SU	■ Disable ■ Enable	Enable	Yes
Send GPS Alarm In Trap	GU	■ Disable ■ Enable	Enable	Yes
Send GPS Alarm Out Trap	GU	■ Disable ■ Enable	Enable	Yes
Send GPS UTC Status Trap	GU	■ Disable ■ Enable	Enable	Yes
Send Power Up From Reset Trap	All	■ Disable ■ Enable	AU & GU: Enable SU: Disable	Yes
Send Monitor Status Trap	All	■ Disable ■ Enable	Enable	Yes
Send Cold \ Warm Start Trap	All	■ Disable ■ Enable	AU & GU: Enable SU: Disable	Yes
Send AU Loss Of Sync Trap	BS-AU	■ Disable ■ Enable	Enable	Yes
Send AU Alarms Traps	AU	■ Disable ■ Enable	Enable	Yes
Send Ethernet Broadcast Limiter Trap	AU, SU	■ Disable ■ Enable	Disable	Yes

Bridge Parameters

Table C-6: Bridge Parameters

Parameter	Unit	Range	Default	Run-Time
VLAN ID-Data	SU	1 – 4094	1	No
VLAN ID – Management	All	1 – 4094, 65535	65535 (no VLAN)	No
VLAN Link Type	All	■ 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	All	0 – 7	0	No
VLAN Priority Threshold	AU, SU	0 – 7	4	Yes
ToS Precedence Threshold	AU, SU	0 – 7	3	Yes
Ethernet Broadcast Filtering Options	SU	■ Disable, ■ On Ethernet Only ■ On Wlan Only ■ On Both Ethernet & Wlan	Disable	Yes
DHCP Broadcast Override Filter	SU	■ Disable ■ Enable	Disable	Yes
PPPoE Broadcast Override Filter	SU	■ Disable ■ Enable	Disable	Yes
ARP Broadcast Override Filter	SU	■ Disable ■ Enable	Enable	Yes

Table C-6: Bridge Parameters

Parameter	Unit	Range	Default	Run-Time
Ethernet Broadcast/Multicast Limiter Option	AU, SU	■ Disable ■ Limit only Broadcast Packets ■ Limit Multicast Packets that are not Broadcasts ■ Limit All Multicast Packets (including broadcast)	Disable	Yes
Ethernet Broadcast Limiter Threshold	AU, SU	0 to 20480 (packets/second)	20480	Yes
Bridge Aging Time	AU, SU	20 – 2000 seconds	300	No
LAN to WLAN Bridging Mode	AU	■ Reject Unknown ■ Forward Unknown	Forward Unknown	Yes
Broadcast Relaying	AU	■ Disable ■ Enable	Enable	No
Unicast Relaying	AU	■ Disable ■ Enable	Enable	No
Ethernet Port Control	SU	■ Disable ■ Enable	Enable	No
Roaming Option`	SU	■ Disable ■ Enable	Disable	No

Performance Parameters

Table C-7: Performance Parameters

Parameter	Unit	Range	Default	Run-Time
RTS Threshold	AU, SU	20 – 1600 (bytes)	AU: 1600 SU: 60	Yes
Number of Retransmissions	AU, SU	1 – 100	1	No
Number of Retransmissions to Decrease Rate	AU, SU	0 – 10	0	No
Number of Dwells to Retransmit	AU, SU	0 – 9	2	No
Minimum Contention Window	AU, SU	7 - 255	31	No
Maximum Multicast Rate	AU	■ 1 Mbps ■ 2 Mbps ■ 3Mbps	1Mbps	Yes
Multi-Rate Support	AU, SU	■ Disable ■ Enable	Enable	No
Multi-Rate Decision Window Size	AU, SU	1 – 50	12	No
Number of Failures in Multi-Rate Decision Window	AU, SU	1 to Multi-Rate Decision window Size	8	No
Dwell Time	AU, GU	32, 64, 128 (Kilo-microseconds)	128	No
Noise Floor	AU, SU	-115 to -50 (dBm)	AU: -112dBm SU: -105dBm	No
Carrier To Interference Difference Level	AU, SU	6 to 60 (dB)	AU: 8dB SU: 9dB	No
Carrier Sense Level	AU, SU	-100 to -40 (dBm)	-85 dBm	No
Adaptive Thresholds Option	SU	■ Disable ■ Enable	Disable	No
Adaptive Thresholds Period	SU	1 – 60 (seconds)	15 (seconds)	No
Adaptive Thresholds Fading Factor	SU	0 – 70 (dB)	10 (dB)	No

