



BreezeMAX™ 3500

System Manual

PRELIMINARY

**S/W Version 1.5
April 2005
P/N 214017**

Legal Rights

© Copyright 2005 Alvarion Ltd. All rights reserved.

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

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

Trade Names

Alvarion®, BreezeCOM®, WALKair®, WALKnet®, BreezeNET®, BreezeACCESS®, BreezeMANAGE™, BreezeLINK®, BreezeCCONFIG™, BreezeMAX™, AlvariSTAR™, MGW™, eMGW™, WAVEXpress™, MicroXpress™, WAVEXchange™, WAVEView™, GSM Network in a Box and TurboWAVE™ and/or other products and/or services referenced here in are either registered trademarks, trademarks or service marks of Alvarion Ltd.

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

Statement of Conditions

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

Warranties and Disclaimers

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

Exclusive Warranty

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

(b) With respect to the Firmware, Alvarion warrants the correct functionality according to the attached documentation, for a period of fourteen (14) month from invoice date (the "Warranty Period"). During the Warranty Period, Alvarion may release to its Customers firmware updates, which include additional

performance improvements and/or bug fixes, upon availability (the “Warranty”). Bug fixes, temporary patches and/or workarounds may be supplied as Firmware updates.

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

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

Disclaimer

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

(b) PURCHASER’S SOLE REMEDY FOR BREACH OF THE EXPRESS WARRANTIES ABOVE SHALL BE REPLACEMENT OR REFUND OF THE PURCHASE PRICE AS SPECIFIED ABOVE, AT ALVARION’S OPTION. TO THE FULLEST EXTENT ALLOWED BY LAW, THE WARRANTIES AND REMEDIES SET FORTH IN THIS AGREEMENT ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING BUT NOT LIMITED TO WARRANTIES, TERMS OR CONDITIONS OF MERCHANTABILITY,

FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, NON-INFRINGEMENT, AND ACCURACY OF INFORMATION GENERATED. ALL OF WHICH ARE EXPRESSLY DISCLAIMED. ALVARION'S WARRANTIES HEREIN RUN ONLY TO PURCHASER, AND ARE NOT EXTENDED TO ANY THIRD PARTIES. ALVARION NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS.

Limitation of Liability

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

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

Radio Frequency Interference Statement

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

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

cause harmful interference in which case the user will be required to correct the interference at the user's own expense.

R&TTE Compliance Statement

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

Safety Considerations - General

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

Grounding

Base Station chassis, Micro Base Station and outdoor units are required to be bonded to protective grounding using the bonding stud or screw provided with each unit.

The Micro Base Station shall be bonded to earth at final installation.

Safety Considerations – DC Powered Equipment



CAUTION – Modular Base Station	ATTENTION – Station de Base Modulaire
<p>Risk of electric shock and energy hazard.</p> <p>Disconnecting one Power Interface Unit (PIU) disconnects only one PIU module. To isolate the Modular Base Station completely, disconnect both PIUs.</p>	<p>Risque de décharge électrique et d'électrocution.</p> <p>La déconnection d'un seul module d'alimentation (PIU) n'isole pas complètement la Station de Base Modulaire. Pour cela, il faut impérativement débrancher les deux modules d'alimentation (PIU).</p>

Restricted Access Area: The DC powered equipment should only be installed in a Restricted Access Area.

Installation Codes: The equipment must be installed according to the latest edition of the country national electrical codes. For North America, equipment must be installed in accordance with the US National Electrical Code and the Canadian Electrical Code.

Overcurrent Protection: A readily accessible Listed branch circuit overcurrent protective device, rated 40A for the modular Base Station or 20A for the Micro Base Station, must be incorporated in the building wiring.

CAUTION: This equipment is designed to permit connection between the earthed conductor of the DC supply circuit and the grounding conductor at the equipment. See installation instructions.

- The equipment must be connected directly to the DC Supply System grounding electrode conductor.

- All equipment in the immediate vicinity must be grounded in the same way, and not be grounded elsewhere.
- The DC supply system is to be local, i.e. within the same premises as the equipment.
- There shall be no disconnect device between the grounded circuit conductor of the DC source (return) and the point of connection of the grounding electrode conductor.

Lithium Battery

The battery on the NPU card and in the Micro Base Station is not intended for replacement.

Caution

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

Line Voltage

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

Radio

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

Outdoor Units and Antennas Installation and Grounding

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

Important Notice

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

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

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

About This Manual

This manual describes the BreezeMAX 3500 (“BreezeMAX”) Broadband Wireless Access System Release 1.5 and details how to install, operate and manage the system components.

This manual is intended for technicians responsible for installing, setting and operating the BreezeMAX system, and for system administrators responsible for managing the system.

This manual contains the following chapters and appendices:

- **Chapter 1 – System description:** Describes the BreezeMAX system and its components.
- **Chapter 2 – Installation:** Describes how to install the system components.
- **Chapter 3 – Commissioning:** Describes how to configure basic parameters, align the Subscriber Unit (SU) antenna and validate unit operation.
- **Chapter 4 – Operation and Administration:** Describes how to use the Monitor application for configuring parameters, checking system status and monitoring performance.
- **Appendix A – Preparing the Indoor to Outdoor Cable:** Provides details on preparation of the indoor to outdoor Ethernet cable.
- **Appendix B – Using the SU Installer Program:** Describes how to access and use the SU Installer Program.
- **Appendix C – Software Upgrade:** Describes how to load new software files using TFTP, and how to switch to a new software version in BreezeMAX units.

NOTE



This guide covers the installation, commissioning and administration of BreezeMAX Base Station equipment (modular Base station and Micro Base Station) and of the CPE with a CPE-IDU-1D indoor unit (Basic IDU). For details on installation, commissioning and administration of other types of indoor units (Gateway IDU), refer to the manual for the applicable equipment.

- **Appendix D – Traps and Alarms:** Describes the BreezeMAX Traps and Alarms.
- **Appendix E – Defining Service Profiles for Generic VoIP Gateways:** Describes the principles of defining Service Profiles for 3rd party generic (non-DRAP-based) VoIP devices.



Contents

Chapter 1 - System Description	1
1.1 Introducing BreezeMAX	2
1.2 Subscriber Units	5
1.3 Voice and Networking Gateways	6
1.4 Base Station Equipment	8
1.5 Networking Equipment	14
1.6 Management Systems	15
1.7 Specifications	17
Chapter 2 - Installation	31
2.1 Installing the ODU	32
2.2 Installing the Modular Base Station Equipment	43
2.3 Installing the Micro Base Station Equipment	60
2.4 Installing the CPE-IDU-1D Indoor Unit	65
Chapter 3 - Commissioning	69
3.1 Base Station and Micro Base Station Commissioning	70
3.2 SU Commissioning	77
Chapter 4 - Operation and Administration	83
4.1 BreezeMAX System Management	84
4.2 The Monitor Program	85
4.3 The Micro Base Station's Main Menu	88

4.4 Micro Base Station Menu	89
4.5 The NPU's Main Menu.....	95
4.6 Base Station Menu	97
4.7 NPU Menu	102
4.8 AU Menu.....	115
4.9 SU Menu	132
4.10 Services Menu	150
4.11 NPU/Micro Base Station Parameters Summary.....	177

Appendix A - Preparing the SU IDU-ODU Cable	191
--	------------

Appendix B - Using the SU Installer Monitor Program	195
--	------------

B.1 The SU Installer Monitor Program.....	196
B.2 Using the Monitor Program.....	197
B.3 The Main Menu	199
B.4 Unit Control Menu	201
B.5 Registration Parameters Menu	210
B.6 Base Station ID Parameters Menu.....	212
B.7 Radio Parameters Menu	215
B.8 Performance Monitoring Menu	217
B.9 Multirate and ATPC Parameters Menu.....	221
B.10SU Parameters Summary	223

Appendix C - Software Upgrade.....	225
---	------------

C.1 Before you Start	226
C.2 File Loading Procedure	227
C.3 Completing the Software Upgrade (Switching Versions)	228

Appendix D - Traps and Alarms	229
--	------------

D.1 Traps and Alarms Structure	230
D.2 Traps and Alarms Sources	231
D.3 Traps and Alarms Severities	232
D.4 Trap/Alarm Categories	233
D.5 BreezeMAX Traps	234
D.6 Active Alarms	261
 Appendix E - Defining Service Profiles for Generic VoIP Gateways ...	 267
E.1 Introduction.....	268
E.2 1 POTS Basic VoIP G.729 Service Profile	270
E.3 1 POTS Advanced VoIP G.729 Service Profile.....	272
E.4 1 POTS Basic VoIP G.711 Service Profile	274
E.5 1 POTS Advanced VoIP G.711 Service Profile.....	276



Figures

Figure 1-1: BreezeMAX System Architecture	4
Figure 2-2: ODU Pole Installation Using Special Brackets	37
Figure 2-3: ODU Pole Installation Using Metal Bands	38
Figure 2-4: Bottom Panel of the AU-ODU	39
Figure 2-5: Bottom Panel of the SU-ODU (Without the Service Box)	40
Figure 2-6: BMAX-BST-SH Chassis Slot Assignments	44
Figure 2-7: PIU Module Front Panel	46
Figure 2-8: PSU Module Front Panel	49
Figure 2-9: AU-IDU Module Front Panel	50
Figure 2-10: NPU Module Front Panel	52
Figure 2-11: AVU Drawer Front Panel	58
Figure 2-12: Micro Base Station Front Panel	61
Figure 2-13: CPE-IDU-1D Front Panel	66
Figure 2-14: CPE-IDU-1D 3D View	66
Figure 4-1: Micro Base Station Monitor's Main Menu	88
Figure 4-2: NPU Monitor's Main Menu	95
Figure 4-3: Base Station Chassis Slot Assignments	98
Figure 4-4: Counters Description	128
Figure 4-5: Counters Description	146
Figure 4-6: Uplink and Downlink Scheduled Transmissions	148
Figure A-1: Ethernet Connector Pin Assignments	192
Figure B-1: Counters Description	218
Figure D-1: Base Station's Chassis Slots Assignment	231



Tables

Table 1-1: BreezeMAX Frequency Bands	2
Table 1-2: Subscriber Unit ODU's Types.....	5
Table 1-3: PSU Requirements, Configurations with one NPU (excluding PSU redundancy)	11
Table 1-4: PSU Requirements, Configurations with two NPUs (excluding PSU redundancy)	11
Table 1-5: Radio Specifications	17
Table 1-6: Base Station Antennas Electrical Specifications	19
Table 1-7: SU IDU/ODU Communication.....	19
Table 1-8: AU and Micro Base Station IDU/ODU Communication	20
Table 1-9: Data Communication (Ethernet Ports).....	20
Table 1-10: Configuration and Management	21
Table 1-11: Standards Compliance, General	21
Table 1-12: Environmental Specifications.....	22
Table 1-13: Services	22
Table 1-14: Mechanical Specifications, Subscriber Unit.....	24
Table 1-15: Connectors, Subscriber Unit.....	24
Table 1-16: Electrical Specifications, Subscriber Unit	25
Table 1-17: Mechanical Specifications, Modular Base Station Equipment	25
Table 1-18: Electrical Specifications, Modular Base Station Equipment.....	26
Table 1-19: Connectors, Modular Base Station Equipment.....	27
Table 1-20: Mechanical Specifications, Micro Base Station Equipment.....	27
Table 1-21: Electrical Specifications, Micro Base Station Equipment	28
Table 1-22: Connectors, Micro Base Station Equipment.....	28
Table 1-23: Mechanical Specifications, Base Station Antennas.....	29
Table 2-1: IF Cables Requirements	35

Table 2-2: Maximum IF Cable Length (Double Shielded Cables).....	35
Table 2-3: Approved Category 5E Ethernet Cables.....	36
Table 2-4: AU-ODU LEDs	39
Table 2-5: AU-ODU Connectors.....	39
Table 2-6: SU-ODU LEDs	40
Table 2-7: SU-ODU Connectors.....	41
Table 2-8: Power Requirements, Modular Base Station Equipment.....	45
Table 2-9: PIU LEDs.....	46
Table 2-10: PSU Requirements, Configurations with one NPU (excluding PSU redundancy).....	48
Table 2-11: PSU Requirements, Configurations with two NPUs (excluding PSU redundancy)	48
Table 2-12: PSU LEDs	49
Table 2-13: AU-IDU LEDs	51
Table 2-14: NPU Connectors	53
Table 2-15: NPU LEDs	54
Table 2-16: AVU LEDs	58
Table 2-17: Micro Base Station Connectors.....	61
Table 2-18: Micro Base Station LEDs	62
Table 2-19: CPE-IDU-1D Connectors	67
Table 2-20: CPE-IDU-1D LEDs	67
Table 3-1: Basic NPU/Micro Base Station Parameters.....	70
Table 3-2: AU-ODU LEDs	72
Table 3-3: AU-IDU LEDs	73
Table 3-4: NPU LEDs	74
Table 3-5: PIU LEDs.....	75
Table 3-6: PSU LEDs	75
Table 3-7: AVU LEDs	75
Table 3-8: Micro Base Station LEDs	76
Table 3-9: SU's Basic Parameters	78
Table 3-10: CPE-IDU-1D LEDs	80