Service Parameters

Table C-8: Service Parameters

Parameter	Unit	Range	Default	Run-Time
User Filtering Option	SU	■ Disable ■ IP Protocol Only ■ User Defined Addresses Only ■ PPPoE Protocol Only	Disable	Yes
Set User Filter Address	SU	IP address (8 entries)	0.0.0.0 (all 8 entries)	Yes
Set User Filter Mask	SU	IP address (8 entries)	255.255.255.255 (all 8 entries)	Yes
Set User Filter Range	SU	0 – 255. 0 means that the range is not used.	0 (all 8 entries)	Yes
MIR/CIR Option	AU, SU	■ Disable ■ Enable	Disable	No
MIR: AU to SU	SU	32 – 2200Kbps	128Kbps	No
MIR: SU to AU	SU	32 – 2200Kbps	128Kbps	No
CIR: AU to SU	SU	0 – 2200Kbps	64Kbps	No
CIR: SU to AU	SU	0 – 2200Kbps	64Kbps	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	Disable, Enable	Disable	No

Security Parameters

Table C-9: Security Parameters

Parameter	Unit	Range	Default	Run-Time
Authentication Algorithm*	AU, SU	■ Open system ■ Shared Key ■ Support All (AU only)	Open system	No
Default Key ID	SU	1-4	1	No
Key # 1 to Key # 4	AU, SU	10 hexadecimal digits	0…0 (all 0=no key)	No
Encryption Seed	AU, SU	1 – 127	7	No
Encryption Polynom Index	AU, SU	0-9	0	No

RADIUS Parameters

Table C-10: RADIUS Parameters

Parameter	Unit	Range	Default	Run-Time
User Name	SU	Up to 64 printable ASCII characters	The units' MAC Address	No
User Password	SU	Up to 64 printable ASCII characters	RadiusPassword1	No
Shared Secret	SU	Up to 20 characters	RadiusSecret1234	No
Authentication Option	SU	■ Disable ■ Enable	Disable	No
RADIUS Server Authentication IP Address	SU	IP Address	0.0.0.0	No
RADIUS Server Authentication Port	SU	1000 to 65535	1812	No
Accounting Option	SU	■ Disable ■ Enable	Disable	No
RADIUS Server Accounting IP Address	SU	IP Address	0.0.0.0	No
RADIUS Server Accounting Port	SU	1000 to 65535	1813	No
Accounting Interval	SU	60 to 6000 (seconds)	90 (seconds)	No

Hopping Parameters

Table C-11: Hopping Parameters

Parameter	Unit	Range	Default	Run-Time
Number of Hopping Frequencies	GU	2-12		No
Automatic Recovery Option	GU	■ Disable ■ Enable	Enable	Yes
Automatic Recovery Interval	GU	5 – 1440 (minutes)	15 (minutes)	Yes
Dwell Time	GU	32, 64, 128	128 Same as in AU	No

Alarm Parameters

Table C-12: Alarm Parameters

Parameter	Unit	Range	Default	Run-Time
Alarm In Names	GU	Up to 31 printable ASCII characters	Alarm In 1 through Alarm In 4	Yes
Alarm Out Names	GU	Up to 31 printable ASCII characters	Alarm Out 1 through Alarm Out 3	Yes
Automatic Alarm Out Definition	GU	1 -10, N (None), A (Any)	N (None) for all 3 Alarm Outs	Yes
Alarm Out Control	GU	■ On ■ Off ■ Automatic	Automatic for all 3 Alarm Outs	Yes