Table 3-11: SU-ODU LEDs.....	81
Table 3-12: SU-ODU LINK QUALITY Bar LEDs Functionality	82
Table 4-1: COM Port Configuration	85
Table 4-2: Group A Traps	100
Table 4-3: Group B Traps	101
Table 4-4: Range for the Downlink (Tx) Frequency Parameter	123
Table 4-5: Rates (Modulation Schemes and Coding).....	125
Table 4-6: Priority Marking Values.....	162
Table 4-7: CT values.....	168
Table 4-8: Pre-Configured Data Service Profiles.....	171
Table 4-9: Pre-Configured Forwarding Rules for Data Service	172
Table 4-10: Pre-Configured Priority Classifiers for Data Services.....	173
Table 4-11: Pre-Configured QoS Profiles for Data Services	173
Table 4-12: Pre-Configured Voice Service Profiles (for DRAP-based Gateways)	174
Table 4-13: Pre-Configured Service Profiles for Generic (non-DRAP) VoIP Services.....	174
Table 4-14: Pre-Configured Forwarding Rule for Voice Services.....	175
Table 4-15: Pre-Configured Priority Classifiers for Generic (non-DRAP) VoIP Services	175
Table 4-16: Pre-Configured BE and RT QoS Profile for Voice Services	176
Table 4-17: Pre-Configured CG QoS Profile for Generic (non-DRAP) VoIP Services	176
Table 4-18: NPU/ μ BST Monitor Parameters Summary	177
Table A-1: Cable Color Codes	192
Table B-1: SU's Parameters Summary	223
Table D-1: BreezeMAX Trap/Alarm Variables	230
Table D-2: Trap/Alarm Severities.....	232
Table D-3: Trap/Alarm Categories	233

Chapter 1 - System Description

In This Chapter:

- [Introducing BreezeMAX](#), page 2
- [Subscriber Units](#), page 5
- [Voice and Networking Gateways](#), page 6
- [Base Station Equipment](#), page 8
- [Networking Equipment](#), page 14
- [Management Systems](#), page 15
- [Specifications](#), page 17

1.1 Introducing BreezeMAX

BreezeMAX 3500 is Alvarion's WiMAX platform for the licensed 3.5 GHz frequency band. It leverages Alvarion's market-leading knowledge of Broadband Wireless Access (BWA), industry leadership, proven field experience, and core technologies including many years of experience with OFDM technology.

Built from the ground up based on the IEEE 802.16/ETSI HIPERMAN standards, BreezeMAX 3500 is designed specifically to meet the unique requirements of the wireless Metropolitan Area Network (MAN) environment and to deliver broadband access services to a wide range of customers, including residential, SOHO, SME and multi-tenant customers. Its Media Access Control (MAC) protocol was designed for point-to-multipoint broadband wireless access applications, providing a very efficient use of the wireless spectrum and supporting difficult user environments. The access and bandwidth allocation mechanisms accommodate hundreds of subscriber units per channel, with subscriber units that may support different services to multiple end users.

The system uses OFDM radio technology, which is robust in adverse channel conditions and enables operation in non line of sight links. This allows easy installation and improves coverage, while maintaining a high level of spectral efficiency. Modulation and coding can be adapted per burst, ever striving to achieve a balance between robustness and efficiency in accordance with prevailing link conditions.

BreezeMAX supports a wide range of network services, including Internet access (via IP or PPPoE tunneling), VPNs and Voice over IP. Service recognition and multiple classifiers that can be used for generating various service profiles enable operators to offer differentiated SLAs with committed QoS for each service profile.

BreezeMAX products are currently available in the 3.4 – 3.6 GHz frequency band, as shown in Table 1-1. The actual operating frequencies used by the system can be configured according to applicable radio regulations, license conditions and specific deployment considerations.

Table 1-1: BreezeMAX Frequency Bands		
Series (band)	Uplink Frequency	Downlink Frequency
3.5a	3.3995 to 3.4535 GHz	3.4995 to 3.5535 GHz
3.5b	3.450 to 3.500 GHz	3.550 to 3.600 GHz

* The 3.5 GHz CPEs support the full range. The base station equipment support either band 3.5a or band 3.5b.

A BreezeMAX system comprises the following:

- **Customer Premise Equipment (CPE):** BreezeMAX Subscriber Units and alvarion's Voice/Networking Gateways.
- **Base Station (BST) Equipment:** BreezeMAX Base Station equipment, including the modular Base Station and its components and the stand-alone Micro Base Station.
- **Networking Equipment:** Standard switches/routers and other networking equipment, supporting connections to the backbone and/or Internet.
- **Management Systems:** SNMP-based Management, Billing and Customer Care, and other Operation Support Systems.

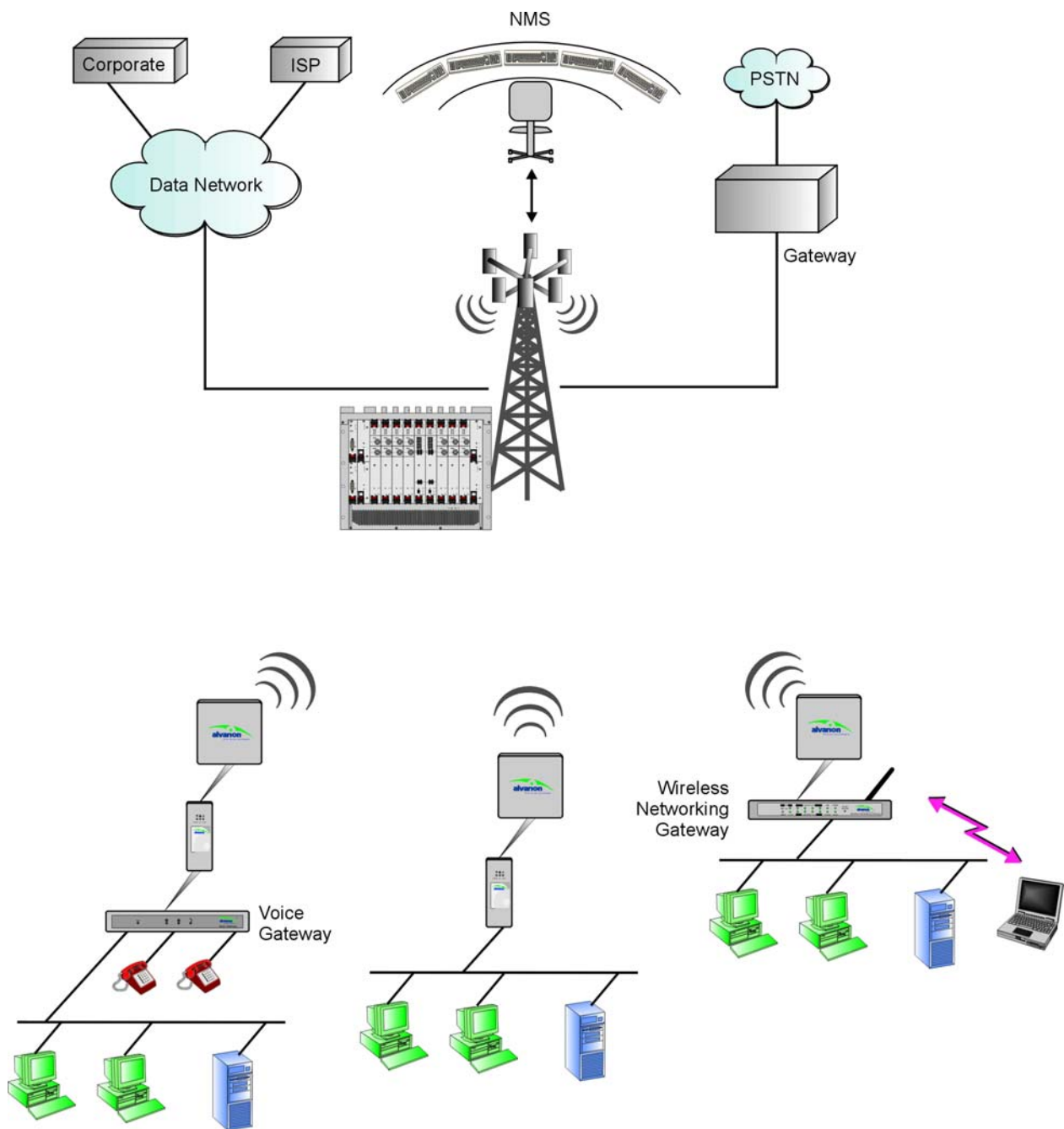


Figure 1-1: BreezeMAX System Architecture

1.2 Subscriber Units

The Subscriber Unit (SU) installed at the customer premises, comprises an Outdoor Unit (ODU) and an Indoor Unit (IDU).

The SU-ODU includes the modem, radio, data processing and management components of the SU, serving as an efficient platform for a wide range of services. It also includes an integral high-gain flat antenna or a connection to an external antenna, as described in Table 1-2. The SU-ODU provides data connections to the Access Unit (AU), providing bridge functionality, traffic shaping and classification. It connects to the IDU and to the user's equipment through a 10/100BaseT Ethernet port, and it can support up to 512 MAC addresses.



Table 1-2: Subscriber Unit ODU's Types

ODU Type	Description
BMAX-CPE-ODU-AV-3.5	Subscriber Outdoor Unit supporting the 3.5a and 3.5b bands with an integrated vertically polarized antenna
BMAX-CPE-ODU-AH-3.5	Subscriber Outdoor Unit supporting the 3.5a and 3.5b bands with an integrated horizontally polarized antenna
BMAX-CPE-ODU-E-3.5	Subscriber Outdoor Unit supporting the 3.5a and 3.5b bands with a connection to an external antenna

The indoor unit is powered from the mains and connects to the SU-ODU via a Category 5E Ethernet cable. This cable carries the Ethernet data between the two units as well as power (-54 VDC) and control signals to the SU-ODU. It also carries status indications from the SU-ODU.

There are two types of SU-IDUs:

- The BMAX-CPE-IDU-1D is the basic IDU, functioning as a simple interface unit with a 10/100BaseT Ethernet port that connects to the user's equipment.
- The IDU-NG-4D1W Wireless Networking Gateway IDU provides advanced routing capabilities and can also serve as a Wireless LAN Access Point.

1.3 Voice and Networking Gateways

The following Gateways are currently available from Alvarion:

- IDU-NG-4D1W: A Networking Gateway that serves also as an SU-IDU, supporting 4 data ports and 1 Wireless LAN port.
- VG-1D1V: A stand-alone (external) Voice Gateway, connecting to an SU-IDU and supporting 1 data port and 1 POTS port, with advanced routing functionality.
- VG-1D2V: A stand-alone (external) Voice Gateway, connecting to an SU-IDU and supporting 1 data port and 2 POTS ports, with advanced routing functionality.

Details on installing, managing and using the Voice Gateways and the Wireless Networking Gateway is provided separately in the relevant manuals.

These Gateways incorporate the proprietary DRAP protocol for automatic registration and allocation of resource.

1.3.1 DRAP (Dynamic Resources Allocation Protocol)

DRAP is a protocol based on IP/UDP between the Gateway (installed behind the SU) and the BreezeMAX system. The protocol provides an auto-discovery mechanism for the Gateway, so no specific configuration is required and the Gateway can automatically locate and register with the BreezeMAX base station. The protocol uses a few simple messages enabling a Voice Gateway to request resources when calls are made, and the BreezeMAX to dynamically allocate them.

1.3.2 IDU-NG-4D1W Wireless Networking Gateway IDU

Alvarion's Wireless Networking Gateway enables operators and service providers using Alvarion's BWA system to provide subscribers with a number of broadband services transparently.

The Wireless Networking Gateway IDU together with the SU-ODU comprises an SU that provides data connections to the Base Station. The four 10/100Base-T Ethernet ports connect to the user's data equipment, providing comprehensive routing functionality and supporting various security features. User's data equipment equipped with either IEEE 802.11b (11M) or IEEE 802.11g (54M) compatible wireless adapters can connect to the unit via its built-in Wireless LAN port, functioning as an Access Point.

The Wireless Networking Gateway IDU is powered from the mains and connects to the ODU via a Category 5E Ethernet cable. This cable carries the Ethernet data between the two units as well as power (54 VDC) and control signals to the ODU. It also carries status indications from the ODU.



The Wireless Networking Gateway is designed for remote management and supervision using either the built-in internal web server or SNMP.

The Wireless Networking Gateway is easily updated and upgraded as it supports remote software and configuration file download.

1.3.3 VG-1D1V and VG-1D2V Voice Gateways

Alvarion's Voice Gateways enable operators and service providers to offer end users a combination of IP-telephony and broadband data services.

IP-telephony services are supported for standard analog phones or G3 fax machines.

The VG-1D1V has a single POTS interface, and the VG-1D2V has two POTS interfaces.



The Voice Gateways is built on the H.323 and SIP standards and support both narrow (compressed) and wideband (uncompressed) speech codecs, silence suppression with comfort noise, line echo cancellation and regional telephone parameters. Class 5 services such call waiting and 3-party call are also supported.

Up to five telephones can be connected in series to each telephone port. Daisy chaining of Voice Gateways enables the service provider to offer certain end users, for example small offices, additional telephone numbers.

The Voice Gateway also supports Internet access or any other Ethernet based services, and can be configured to work in switch (layer 2) or router (layer 3) mode. The unit can be installed behind a router/NAT due to NAT traversal support allowing signaling as well as voice packets to correctly reach Softswitch or Gatekeeper for bi-directional call initiations. The Gateway can handle up to 16 simultaneous VLANs, enabling the operator to offer different services to different end users behind the unit.

The Voice Gateways are designed for remote management and supervision using either the built-in internal web server or SNMP.

The Voice Gateways are easily updated and upgraded as they support remote software and configuration file download.

1.4 Base Station Equipment

The BreezeMAX Base Station Equipment includes a modular Base Station that can serve up to six sectors and a stand-alone Micro Base Station. The Multi Carrier, High Power, Full Duplex Base Station and Micro Base Station provide all the functionality necessary to communicate with SUs and to connect to the backbone of the Service Provider.

1.4.1 Modular Base Station

The modular Base Station comprises the following elements:

1.4.1.1 Base Station Chassis

The Base Station Equipment is based on an 8U high cPCI (compact Peripheral Component Interconnect) shelf designed for installation in a 19" or 21" (ETSI) rack. This chassis has a total of nine double Euro (6U high) slots and six single Euro (3U high) slots. All the modules are hot swappable, and high availability can be provided through multiple redundancy schemes.



The six single Euro slots are intended for one or two redundant Power Interface Units (PIU) and up to four redundant Power Supply Units (PSUs).

One of the double Euro slots is dedicated to the Network Processing Unit (NPU) module, supporting a central networking and management architecture. Another double Euro slot is reserved for an optional redundant NPU (NPU redundancy support is planned for a future release).

The remaining seven double Euro slots are dedicated mainly for Access Unit (AU) indoor modules, thus enabling various future redundancy configurations. Each of these slots will also be able to host a Network Interface Unit (NIU) to allow for Nx1 or ATM backbone connectivity in future releases.

Additionally, the Base Station chassis contains an air convection and ventilation fan tray (AVU).

1.4.1.2 Network Processing Unit (NPU)

The Network Processing Unit is the “heart” of the BreezeMAX Base Station. The NPU module serves as the central processing unit that manages the base station’s components and the SUs served by it. It also aggregates the traffic from the AU modules and transfers it to the IP Backbone through a dedicated Gigabit/Fast Ethernet interface. The NPU main functions are:

- Aggregate backbone Ethernet connectivity via a 100/1000 Base-T network interface.
- Traffic classification and connection establishment initiation.
- Policy based data switching.
- Service Level Agreements management.
- Centralized agent in the Base Station to manage all cell site’s AUs and all registered SUs.
- Base Station overall operation control, including AU diagnostic and control, PSU monitoring, AVU management and redundancy support.
- Alarms management, including external alarm inputs and activation of external devices (future option).
- Synchronization, including GPS antenna interface (future option), clock and IF reference generation and distribution to the Base Station modules as well as to other collocated Base Station chassis.



An SNMP agent incorporated into the NPU enables extensive In Band (IB) management of the Base Station and all its registered SUs. Out Of Band (OOB) management is supported through a dedicated 10/100 Base-T interface. A serial RS-232 port supports local configuration, monitoring and debugging.

Two NPU modules can be used to provide a 1+1 redundancy scheme. The redundancy mechanism, to be supported in future releases, will be based on a Master <-> Slave principle, where the slave is in passive mode and is constantly updating all the learning tables and networking parameters of the master card.

1.4.1.3 Access Unit (AU)

The AU comprises an Indoor Unit (IDU) and an Outdoor Unit (ODU). The double Euro AU-IDU module connects to the AU-ODU via an Intermediate Frequency (IF) cable. The IF cable carries full duplex data, control and management signals between the AU-IDU and the AU-ODU, as well as power (48 VDC) and 64 MHz synchronization reference clock from the AU-IDU to the AU-ODU. The IF Tx and Rx frequencies are 240 MHz and 140 MHz, respectively. IDU-ODU service channel at 14 MHz serves for bi-directional control, status and management signaling.

1.4.1.3.1 AU-IDU

The double Euro AU-IDU module contains the wireless IEEE 802.16a MAC and modem and is responsible for the wireless network connection establishment and for bandwidth management. Each AU-IDU connects to the NPU via the back plane. In addition, each AU-IDU connects to all other AU/NIU slots via the back plane over a shared bus for future support of TDM traffic connectivity.

Each AU-IDU includes two 3.5/1.75 MHz PHY channels that provide provisioning to the planned support for a future release of 2nd order of diversity and IF and radio link redundancy. In the current release, a single channel is supported.



1.4.1.3.2 AU-ODU

The AU-ODU is a high power, full duplex multi-carrier radio unit that connects to an external antenna. It is designed to provide high system gain and interference robustness utilizing high transmit power and low noise figure. It supports a bandwidth of up to 14 MHz, enabling future options such as increased capacity through the use of a multiplexer or larger channels (e.g. 7/14MHz).



1.4.1.4 Power Interface Unit (PIU)



The single Euro PIU module is the interface between the Base Station site's DC power source and the Base Station chassis PSUs and external AU-ODUs, which receive power via the AU-IDUs.

The PIU filters and stabilizes the Base Station input power and protects the system from power problems such as over voltage, surge pulses, reverse polarity connection and short circuits. It also filters high frequency interference (radiated emissions) and low frequency interference (conducted emissions) to the external power source. Each Base Station chassis contains two slots for an optional 1+1 PIU redundancy. One

PIU is sufficient to support a fully populated chassis. Two PIU modules provide redundant power feeding (two input sources) while avoiding current flow between the two input sources.

1.4.1.5 Power Supply Unit (PSU)

The single Euro PSU module is a 48 VDC power supply unit. Each Base Station chassis can contain up to four PSU modules providing N+1 redundancy configurations.

Table 1-3 displays the number of PSU modules (excluding redundant units) required for various Base Station configurations without NPU redundancy (one NPU):



Table 1-3: PSU Requirements, Configurations with one NPU (excluding PSU redundancy)	
Number of AUs	Minimum Required Number of PSUs
1 - 2	1
3 - 6	2

Table 1-4 displays the number of PSU modules (excluding redundant units) required for various Base Station configurations with NPU redundancy (two NPUs, not supported in current version):

Table 1-4: PSU Requirements, Configurations with two NPUs (excluding PSU redundancy)	
Number of AUs	Minimum Required Number of PSUs
1 - 5	2
6	3

1.4.1.6 Air Ventilation Unit (AVU)

The 2U high AVU includes a 1U high integral chamber for inlet airflow and a 1U high fan tray with an internal alarm module. To support high availability Base Station, the fan tray includes 10 brush-less fans, where 9 fans are sufficient for cooling a fully loaded chassis. A failure in any of the fans is indicated by both the front panel LEDs and a trap that is sent to the management system. To further support high availability, the chassis may operate with the hot-swappable fan tray extracted from it for a period of time sufficient for replacing it (up 10 minutes).

1.4.2 Micro Base Station

The Micro Base Station Unit is designed to provide an alternative to the BreezeMAX Modular Base Station and a low cost solution in places where the number of subscribers is limited, and only one or two sectors are necessary (i.e. communities areas). The use of the same AU-ODU that is used by the modular Base Station provides an easy migration path and protection of the initial investment when the customer base increases and there is a need to replace the Micro Base Station with the full, modular Base Station equipment.

The Micro Base Station equipment comprises an indoor Micro Base Station Unit and an outdoor radio unit (AU-ODU).

1.4.2.1 Micro Base Station Indoor Unit

The Micro Base Station unit provides the full base station functionality necessary for serving a single sector. There are two different models: one is powered from the AC mains (110 or 220 VAC), and the other is powered from a -48 VDC power source. The functionality of the Micro Base station is very similar to the combined functionalities of NPU and AU-IDU modules of the modular Base Station.



The functionality of the Micro Base Station unit includes:

- Backbone Ethernet connectivity via a 10/100 Base-T network interface
- Traffic classification and connection establishment initiation
- Policy based data switching
- Service Level Agreements management
- Centralized agent for managing the Micro Base Station unit and all registered SUs
- Alarms management, including external alarm inputs and activation of external devices (future option).

An SNMP agent incorporated into the unit enables extensive In-Band (IB) management of the Micro Base Station and all its registered SUs. Out-Of-Band

(OOB) management is supported through a dedicated 10/100 Base-T interface. A serial RS-232 port supports local configuration, monitoring and debugging.

The Micro Base Station also contains the wireless IEEE 802.16a MAC and modem. It includes two 3.5/1.75 MHz PHY channels that provide provisioning to the planned support for a future release of 2nd order of diversity and IF and radio link redundancy. In the current release, a single channel is supported.

1.4.2.1.1 AU-ODU

The AU-ODU of the Micro Base Station, identical to the AU-ODU of the modular Base Station, is a high power, full duplex multi-carrier radio unit that connects to an external antenna. It is designed to provide high system gain and interference robustness utilizing high transmit power and low noise figure. It supports a bandwidth of up to 14 MHz, enabling future options such as increased capacity through the use of a multiplexer or larger channels (e.g. 7/14 MHz).

The Micro Base Station unit connects to the AU-ODU via an Intermediate Frequency (IF) cable. The IF cable carries full duplex data, control and management signals between the Micro Base Station and the AU-ODU, as well as power (48 VDC) and 64 MHz synchronization reference clock from the Micro Base Station IDU to the AU-ODU. The IF Tx and Rx frequencies are 240 MHz and 140 MHz, respectively. IDU-ODU service channel at 14 MHz serves for bi-directional control, status and management signaling.

1.5 Networking Equipment

The modular Base Station and the Micro Base Station equipment are connected to the backbone through standard data communication and telecommunication equipment. In the modular Base Station, the NPU aggregates the traffic from all AUs, connecting to the backbone through a 100/1000 Base-T port. The Micro Base Station connects to the backbone through a 10/100 Base-T port.

The point-to-point link from the Base Station/Micro Base Station to the backbone can be either wired or wireless.

1.6 Management Systems

The end-to-end IP-based architecture of the system enables full management of all components, using standard management tools. An SNMP agent in the NPU/Micro Base Station implements standard and proprietary MIBs for remote setting of operational modes and parameters of the NPU/Micro Base Station as well as all other system components that are managed by the NPU/Micro Base Station. The same SNMP management tools can also be used to manage other system components including switches, routers and transmission equipment. Security features incorporated in BreezeMAX units restrict the access for management purposes.

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

1.6.1 AlvariSTAR™

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

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

AlvariSTAR provides the following BWA network management functionality:

- Device Discovery
- Device Inventory
- Topology
- Fault Management
- Configuration Management
- Service Management

- Performance Monitoring
- Device embedded software upgrade
- Security Management
- Northbound interface to other Network Management Systems.

Embedded with the entire knowledge base of BWA network operations, AlvariSTAR is a unique state-of-the-art power multiplier in the hands of the service provider that enables the provisioning of satisfied customers. AlvariSTAR dramatically extends the abilities of the service provider to provide a rich portfolio of services and to support rapid customer base expansion.