D

Appendix D - RSSI to dBm conversion

RSSI to dBm Conversion – AU

Table D-1: RSSI to dBm Conversion - AU

RSSI	dBm		RSSI	dBm
71	-100		114	-64
72	-99		115	-63
74	-98		116	-62
75	-97		118	-61
77	-96		119	-60
78	-95		120	-59
81	-94		121	-58
82	-93		122	-57
83	-92		123	-56
84	-91		125	-55
85	-90		126	-54
86	-89		127	-53
88	-88		128	-52
89	-87		129	-51
90	-86		130	-50
91	-85		131	-49
92	-84		133	-48
93	-83		134	-47
94	-82		135	-46
96	-81		136	-45
97	-80		137	-44
98	-79		138	-43
99	-78		139	-42
100	-77		141	-41
101	-76		142	-40
102	-75		143	-39
103	-74		144	-38
104	-73		145	-37
105	-72		146	-36
106	-71		148	-35
107	-70		149	-34
108	-69		150	-33
110	-68		151	-32
111	-67		152	-31
112	-66		153	-30
113	-65			

RSSI to dBm Conversion – SU

Table D-2: RSSI to dBm Conversion – SU

RSSI	dBm		RSSI	dBm
26	-100		81	-64
27	-99		82	-63
29	-98		83	-62
30	-97		84	-61
32	-96		85	-60
33	-95		86	-59
35	-94		88	-58
36	-93		89	-57
38	-92		90	-56
39	-91		91	-55
41	-90		92	-54
42	-89		93	-53
44	-88		94	-52
45	-87		96	-51
47	-86		97	-50
48	-85		98	-49
50	-84		99	-48
51	-83		100	-47
53	-82		101	-46
54	-81		102	-45
56	-80		103	-44
57	-79		104	-43
59	-78		105	-42
60	-77		106	-41
62	-76		107	-40
63	-75		108	-39
65	-74		110	-38
66	-73		111	-37
68	-72		112	-36
69	-71		113	-35
71	-70		114	-34
72	-69		115	-33
74	-68		116	-32
75	-67		118	-31
77	-66		119	-30
78	-65			

E

Appendix E - Configuration File Download and Upload Using TFTP

The BreezeACCESS Configuration 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.

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

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

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

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

Use the SNMP write community string (the default is private) to define both the uploaded file (put) and the downloaded file (get). Use the extension cfg for a configuration file. Use the extension cmr for the Operator Defaults file. The file should be transferred in ASCII mode.

For Example:

To upload the configuration file using a DOS based TFTP Client to an SU whose IP address is 206.25.63.65, enter:

tftp 206.25.63.65 put Suconf private.cfg

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

tftp 206.25.63.65 get private.cmr Suconf

F

Appendix F - Software Version Loading Procedure

Software Version Loading Procedure

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

NOTE

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

Verify that you have IP connectivity to the unit to be loaded with a new version. Verify that the IP address of the PC from which you intend to perform the upgrade 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.

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 and use the following procedure:

1. From the Main Menu select 1 – Info Screens. The Info Screens menu opens.

2. From the Info Screen menu select 2 – Show Basic Configuration. A display of the current configuration of the basic parameters appears, including the IP Address, Subnet Mask and Default Gateway Address parameters.

To configure any of the IP parameters, use the following procedure:

1. From the Main Menu select 3 – Basic Configuration. The Basic Configuration menu opens.

2. To configure the IP Address select: 1 – IP Address.

3. To configure the Subnet Mask, select 2 – Subnet Mask.

4. To configure the Default Gateway Address select 3 – Default

Gateway Address.