1.7 Specifications

1.7.1 Radio

Table 1-5: Radio Specifications			
Item	Description		
Frequency	Unit/Band	Uplink (MHz)	Downlink (MHz)
	AU-ODU-3.5a	3399.5-3453.5	3499.5-3553.5
	AU-ODU-3.5b	3450-3500	3550-3600
	SU-ODU-3.5	3399.5-3500	3499.5-3600
Operation Mode	AU, Micro Base Station	FDD, Full duplex	
	SU	FDD, Half Duplex	
Channel Bandwidth	■ 3.5 MHz ■ 1.75 MHz		
Central Frequency Resolution	0.125 MHz		
SU-ODU-AV Integral Vertical Antenna	18 dBi, 15° AZ x 18° EL, vertical polarization, compliant with EN 302 085, V1.1.1 Range 1		
SU-ODU-AH Integral Horizontal Antenna	18 dBi, 18° AZ x 15° EL, horizontal polarization, compliant with EN 302 085 V1.1.2 Range 1		
Antenna Port (SU-ODU-E, AU-ODU)	N-Type, 50 ohm		
Max. Input Power (at antenna port)	AU-ODU	-60 dBm before saturation, -17 dBm before damage	
	SU-ODU	-20 dBm before saturation 0 dBm before damage	

Table 1-5: Radio Specifications					
Item	Description				
Output Power (at antenna port)	AU-ODU	28 dBm +/-1 dB maximum. Power control range: 15dB 18-28 dBm @ +/-1 dB, 13-18 dBm @ +/-2 dB			
	SU-ODU	20 dBm +/-1 dB maximum, ATPC Dynamic range: 40 dB			
Modulation	OFDM modulation, 256 FFT points; BPSK, QPSK, QAM16, QAM64				
FEC	Convolutional Coding: 1/2, 2/3, 3/4				
Bit Rate and Typical Sensitivity (PER=1%)	Channel Spacing	3.5 MHz bandwidth		1.75 MHz bandwidth	
	Modulation & Coding	Net Phy Bit rate (Mbps)	Sensitivity (dBm)	Net Phy Bit rate (Mbps)	Sensitivity (dBm)
	BPSK 1/2	1.41	-100	0.71	-103
	BPSK 3/4	2.12	-98	1.06	-101
	QPSK 1/2	2.82	-97	1.41	-100
	QPSK 3/4	4.23	-94	2.12	-97
	QAM16 1/2	5.64	-91	2.82	-94
	QAM16 3/4	8.47	-88	4.24	-91
	QAM64 2/3	11.29	-83.0	5.65	-86
	QAM64 3/4	12.71	-82.0	6.35	-85

1.7.2 Base Station Antennas (optional)

Table 1-6: Base Station Antennas Electrical Specifications	
Item	Description
BST ANT 3.5/60V	16 dBi, 60° AZ x 10° EL, vertical polarization, compliant with EN 302 085, V1.1.2 CS3
BST ANT 3.5/90V	14 dBi, 90° AZ x 8° EL, vertical polarization, compliant with EN 302 085, V1.1.1 CS3
BST ANT 3.5/60H	16 dBi, 60° AZ x 9° EL, horizontal polarization, compliant with EN 302 085, V1.1.1 CS3
BST ANT 3.5/90H	14 dBi, 85° AZ x 9° EL, vertical polarization, compliant with EN 302 085, V1.1.1 CS3
BST ANT 3.5/OMNI	10 dBi, 360° AZ x 8° EL, vertical polarization

1.7.3 SU IDU/ODU Communication

Table 1-7: SU IDU/ODU Communication	
Item	Description
Cable Type	Category 5E, Outdoor Data Cable, Double Jacket, 4x2x24# FTP
Maximum Length	100 meter

1.7.4 AU and Micro Base Station IDU/ODU Communication

Table 1-8: AU and Micro Base Station IDU/ODU Communication	
Item	Description
IF Frequency	<ul style="list-style-type: none"> ■ Tx: 240 MHz ■ Rx: 140 MHz
Ref Synchronization Frequency	64 MHz
Bi-Directional Control Frequency	14 MHz
IF cable Impedance	50 ohm
Maximum IF cable Attenuation	<ul style="list-style-type: none"> ■ 19 dB @ 240 MHz ■ 15 dB @ 140 MHz ■ 8 dB @ 64 MHz
Minimum IF cable Shielding Effectiveness	90 dB in the 10-300 MHz band
Maximum IF cable Return Loss	20 dB in the 10-300 MHz band
Maximum IF cable DC Resistance	4.0 ohm

1.7.5 Data Communication (Ethernet Ports)

Table 1-9: Data Communication (Ethernet Ports)		
Item	Description	
Standard Compliance	IEEE 802.3 CSMA/CD	
Speed	NPU Data Port	100/1000 Mbps, Full Duplex
	Micro Base Station Data Port	10/100 Mbps, Full Duplex
	NPU/Micro Base Station Management Port	10/100 Mbps, Half/Full Duplex with Auto Negotiation
	SU Data Port	10/100 Mbps, Half/Full Duplex with Auto Negotiation

1.7.6 Configuration and Management

Table 1-10: Configuration and Management	
Item	Description
SU Local Management (OOB)	Telnet via the Ethernet port
NPU/Micro Base Station Out Of Band (OOB) Management	<ul style="list-style-type: none"> ■ Telnet via Management port ■ SNMP via Management port ■ Monitor port
NPU/Micro Base Station In Band (IB) Management via Data Port	<ul style="list-style-type: none"> ■ SNMP ■ Telnet
SNMP Agents	SNMP ver 1 client MIB II (RFC 1213), Private BreezeMAX MIBs
Authentication	X509v3 digital certificate
Software upgrade	Using TFTP via NPU/Micro Base Station
Configuration upload/download	Using TFTP via NPU/Micro Base Station

1.7.7 Standards Compliance, General

Table 1-11: Standards Compliance, General	
Type	Standard
EMC	ETSI EN 300 489-1
Safety	<ul style="list-style-type: none"> ■ EN 60950 (CE) ■ IEC 60 950 US/C (TUV)
Environmental	ETS 300 019: <ul style="list-style-type: none"> ■ Part 2-1 T 1.2 & part 2-2 T 2.3 for indoor & outdoor ■ Part 2-3 T 3.2 for indoor ■ Part 2-4 T 4.1E for outdoor
Radio	<ul style="list-style-type: none"> ■ ETSI EN 301 021 V.1.5.1 ■ ETSI EN 301 753 V.1.1.1

1.7.8 Environmental

Table 1-12: Environmental Specifications		
Type	Unit	Details
Operating temperature	Outdoor units	-40°C to 55°C
	Indoor equipment	0°C to 40°C
Operating humidity	Outdoor units	5%-95% non condensing, Weather protected
	Indoor equipment	5%-95% non condensing

1.7.9 Services

Table 1-13: Services	
Item	Description
Max number of Services per BST/ μ BST	BST: 4,095 μ BST: 1,023 (One or several services may be defined per subscriber, one or more subscribers can be supported per SU)
Min number of data connections per Service	2 (1 uplink, 1 downlink)
Max number of data connections per Service	8 (4 uplink, 4 downlink)
Max number of data connections per SU	126
Max number of data connections per AU/ μ BST	3999 - 3 x number of SUs (3 connections are reserved for each SU)
Max number of SUs per AU	510
Max number of SUs per μ BST	254
Max number of AUs per BST	7

Table 1-13: Services	
Item	Description
Max number of MAC addresses in Bridging Table	BST: 6,000 μ BST: 1,000 SU: 512 (Aging time is configurable. The default is 3 minutes for SU, 10 minutes for NPU/ μ BST)
Max number of VLANs per Service	16
Max number of VLANs per BST/ μ BST	1,024
Max number of concurrent calls per Voice Service	10
Max number of MAC Addresses forwarded by SU	512

1.7.10 Physical and Electrical

1.7.10.1 Subscriber Unit

1.7.10.1.1 Mechanical

Table 1-14: Mechanical Specifications, Subscriber Unit		
Unit	Dimensions (cm)	Weight (kg)
CPE-IDU-1D	14 x 6.6 x 3.5	0.3
CPE-ODU-AV/AH	31.5 x 11 x 31.5	3
CPE-ODU-E	31.5 x 8.8 x 15.7	2.4

1.7.10.1.2 Connectors

Table 1-15: Connectors, Subscriber Unit		
Unit	Connector	Description
CPE-IDU-1D	ETHERNET	10/100Base-T (RJ-45). Cable connection to a PC: Straight Cable connection to a hub: Crossed
	RADIO	10/100Base-T (RJ-45)
	AC IN	3 pin AC power plug
CPE-ODU-AV/AH	INDOOR	10/100Base-T (RJ-45), protected by a waterproof sealing assembly
CPE-ODU-E	INDOOR	10/100Base-T (RJ-45), protected by a waterproof sealing assembly
	ANT	N-Type jack, 50 ohm, lightning protected

1.7.10.1.3 Electrical

Table 1-16: Electrical Specifications, Subscriber Unit	
Item	
Power Consumption (including ODU)	44W
CPE-IDU Power Input	100-240 VAC, 47-63 Hz
CPE-ODU Power Input	54 VDC from the IDU over the indoor-outdoor Ethernet cable

1.7.10.2 Modular Base Station Equipment

1.7.10.2.1 Mechanical

Table 1-17: Mechanical Specifications, Modular Base Station Equipment		
Unit	Dimensions (cm)	Weight (kg)
BST-SH	8U ETSI type shelf, 8U x 43.19 x 24	6.9 (excluding AVU)
PIU	3U x 5HP x 16	0.35
PSU	3U x 8HP x 16	0.7
NPU	6U x 7HP x 16	0.7
AU-IDU	6U x 7HP x 16.	0.6
AU-ODU	31.5 x 8.8 x 15.7	2.9
AVU	2U x 84HP x 16	1.7

* 1U=44.45 mm (1.75”), 1HP=5.08 mm (0.2”)

1.7.10.2.2 Electrical

Table 1-18: Electrical Specifications, Modular Base Station Equipment	
Unit	Details
Power Source	-40.5 to -60 VDC
Full Base station (including ODUs)	671W maximum for a fully equipped base station, including ODUs (1 NPU, 6 AUs with 1 ODU per AU, 1+1 PIUs, 2+1 PSUs)
Full Chassis (excluding ODUs)	479W maximum for a fully equipped chassis, excluding ODUs (1 NPU, 6 AU-IDUs, 1+1 PIUs, 2+1 PSUs)
PIU	16W maximum
PSU	200W maximum output power Efficiency: 75% minimum, 80% typical
NPU	65W maximum, 44W typical
AU-IDU	41W maximum, 29W typical
AU-ODU	32W maximum, 27W typical
AVU	24W maximum, 23W typical

1.7.10.2.3 Connectors

Table 1-19: Connectors, Modular Base Station Equipment		
Unit	Connector	Description
PIU	-48V	3 pin/40A D-Type male Amphenol P/N 717TWA3W3PHP2V4RRM6
NPU	DATA	100/1000Base-T (RJ-45) with 2 embedded LEDs. Cable connection to a PC: Crossed Cable connection to a hub: Straight
	MGMT	10/100Base-T (RJ-45) with 2 embedded LEDs. Cable connection to a PC: crossed Cable connection to a hub: Straight
	GPS/SYNC IN	15-pin micro D-Type jack
	GPS/SYNC OUT	15-pin micro D-Type jack
	AL-IN	9-pin micro D-Type jack
	AL-OUT	9-pin micro D-Type jack
	MON	3-pin low profile jack
AU-IDU	ODU 1, ODU 2	2 x TNC jack, lightning protected
AU-ODU	IF	TNC jack, lightning protected
	ANT	N-Type jack, 50 ohm, lightning protected

1.7.10.3 Micro Base Station Equipment

1.7.10.3.1 Mechanical

Table 1-20: Mechanical Specifications, Micro Base Station Equipment		
Unit	Dimensions (cm)	Weight (kg)
Micro Base Station IDU	1U ETSI type shelf, 1U x 44.4 x 27.2	3
AU-ODU	31.5 x 8.8 x 15.7	2.9

* 1U=44.45 mm (1.75")

1.7.10.3.2 Electrical

Table 1-21: Electrical Specifications, Micro Base Station Equipment	
Unit	Details
Power Source	AC model: 85 – 265 VAC, 47 – 63 Hz DC model: -40.5 to -60 VDC
Micro Base Station IDU Power Consumption	85W maximum
AU-ODU Power Consumption	32W maximum, 27W typical

1.7.10.3.3 Connectors

Table 1-22: Connectors, Micro Base Station Equipment		
Connector		Description
Micro Base Station IDU	AC IN (on rear panel of AC model)	3 pin AC power outlet
	DC IN (on rear panel of DC model)	3 pin D-Type male Amphenol P/N 17TWA3W3PR157
	DATA	10/100Base-T (RJ-45) with 2 embedded LEDs. Cable connection to a PC: crossed Cable connection to a hub: Straight
	MGMT	10/100Base-T (RJ-45) with 2 embedded LEDs. Cable connection to a PC: crossed Cable connection to a hub: Straight
	ALRM IN	9-pin micro D-Type jack
	ALRM OUT	9-pin micro D-Type jack
	MON	3-pin low profile jack
	ODU 1, ODU 2	2 x TNC jack, lightning protected
AU-ODU	IF	TNC jack, lightning protected
	ANT	N-Type jack, 50 ohm, lightning protected

1.7.10.4 Base Station Antennas

Table 1-23: Mechanical Specifications, Base Station Antennas			
Unit	Description	Dimensions (cm)	Weight (kg)
BST ANT 3.5/60V	Mounting kit: 2" to 4" pole. Connector: N-Type female	50 x 20 x 3	1.5
BST ANT 3.5/90V	Mounting kit: 2" to 4" pole. Connector: N-Type female	60 x 25 x 5.5	2
BST ANT 3.5/60H	Mounting kit: 2" to 4" pole. Connector: N-Type female	48 x 20 x 4	2
BST ANT 3.5/90H	Mounting kit: 2" to 4" pole. Connector: N-Type female	60 x 25 x 5.5	2
BST ANT 3.5/OMNI	Mounting bracket: 30 to 53 mm pole Connector: N-Type female	68 x 3.4 diameter	0.8

Chapter 2 - Installation

In This Chapter:

- [Installing the ODU](#), page 32
- [Installing the Modular Base Station Equipment](#), page 43
- [Installing the Micro Base Station Equipment](#), page 60
- [Installing the CPE-IDU-1D Indoor Unit](#), page 65

2.1 Installing the ODU

The following sections describe how to install the outdoor units of the CPE (SU-ODU) and of the Base Station equipment (the AU-ODU is the outdoor unit of each AU-IDU in the modular Base Station and of the Micro Base Station), including pole mounting the ODU, and connecting the cables.