5. Reset the unit in order for the new configuration to apply.

6. To verify the connection, ping the unit’s IP address. Verify that ping replies are being received.

The procedure to be used depends on the unit's FLASH memory type. Identify the FLASH memory type by using the monitor program, connecting the PC to the unit either directly or via Telnet.

From the Main Menu, select 1 – Info Screens. From the Info Screen menu select 1 – Show Unit Status. The Unit Status display includes the FLASH type (type F or type S).

Use the TFTP utility, with the following syntax, to perform the upgrade: *tftp –i hostaddress put sourcefile [destinationfile]*

Where -i is for binary mode, *hostaddress* is the IP address of the unit to be upgraded, *put* defines that the PC (client) will send a file to the *hostaddress* and *destinationfile* is the name of the file to be loaded.

Use the following tables to determine which source file name to use, according to the unit's type and FLASH type.

Table F-1: Source File Names, FLASH Type F

Unit Type	Source File Name
AU	AXF.BS
SU	AXF.SU
GU	AXF.GU

Table F-2: Source File Names, FLASH Type S

Unit Type	Source File Name
AU	AXF.BS
SU	AXF.SU
GU	AXF.GU

X refers to the software version number, up to 5 decimal digits (e.g. for software release 4.5.15, X=4515).

Loading to a unit with FLASH Type: F

Use the SNMP write community <SnmpWriteCommunity>.dwn (the default write community is private) to define the destination filename.

For example, to load the upgrade file A4515F.BS to an AU whose IP address is 206.25.63.65 use the following syntax:

>tftp –i 206.25.63.65 put A4515F.BS private.dwn

Loading to a unit with FLASH Type: S

Use the SNMP write community <SnmpWriteCommunity>.fmr (default write community is private) to define the destination filename. For example: to load the upgrade file A4515S.SU to an SU whose IP address is 206.25.63.55 use the following syntax:

>tftp –i 206.25.63.55 put A4515S.SU private.fmr

NOTE

If you are upgrading a Subscriber Unit which is not associated with an AU, the unit will reset every five minutes (approximately) and the following message will be displayed:

FTL: file src\wpscan.c line 262 Too large number of scanning attempts

The unit will reset and it will take more than a minute before you can re-establish the connection to it. You should either have the SU associated with an AU before starting the loading process or complete the loading process before the unit resets. Otherwise you will have to try again until you complete the loading process.

When version loading is completed the following message is displayed:

Loading operation has been completed successfully

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 loaded properly, view the firmware versions stored in the FLASH using the following procedure:

1. From the Main Menu, select 2 – Unit Control. The Unit Control menu opens.

2. From the Unit Control menu, select 5 – Flash Memory Control. The Flash Memory Control menu opens.

3. From the Flash Memory Control menu select S – Show Flash Versions. The display appears as follows:

Flash Versions

==========

Current Version: 4.5.14

Shadow Version: 4.5.15

Version After Reset: 4.5.14

From the Flash Memory Control menu select the active software version, using the following procedures:

To activate the backup (shadow) version:

1. From the Flash Memory Control menu select 1 - Reset and Boot from Shadow Version. The Reset and Boot from Shadow Version menu opens.

2. Select 1 – Reset Now and press ENTER.

3. The unit resets and the Shadow version is used as the new active version. Note that after the next reset, the Current version will be activated again.

If the active version is the Shadow version and you wish to continue using it after the next Reset, use the following procedure:

1. From the Flash Memory Control menu select 2 - Use Current Version

After Reset. The Use Current Version After Reset menu opens.

2. Select 1 – Set As Default Now and press ENTER. This will actually cause the names of the two versions to switch. The previous Shadow version will now be called Current and vise versa. The following message will be displayed:

UP (DOWN) Image FLASH will be operational (UP or DOWN refers to the location in the flash memory).

The loading procedure is protected. An attempt to load an invalid version (e.g. using <SnmpWriteCommunity>.fmr when trying to load a new version to units with a FLASH Type: F) will be rejected.

This page left intentionally blank.