2.1.1 ODU Installation Requirements

2.1.1.1 AU-ODU Packing List

■ ODU:

- ◇ BMAX-BST-AU-ODU-3.5a, AU-ODU operating in the 3.5a band

OR

- ◇ BMAX-BST-AU-ODU-3.5b, AU-ODU operating in the 3.5b band

■ Pole mounting kit

2.1.1.2 SU-ODU Packing List

■ ODU:

- ◇ BMAX-CPE-ODU-AV-3.5, a CPE ODU with an integral vertically polarized antenna

OR

- ◇ BMAX-CPE-ODU-AH-3.5, a CPE ODU with an integral horizontally polarized antenna

OR

- ◇ BMAX-CPE-ODU-E-3.5, a CPE ODU with a connector to an external antenna (not included)

■ Pole mounting kit

2.1.1.3 Additional Installation Requirements

The following items are also required to install the ODU:

- For AU-ODU: IF cable with two TNC connectors* (see [IF Cables](#) on page 35 for details on IF cable types and length).
- For SU-ODU: Indoor-to-outdoor Category 5E Ethernet cable with two shielded RJ-45 connectors* (see [Subscriber Unit's IDU-ODU Cables](#) on page 36 for details on approved cables and maximum length), and an RJ-45 connectors crimping tool.
- For units that connect to an external antenna: Antenna* and RF cable* for connecting the antenna to the ODU
- Grounding cable with an appropriate termination.
- Installation tools and materials, including appropriate means (e.g. a 1" to 4" pole) for installing the ODU (and antenna where applicable).



NOTE

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

2.1.2 Guidelines for Positioning the ODU

This section provides key guidelines for selecting the optimal installation locations for the various BreezeMAX components.



CAUTION

ONLY experienced installation professionals who are familiar with local building and safety codes and, wherever applicable, are licensed by the appropriate government regulatory authorities should install outdoor units and antennas.

Failure to do so may void the BreezeMAX product warranty and may expose the end user or Service Provider to legal and financial liabilities. Alvarion and its resellers or distributors are not liable for injury, damage or regulation violations associated with the installation of Outdoor Units or antennas.

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

- The ODU can be either pole or wall mounted. Its location should enable easy access to the unit for installation and testing.
- The higher the placement of the antenna, the better the achievable link quality.
- The antenna of the Access Unit/Micro Base Station should be installed so as to provide coverage to all Subscriber Units within its service area.



NOTE

The recommended minimum distance between any two antennas is 0.5 meters.

- The antenna of the SU should be installed to provide a direct, or near line of sight with the Base Station antenna. The antenna should be aligned to face the Base Station.
- Outdoor units with a connection to an external antenna should be installed as close as possible to the antenna.

2.1.3 IF Cables

The AU-ODU is connected to the AU-IDU/Micro Base Station via an IF cable carrying both signals and power. The maximum permitted attenuation of the IF cable at applicable frequencies, its screening effectiveness and its maximum permitted DC resistance (the sum of the DC resistance of the inner and outer conductors) are provided in Table 2-1.

Table 2-1: IF Cables Requirements	
Item	Description
Screening Effectiveness	90 dB minimum in the 10-300 MHz band.
IF cable Impedance	50 ohm
Maximum IF cable Attenuation	<ul style="list-style-type: none"> ■ 19 dB @ 240 MHz ■ 15 dB @ 140 MHz ■ 8 dB @ 64 MHz
Maximum IF cable DC Resistance	4.0 ohm
Maximum IF cable Return Loss	20 dB in the 10-300 MHz band

To comply with the required screening effectiveness requirement, it is recommended to use double shielded cables. Table 2-2 provides details on maximum length for some popular cables.

Table 2-2: Maximum IF Cable Length (Double Shielded Cables)	
Cable	Maximum Length
LMR-195	80 meters
LMR-240	150 meters

2.1.4 SU's IDU-ODU Cables



NOTE

The length of the Indoor-to-Outdoor cable, together with the length of the Ethernet cable connecting the CPE-IDU-1D to the data equipment, should not exceed 100 meters.

Use only Category 5E Ethernet cables from approved manufacturers, listed in Table 2-3. Consult with Alvarion specialists on the suitability of other cables.

Table 2-3: Approved Category 5E Ethernet Cables	
Manufacturer	Part Number
Superior Cables Ltd. www.cvalim.co.il	612098
HES Cabling Systems www.hescs.com	H5E-00481
Southbay Holdings Limited 11 th Fl., 15, Lane 347, Jong Jeng Rd. Shin Juang City, Taipei County Taiwan, R.O.C. Attn: Eva Lin Tel. 886-2-2832 3339 Fax. 886-2-2206 0081 E-mail: eva@south-bay.com.tw	TSM2404A0D
Teldor www.teldor.com	8393204101

2.1.5 Pole Mounting the Outdoor Unit

The Outdoor Unit can be mounted on a 1" to 4" pole using one of the following options:

- Special brackets and open-ended bolts are supplied with each unit. There are two pairs of threaded holes on the back of the unit, enabling the special brackets to be mounted on diverse pole diameters.
- The protrusions with grooves on the top backsides of the unit, and the protrusion on the bottom backside, enable the use of 9/16 inches wide metal bands (not included with the package) to secure the unit to a pole.

NOTE

Install the unit with the bottom panel, which includes the LEDs, facing downward.



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

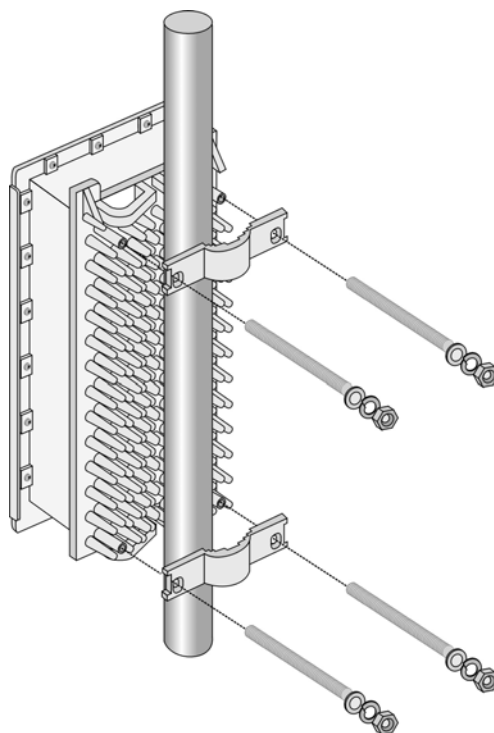


Figure 2-2: ODU Pole Installation Using Special Brackets

NOTE

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



Figure 2-3 illustrates the method of mounting an outdoor unit on a pole, using metal bands.

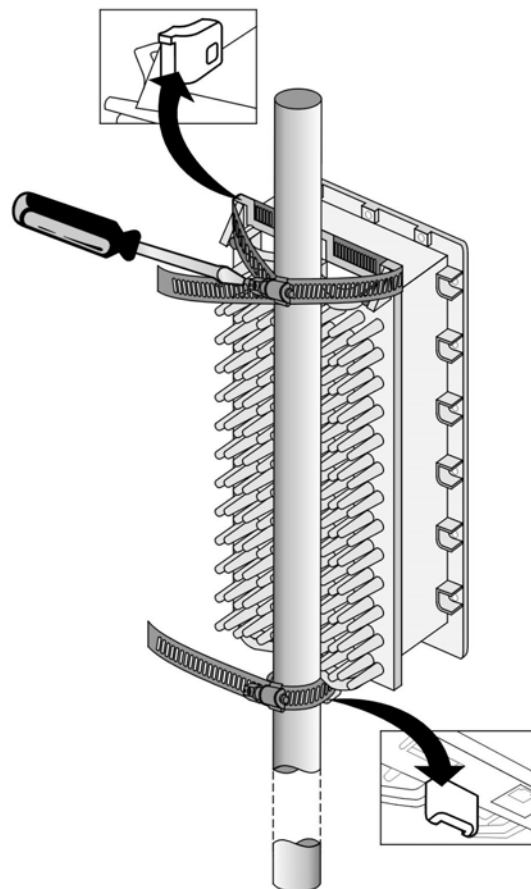


Figure 2-3: ODU Pole Installation Using Metal Bands

2.1.6 AU-ODU

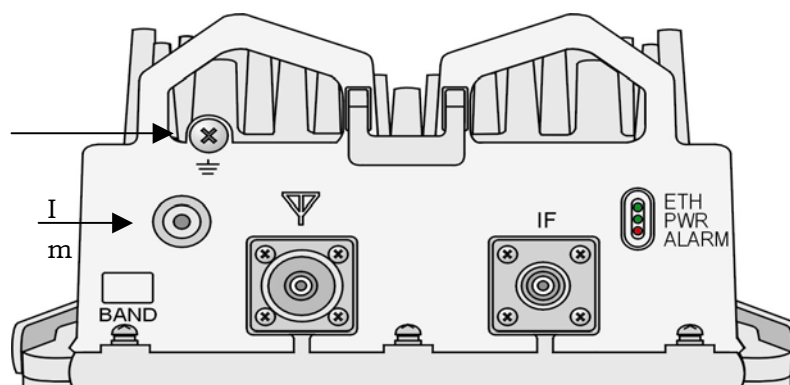


Figure 2-4: Bottom Panel of the AU-ODU



CAUTION

Do not open the impermeability test screw – you may impair the sealing of the unit against moisture and humidity.

Table 2-4: AU-ODU LEDs

Name	Description	Functionality
PWR	Power indication	<ul style="list-style-type: none"> ■ Off – ODU is not powered ■ Green – ODU power OK
ALARM	Not Used	(Red – blinks shortly during ODU power up)
ETH (WLNK)	Wireless link status indication	<ul style="list-style-type: none"> ■ Off – No SU is associated ■ Green – At least one SU is associated

Table 2-5: AU-ODU Connectors

Name	Connector	Functionality
IF	TNC jack	Connection to the AU-IDU/Micro Base Station
Y (ANT)	N-Type jack, 50 ohm	Connection to an external antenna

2.1.7 SU-ODU

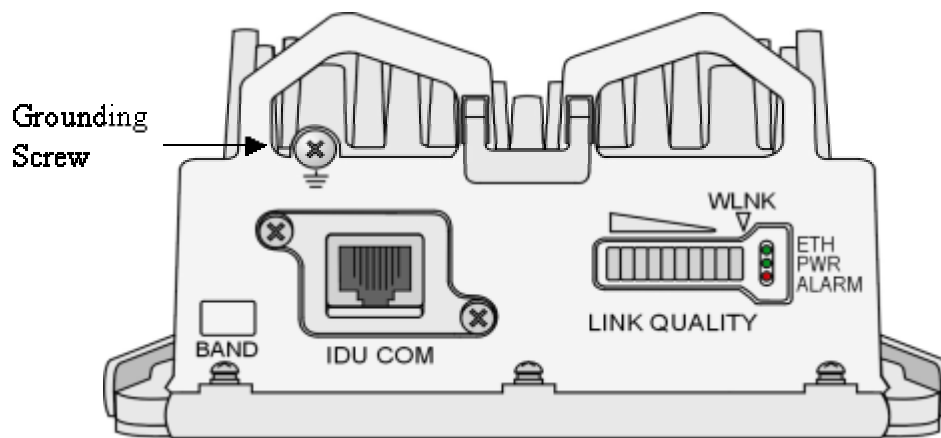




Figure 2-5: Bottom Panel of the SU-ODU (Without the Service Box)

Table 2-6: SU-ODU LEDs		
Name	Description	Functionality
PWR	Power indication	<ul style="list-style-type: none"> ■ Off – ODU is not powered ■ Green – ODU power is OK
ALARM	Alarm indication	<ul style="list-style-type: none"> ■ Off – ODU is OK, diagnostic test passed ■ Red – ODU failure
ETH	Ethernet link status indication (Ethernet integrity)	<ul style="list-style-type: none"> ■ Off – No Ethernet connectivity has been detected between the outdoor unit and the device connected to the indoor unit. ■ Green – Ethernet connectivity has been detected between the outdoor unit and the device connected to the indoor unit
LINK QUALITY bar display	Wireless link status and signal quality Indication	<ul style="list-style-type: none"> ■ LED 1 (orange): WLNK (wireless link status) – on when the SU is associated with and receives services from AU/μBST. ■ LED 2 – LED 9 (green): Link quality ■ LED 10 (red): Saturation (RSSI > -20 dBm) <p>See also Table 3-12.</p>

Table 2-7: SU-ODU Connectors		
Name	Connector	Functionality
IDU COM	10/100Base-T (RJ-45)	Connection to the SU-IDU
 (ANT) (only in SU-ODU-E)	N-Type jack, 50 ohm	Connection to an external antenna

2.1.8 Connecting the Cables

2.1.8.1 Connecting the Grounding Cable

The Grounding screw (marked ) is located on the bottom panel of the outdoor unit.




To connect the grounding cable:

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

2.1.8.2 Connecting the Antenna Cable



To connect the RF cable (units with external antenna):

- 1 Connect one end of the coaxial RF cable to the RF connector (marked ) located on the bottom panel of the unit.
- 2 Connect the other end of the RF cable to the antenna.
- 3 The RF connectors should be properly sealed to protect against rain and moisture.

2.1.8.3 Connecting the AU-ODU's IF Cable



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 AU-IDU/Micro Base Station. See IF cable length limitation in [IF Cables](#) on page 35.

- 3 The IF cable connector should be properly sealed to protect against rain and moisture.
- 4 Route the cable to the location selected for the indoor equipment.

2.1.8.4 Connecting the SU's IDU-ODU Cable



CAUTION

Use only Category 5E 4x2x24# FTP outdoor cables from an approved manufacturer. See list of approved cables in Table 2-3 on page 36.



To connect the IDU-ODU cable:

- 1 Remove the two screws holding the waterproof service box to the outdoor unit and remove the service box.
- 2 Unscrew the top nut from the service box.
- 3 Route a straight, uncrimped Category 5E Ethernet cable (8-wire, 24 AWG) through both the top nut and the body of the service box.
- 4 Insert and crimp the RJ-45 connector. Refer to [Appendix A](#) for instructions on preparing the cable.
- 5 Connect the Ethernet cable to the IDU COM RJ-45 connector.
- 6 Reposition the service box and then tighten the top nut. Make sure that the external jack of the cable is well inside the service box to guarantee a good seal.
- 7 Route the cable to the location selected for the indoor equipment.
- 8 Assemble an RJ-45 connector with a protective cover on the indoor end of the IDU-ODU cable.



NOTE

The length of the Indoor-to-Outdoor cable, together with the length of the Ethernet cable connecting the CPE-IDU-1D to the data equipment, should not exceed 100 meters.

2.2 Installing the Modular Base Station Equipment

2.2.1 BST Installation Requirements

2.2.1.1 Packing List

- Base Station Chassis:
 - ◇ BMAX-BST-SH Base Station Chassis
 - ◇ BMAX-BST-AVU Air Ventilation Unit (installed)
 - ◇ Cables Tray kit
 - ◇ 2.5 meter DC cable
- BMAX-BST-PIU (1 or 2 per chassis) Power Interface Unit(s)
- 2.5 meter DC cable (for a redundant PIU. One cable is supplied with each chassis)
- BMAX-BST-PSU (up to 4 per chassis) Power Supply Unit(s)
- BMAX-BST-NPU Network Processing Unit and Monitor cable
- BMAX-BST-AU-IDU (up to 6 per chassis) Access Unit Indoor Unit(s)

2.2.1.2 Additional Installation Requirements

The following items are also required to install the BST:

- Ethernet cable (straight) for connecting the NPU to a Hub/Switch.



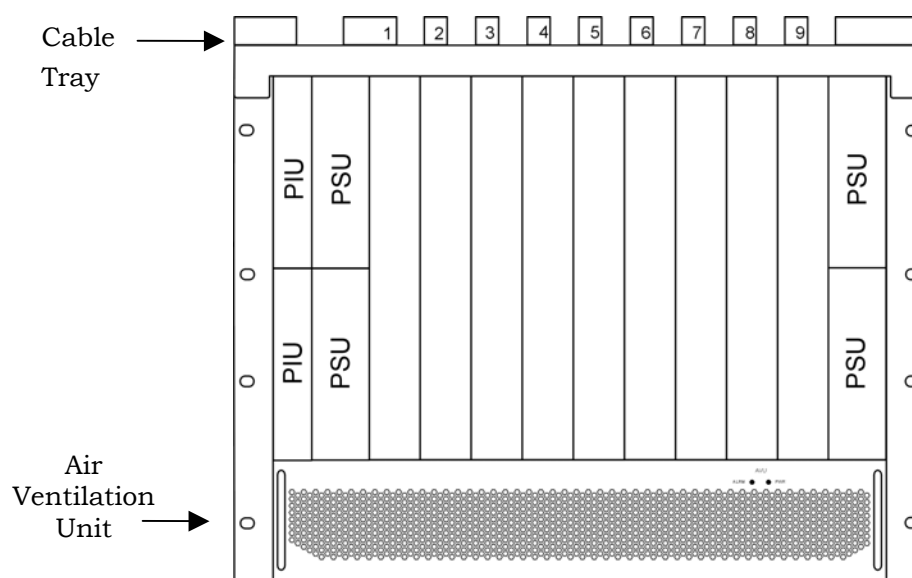
NOTE

The maximum length of the Ethernet cable is 100m when operating at 100 Mbps and 70m when operating at 1 Gbps.

- A grounding cable with appropriate terminations for connecting the chassis to the rack or another ground (earth) connection.
- For installation in a 21" ETSI rack: Two 21" ETSI rack adapters

- A portable PC for configuring parameters using the Monitor cable (supplied with the NPU)
- Other installation tools and materials

2.2.2 BMAX-BST-SH Chassis Slot Assignments



The Base Station chassis comprises 6 3U high slots and 9 6U high slots, as shown in Figure 2-6.

Figure 2-6: BMAX-BST-SH Chassis Slot Assignments

The Cable Tray (the installation kit is supplied with the chassis) should be installed on the top of the chassis front to enable convenient routing of cables connecting to power source(s), outdoor unit(s) and other equipment.

To enable power source and/or Power Interface Unit 1+1 redundancy, two PIU modules can be installed in the designated slots. If a single PIU module is used, it can be inserted into either one of the two available slots.

The number of installed PSU modules depends on the specific configuration (number of AUs) and NPU redundancy scheme (refer to Table 2-10 and Table 2-11 on page 48). If less than 4 PSU modules are used, they can be installed in any of the designated slots.

The NPU should be installed in slot number 5 (slot numbers are marked on the Cable Guide). Slot 6 is reserved for a future redundant NPU.

Slots 1-4 and 7-9 can hold up to six AU-IDU modules.

Unused slots should remain covered until required.

2.2.3 Power Requirements

Use the following table to calculate power source requirements for the Modular Base Station equipment:

Table 2-8: Power Requirements, Modular Base Station Equipment	
Unit	Details
Power Source	-40.5 to -60 VDC
PIU	16W maximum
PSU	200W max output power Efficiency: 80% typical
NPU	65W maximum
AU-IDU	41W maximum
AU-ODU	32W maximum
AVU	24W maximum



NOTE

The PSU(s) do not supply power to the AU-ODUs that are powered directly from the power source via the PIU and the back plane.

2.2.4 Power Interface Unit (PIU)

The single Euro PIU module is the interface between the Base Station site's DC power source and the Base Station Chassis Power Supply Units and external ODUs, which receive power via the IDUs.

The PIU filters and stabilizes the Base Station input power and protects the system from power problems such as over voltage, surge pulses, reverse polarity connection and short circuits. It also filters high frequency interference (radiated emissions) and low frequency interference (conducted emissions) to the external power source. Each Base Station chassis contains two slots for an optional 1+1 PIU redundancy. One PIU is sufficient to support a fully populated chassis. Two PIU modules provide redundant power feeding (two input sources) while avoiding current flow between the two input sources.

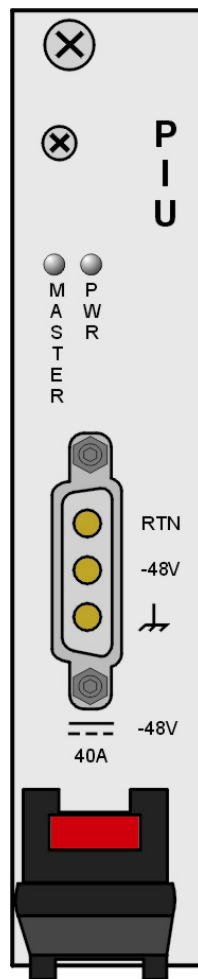


Figure 2-7: PIU Module Front Panel

Table 2-9: PIU LEDs		
LED Status		LED Status
PWR	MASTER	
Off	Off	Chassis is not connected to power.
Red	Off	Power is not connected or power input is out of range or PIU card is damaged. Chassis is powered by the redundant PIU.
Red	Green	Power input is out of range or PIU card is damaged. Chassis is powered by the PIU.
Green	Off	Power to PIU is OK. PIU is in redundant mode and the chassis is powered from the other PIU.
Green	Green	Power to PIU is OK. The chassis is powered from the PIU.

2.2.4.1 Preparing a Power Cable

A 2.5m DC power cable is supplied with each chassis. Additional DC cables can be ordered from Alvarion. If necessary, use the following instruction to prepare a DC cable.



To prepare the power cable:

- 1 Use a cable capable of supporting a current of at least 40A. Use a cable with 2 x 8AWG (or thicker) wires for the power plus an additional 8AWG to 20AWG ground wire.
- 2 The matching power connector to be used is Amphenol D-type power P/N 177TWA/3W3/SP3Y with high power socket contacts P/N 17DM53744-1.
- 3 Connect the cable to the power connector as follows:
 - ◇ Pin 1 (RTN): Red (8 AWG min wire)
 - ◇ Pin 2 (-48V): Black (8 AWG min wire)
 - ◇ Pin 3 (⚡): Ground (shield) (8AWG-20AWG wire)
- 4 Attach suitable terminal rings to the side that connects to the power source.



CAUTION

Disconnect power from the PIU module before inserting/ejecting it to/from the chassis. Before disconnecting the power cable from the PIU, the power source must be disconnected to avoid irreversible damage due to a potential excessively high transient current.

2.2.5 Power Supply Unit (PSU)

The single Euro PSU module is a 48 VDC power supply unit. Each Base Station chassis can contain up to four PSU modules providing N+1 redundancy configurations.

The following tables display the number of PSU modules (excluding redundant units) required for various Base Station configurations:

Table 2-10: PSU Requirements, Configurations with one NPU (excluding PSU redundancy)	
Number of AUs	Minimum Required Number of PSUs
1 - 2	1
3 - 6	2

Table 2-11: PSU Requirements, Configurations with two NPUs (excluding PSU redundancy)	
Number of AUs	Minimum Required Number of PSUs
1 - 5	2
6	3

NOTE



The PSU(s) do not supply power to the AU-ODUs that are powered directly from the power source via the PIU and the back plane.

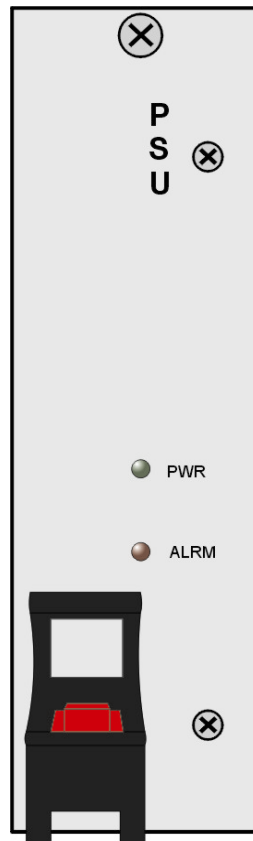


Figure 2-8: PSU Module Front Panel

Table 2-12: PSU LEDs		
LED Status		Description
PWR	ALRM	
Off	Off	No power or fatal damage
Off	Red	Power input is out of range or PSU is damaged or PSU is inhibited by NPU.
Green	Off	Power is OK and PSU operates properly.

2.2.6 Access Unit Indoor Module (AU-IDU)

The double Euro Access Unit IDU module contains the wireless IEEE 802.16a MAC and modem and is responsible for the wireless network connection establishment and for bandwidth management. Each AU-IDU includes two 3.5/1.75 MHz PHY channels that provide provisioning to the planned support for a future release of 2nd order of diversity and IF and radio link redundancy.

In the current release, a single channel (ODU 1) is supported.

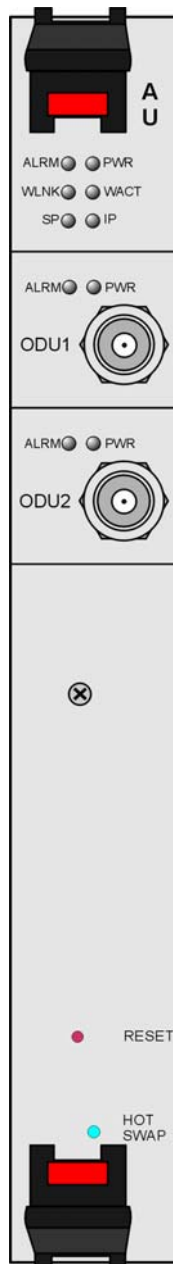


Figure 2-9: AU-IDU Module Front Panel

Table 2-13: AU-IDU LEDs		
Name	Description	Functionality
PWR	Power indication	<ul style="list-style-type: none"> ■ Off – AU-IDU is not powered ■ Red – AU-IDU power supply failed (low power) ■ Green – AU-IDU power is OK
ALARM	Alarm indication	<ul style="list-style-type: none"> ■ Off – AU-IDU is OK ■ Red – AU-IDU failure
WLINK	Wireless link status indication	<ul style="list-style-type: none"> ■ Off – No SU is associated ■ Green – At least one SU is associated
WACT	IDU transmission indication	<ul style="list-style-type: none"> ■ Off – No IDU transmission ■ Green – IDU transmission OK
SP	Spare	Not Used
IP	IP activity indication	<ul style="list-style-type: none"> ■ Off – No downlink (AU to SU) IP activity ■ Green (blinking) – Downlink (AU to SU) IP activity
ODU1/ODU2 PWR	IDU to ODU Power Indication	<ul style="list-style-type: none"> ■ Off – No IDU to ODU power output ■ Red – IDU to ODU power output failed ■ Green – IDU to ODU power output OK
ODU1/ODU2 ALRM		<ul style="list-style-type: none"> ■ Off – IDU-ODU communication OK ■ Red - IDU-ODU communication failure

2.2.7 Network Processing Unit (NPU)

The NPU module serves as the central processing unit that manages the base station's components and the SUs served by it. It also aggregates the traffic from the AU modules and transfers it to the IP backbone through a dedicated Gigabit/Fast Ethernet interface.

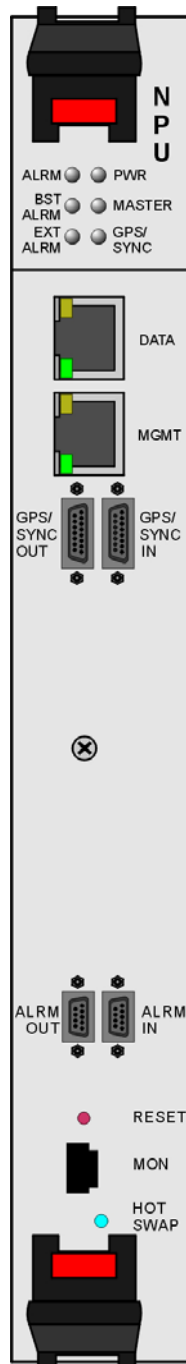


Figure 2-10: NPU Module Front Panel

Table 2-14: NPU Connectors		
Name	Connector	Functionality
DATA	100/1000Base-T (RJ-45) with 2 embedded LEDs.	Connection to the backbone. Cable connection to a hub/switch/router: Straight
MGMT	10/100Base-T (RJ-45) with 2 embedded LEDs.	Connection to OOB management. Cable connection to a PC: Crossed Cable connection to a hub/switch/router: Straight
GPS/SYNC IN	15-pin micro D-Type jack	Not used currently. Connection to a GPS receiver or to an NPU in another chassis that supplies synchronization signals.
GPS/SYNC OUT	15-pin micro D-Type jack	Not used currently. Supply of synchronization signals to another unit.
ALRM-IN	9-pin micro D-Type jack	Not used currently. Connections to external alarm indicators (3 alarm inputs, NC or NO).
ALRM-OUT	9-pin micro D-Type jack	Not used currently. Connections for activation of external devices (4 dry contact pairs).
MON	3-pin low profile jack	Access for debugging and configuration using the Monitor program.

Table 2-15: NPU LEDs		
Name	Description	Functionality
PWR	Power indication	<ul style="list-style-type: none">■ Off – NPU is not powered■ Red – NPU power failure■ Green – NPU power is OK
ALRM	NPU Alarm indication	<p>Off – NPU is OK</p> <p>Red – NPU failure</p>
BST ALRM	Base Station chassis alarm indication	<p>Off – All Base Station modules are OK</p> <p>Red – Failure in one (or more) Base Station modules</p>
EXT ALRM	External alarm indication	<p>Off – No alarms</p> <p>Red – Alarm received via the ALRM IN connector</p>
MASTER	Master/Slave operation indication	<ul style="list-style-type: none">■ Off – Secondary NPU (backup)■ Green – Primary NPU
GPS/SYNC	GPS/IF clock synchronization functionality indication	<ul style="list-style-type: none">■ Off – GPS/IF clock synchronization is disabled■ Green – GPS/IF clock is synchronization enabled

2.2.8 Using the Hot-Swap Injector/Ejector Handles

The Base Station modules include special handles for high-force insertion/extraction of modules. Each of the 6U high modules (NPU, AU-IDU) includes two such handles, whereas each of the 3U high-modules (PIU, PSU) includes a single handle at the bottom of the front panel.

The bottom injector/ejector handle of the NPU and AU-IDU modules includes a micro-switch to support hot-swap control.

2.2.8.1 Inserting Modules



To insert an NPU or AU-IDU module:

- 1 Firmly push in the module into its intended slot (slot 5 for the NPU, slot 1-4, 7-9 for AU-IDU).
- 2 Press the handles up (the upper handle)/down (the lower handle) simultaneously until you hear the locking click and the red buttons are released. The blue HOT SWAP LED will briefly turn on, indicating that the module is being powered up.
- 3 Secure the module in place by closing the screws at the top and bottom of the front panel.



NOTE

If a module is fully inserted without properly locking the handles, it will become operational. However, in this state the hot-swap mechanism is not supported. A warning message (trap) will be sent.



To insert a PIU or PSU module:

- 1 Firmly push in the module into its intended slot.
- 2 Press the handle down until you hear the locking click and the red button is released.
- 3 Secure the module in place by closing the screw at the top of the front panel.

2.2.8.2 Ejecting Modules



To eject an NPU or AU-IDU module:

- 1 Release the screws at the top and the bottom of the front panel.
- 2 Press the handles' red button until the handles are unlocked.
- 3 Wait until the blue HOT SWAP LED turns on, indicating that the module has been disconnected and can be removed.

- 4 Press the handles down (the upper handle)/up (the lower handle) until the module is unlocked, firmly hold the handles and take the module out of the chassis.



To eject a PIU or PSU module:

- 1 Release the screw at the top of the front panel.
- 2 Press the handle's red button until the handle is unlocked.
- 3 Press the handle up until the module is unlocked, firmly hold the handle and take the module out of the chassis.



CAUTION

Disconnect power from the PIU module before inserting/ejecting it to/from the chassis. Before disconnecting the power cable from the PIU, the power source must be disconnected to avoid irreversible damage due to potentially excessive high transient current.

2.2.9 Installing the Base Station Chassis and Modules

The indoor equipment should be installed as close as possible to the location where the IF cable(s) enters the building. The location of the indoor equipment should take into account its connection to the power source(s) and to the base station networking equipment.



To install the Base Station chassis and modules:

- 1 Attach the Cable Guide to the top panel of the chassis using the screws and washers supplied with the Cable Guide.
- 2 Install the chassis in a 19" cabinet. For installation in a 21" cabinet, attach suitable ETSI rack adapters to the chassis. To provide a sufficient space for the Cable Guide and to allow air flow for preventing over-heating, leave a free space of at least 1U between the upper covers of the chassis and other units in the cabinet.
- 3 Connect one end of a grounding cable to the ground terminal located on the rear panel of the chassis and firmly tighten the grounding screw. Connect the opposite end of the grounding cable to a ground connection or to the cabinet, if applicable.
- 4 Carefully insert the modules into the relevant slots. Secure the modules in their intended locations (refer to [Inserting Modules](#) on page 55 for instructions on modules' insertion).
- 5 Place blank covers over all of the unused slots.
- 6 Connect the DATA port of the NPU to the backbone data equipment (use a straight Ethernet cable to connect to a hub/switch/router). The maximum length of the Ethernet cable is 100m when operating at 100 Mbps and 70m when operating at 1 Gbps.
- 7 If the MGMT port will be used for remote management, connect it to the appropriate data equipment (use a straight Ethernet cable to connect to a hub/switch/router). The maximum length of the Ethernet cable is 100m.
- 8 Connect the DC power cable to the power jack of the PIU module. If a redundant PIU is installed, connect a DC power cable also to the second PIU module. Connect the power cord(s) to the -48 VDC power source(s), as follows.
 - ◇ Connect the black wire to the 48 VDC contact of the power source.
 - ◇ Connect the red wire to the + (Return) contact.

◇ Connect the ground wire to the ground.

- 9 Connect the IF cable(s) (already connected at the other end to the AU-ODU(s)) to the ODU-1 connector(s) of the applicable AU-IDU module(s). To avoid transmissions at undesired frequencies, verify that the frequency and bandwidth parameters are properly configured before connecting the IF cables.

2.2.10 Air Ventilation Unit (AVU)

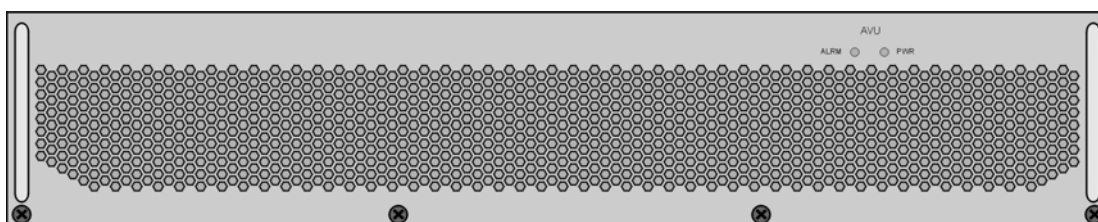


Figure 2-11: AVU Drawer Front Panel

The 2U high, 84 HP wide AVU includes a 1U high integral chamber for inlet airflow and a 1U high fan tray with an internal alarm module. To support a high availability Base Station, the fan tray includes 10 brush-less fans, where 9 fans are sufficient for cooling a fully loaded chassis. To further support high availability, the chassis can operate with the hot-swappable fan tray extracted from it for a period of time sufficient for replacing it (up to 10 minutes).

Table 2-16: AVU LEDs		
LED Status		Description
PWR	ALRM	
Off	Off	No 5V power input
Red	Red	12V power failed
Green	Red	One or more fans have failed
Green	Off	AVU operates properly

If the red ALRM LED is on while the PWR LED is green, it indicates a failure of at least one fan. Although the Base Station chassis may continue operating with one failed fan, it is recommended to replace the AVU as soon as possible.



To replace an AVU drawer:

- 1 Release the 4 screws securing the AVU to the chassis.
- 2 Using the handle take out the faulty chassis.

- 3 Insert a new AVU drawer and close the screws. The replacement should be completed in less than 10 minutes.

2.2.11 Replacing an NPU

To minimize downtime and facilitate fast and easy NPU replacement, it is recommended to maintain an updated copy of the NPU configuration. Refer to [Backup](#) on page 106 for details on preparing and uploading a backup file of the NPU configuration.

- 1 Release the screws at the top and the bottom of the NPU's front panel.
- 2 Press the handles' red button until the handles are unlocked.
- 3 Wait until the blue HOT SWAP LED turns on, indicating that the module has been disconnected and can be removed.
- 4 Press the handles down (the upper handle)/up (the lower handle) until the module is unlocked. Firmly hold the handles and take the module out of the chassis.
- 5 Disconnect all IF cables connecting the AU-IDUs to the AU-ODUs. This is necessary as the initial configuration of the new NPU is most probably inappropriate.
- 6 Firmly push the new NPU module into its intended slot (slot 5).
- 7 Press the handles up (the upper handle)/down (the lower handle) simultaneously until you hear the locking click and the red buttons are released. The blue HOT SWAP LED will briefly turn on, indicating that the module is being powered up.
- 8 Secure the module in place by closing the screws at the top and bottom of the front panel.
- 9 Download the backup file using a DOS based TFTP. Use the command: *tftp-i <NPU port IP address> put <file name>*. The default IP address of the MGMT port is 10.0.0.1.
- 10 Use the monitor program to configure the IP parameters (IP address, Subnet Mask, Default Gateway Address) of the MGMT port. These parameters are not affected by the loaded file.
- 11 Reset the system.
- 12 Reconnect the IF cables.

2.3 Installing the Micro Base Station Equipment

2.3.1 Installation Requirements

2.3.1.1 Packing List

- Micro Base Station Unit
- Mains power cable or a DC power cable
- Monitor cable

2.3.1.2 Additional Installation Requirements

- Ethernet cable (straight) for connecting the unit to a hub/switch.
- A grounding cable with appropriate terminations for connecting the unit's ground terminal to the rack or to a ground connection.
- Mains plug adapter or termination plug (if the power plug on the supplied AC power cord does not fit local power outlets).
- For installation in a 21" ETSI rack: two 21" ETSI rack adapters
- A portable PC for configuring parameters using the Monitor cable.
- Other installation tools and materials

2.3.2 The Micro Base Station Front Panel

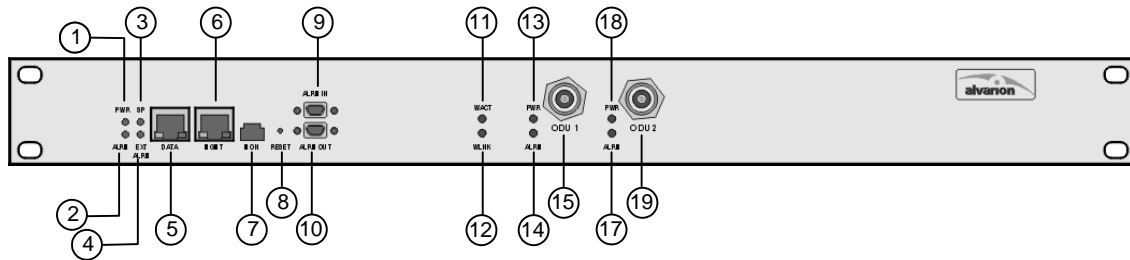


Figure 2-12: Micro Base Station Front Panel

Table 2-17: Micro Base Station Connectors		
Name	Connector	Functionality
DATA (5)	10/100Base-T (RJ-45) with 2 embedded LEDs.	Connection to the backbone. Cable connection to a hub/switch/router: Straight
MGMT (6)	10/100Base-T (RJ-45) with 2 embedded LEDs.	Connection to OOB management. Cable connection to a PC: crossed Cable connection to a hub/switch/router: Straight
MON (7)	3-pin low profile jack	Access for debugging and configuration using the Monitor program.
ALRM IN (9)	9-pin micro D-Type jack	Not used currently. Connections to external alarm indicators (3 alarm inputs, NC or NO)
ALRM OUT (10)	9-pin micro D-Type jack	Not used currently. Connections for activation of external devices (4 dry contact pairs)
ODU 1 (15), ODU 2 (19)	2 x TNC jacks	IF connection to AU-ODU. In the current release only ODU 1 is used.

Table 2-18: Micro Base Station LEDs		
Name	Description	Functionality
PWR (1)	Power indication	<ul style="list-style-type: none"> ■ Off – Micro Base Station is not powered ■ Red – Input power failure ■ Green – Micro Base Station power is OK
ALRM (2)	Micro Base Station alarm indication	<ul style="list-style-type: none"> Off – No Micro Base Station alarm Red – Micro Base Station failure
SP (3)	Spare	Not Used
EXT ALRM (4)	External alarm indication	Red – External alarm (received via the ALRM IN port). Not applicable in the current release.
WACT (11)	IDU transmission indication	<ul style="list-style-type: none"> ■ Off – No IDU transmission ■ Green – IDU transmission OK
WLINK (12)	Wireless link status indication	<ul style="list-style-type: none"> ■ Off – No SU is associated ■ Green – At least one SU is associated
ODU 1 PWR (13), ODU 2 PWR (18)	IDU to ODU Power Indication	<ul style="list-style-type: none"> ■ Off – No IDU to ODU power output ■ Red – IDU to ODU power output failed ■ Green – IDU to ODU power output OK
ODU 1 ALRM (14), ODU 2 ALRM (17)	IDU-ODU communication status	<ul style="list-style-type: none"> ■ Off – IDU-ODU communication OK ■ Red - IDU-ODU communication failure

2.3.2.1 Preparing a Power Cable (DC model)

A 2.5m DC power cable is supplied with each chassis. Additional DC cables can be ordered from Alvarion. If necessary, use the following instruction to prepare a DC cable.



To prepare the power cable:

- 1 Use a cable capable of supporting a current of at least 10A. Use a cable with 2 x 10AWG (or thicker) wires for the power plus an additional 10AWG to 20AWG ground wire.
- 2 The matching power connector to be used is Amphenol D-type power P/N 177TWA/3W3/SP3Y with high power socket contacts P/N 17DM53744-1.
- 3 Connect the cable to the power connector as follows:
 - ◇ Pin 1 (RTN): Red (10 AWG min wire)
 - ◇ Pin 2 (-48V): Black (10 AWG min wire)
 - ◇ Pin 3 (⏏): Ground (shield) (10AWG-20AWG wire)
- 4 Attach suitable terminal rings to the side that connects to the power source.

2.3.3 Installing the Micro Base Station Unit

The indoor equipment should be installed as close as possible to the location where the IF cable(s) enters the building. The location of the indoor equipment should take into account its connection to the power source and to the base station networking equipment.



To install the Micro Base Station:

- 1 Place the unit on a shelf/desk or install it in a 19" cabinet. For installation in a 21" cabinet, attach suitable ETSI rack adapters to the chassis.
- 2 Connect one end of a grounding cable to the grounding screw located on the rear panel of the unit (marked ⚡) and firmly tighten the grounding screw. Connect the opposite end of the grounding cable to a ground (earth) connection or to the cabinet, if applicable.
- 3 Connect the DATA port to the backbone data equipment (use a straight Ethernet cable to connect to a hub/switch/router). The maximum length of the Ethernet cable is 100m.

- 4 If the MGMT port will be used for remote management, connect the it to the appropriate data equipment (use a straight Ethernet cable to connect to a hub/switch/router). The maximum length of the Ethernet cable is 100m.
- 5 For an AC model: Connect the power cord to the unit's AC socket, located on the rear panel. Connect the other end of the power cord to the AC mains. The unit can operate with AC mains of 100-240 VAC, 50-60 Hz.

**NOTE**

The color codes of the power cable are as follows:

Brown	Phase	~
Blue	Neutral	0
Yellow/Green	Ground	≡

- 6 For a DC model: Connect the power cord to the unit's DC socket, located on the rear panel. Connect the other end of the power cord to the -48 VDC power source.
- 7 Connect the IF cable (already connected at the other end to the AU-ODU) to the ODU 1 connector. To avoid transmissions at undesired frequencies, verify that the frequency and bandwidth parameters are properly configured before connecting the IF cables.

2.4 Installing the CPE-IDU-1D Indoor Unit

2.4.1 Installation Requirements

2.4.1.1 Packing List

- BMAX-CPE-IDU-1D
- Wall mounting kit
- Mains power cord

2.4.1.2 Additional Installation Requirements

- Ethernet cable(s): a crossed cable if connecting to a hub/switch and a straight cable if connecting directly to a PC Network Interface Card (NIC).



NOTE

The length of the Ethernet cable connecting CPE-IDU-1D to the user's equipment, together with the length of the IDU-ODU cable, should not exceed 100 meters.

- Mains plug adapter or termination plug (if the power plug on the supplied AC power cord does not fit local power outlets).
- Portable PC with an Ethernet card and a crossed Ethernet cable for configuring parameters using Telnet. TFTP server SW is required for downloading SW versions.
- Other installation tools and materials (a drill for wall-mounting the unit, means for securing cables to walls, etc.)

2.4.2 Introduction

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

2.4.2.1 CPE IDU-1D Connectors and LEDs

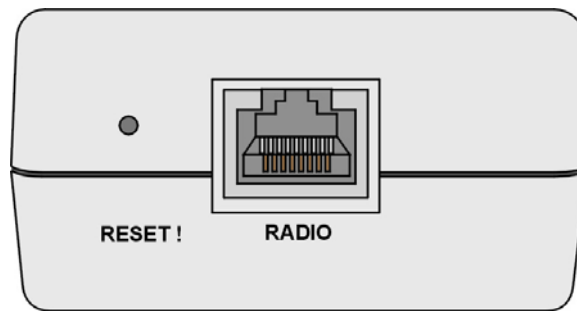


Figure 2-13: CPE-IDU-1D Front Panel

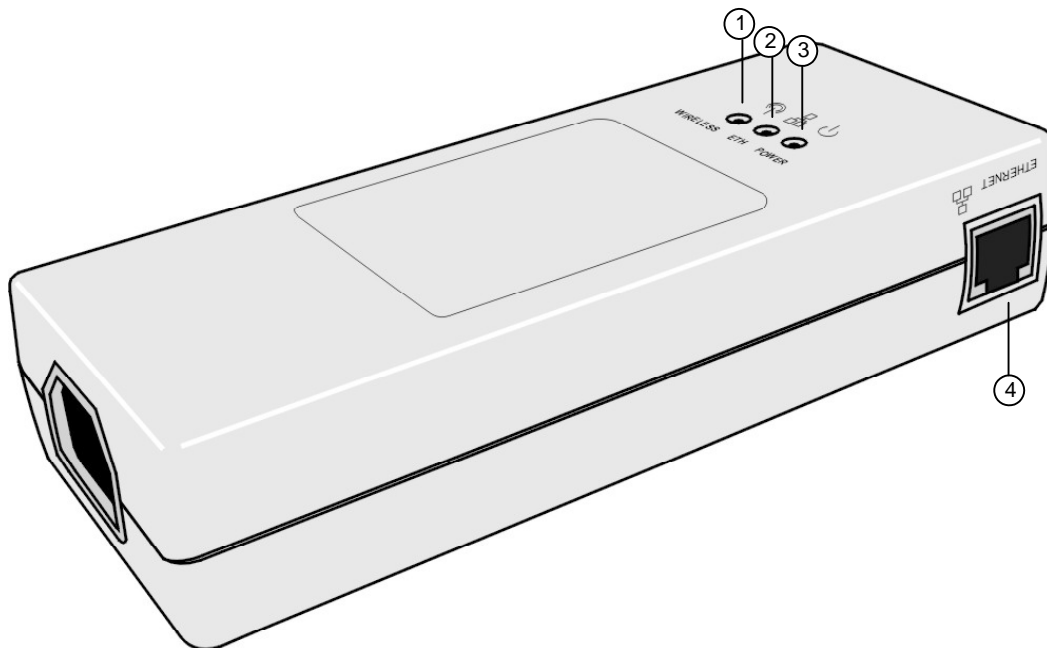


Figure 2-14: CPE-IDU-1D 3D View

Table 2-19: CPE-IDU-1D Connectors		
Name	Connector	Functionality
ETHERNET (4) (on the side panel)	10/100Base-T (RJ-45) with 2 embedded LEDs.	Connection to the user's LAN/PC Cable connection to a hub/switch/router: Crossed Cable connection to a PC: Straight
RADIO (on the front panel)	10/100Base-T (RJ-45)	Connection to the ODU
POWER (on the bottom panel)	3-pin AC	Mains power connection

Table 2-20: CPE-IDU-1D LEDs		
Name	Description	Functionality
POWER (3)	Power Indication	<ul style="list-style-type: none"> ■ Off – IDU is not powered or power failed ■ Green – IDU power is OK
ETH (2)	Ethernet link status (Ethernet integrity)	<ul style="list-style-type: none"> ■ Off – No Ethernet connectivity has been detected between the outdoor unit and the device connected to the indoor unit. ■ Green – Ethernet connectivity has been detected between the outdoor unit and the device connected to the indoor unit.
WIRELESS (1)	Wireless link status	<ul style="list-style-type: none"> ■ Off – SU is not associated with an AU/μBST ■ Green – SU is connected with an AU/μBST

2.4.3 SU-IDU Installation



To install the SU-IDU:

- 1 It is assumed that the IDU-ODU cable is already connected to the ODU (refer to to [Connecting the SU's IDU-ODU Cable](#) on page 42). Assemble an RJ-45 connector with a protective cover on the indoor end of the IDU-ODU cable. Refer to [Appendix A](#) for instructions on preparing the cable.

- 2 Connect the IDU-ODU cable to the RADIO connector. The RADIO connector in the CPE-IDU-1D is located on the front panel as shown in Figure 2-13.

**CAUTION**

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

- 3 Connect the power cord to the unit's AC socket, located on the rear panel. Connect the other end of the power cord to the AC mains after verifying that the unit is rated for the voltage in the country of use; the AC range is indicated on the back side of the CPE-IDU-1D.

**NOTE**

The color codes of the power cable are as follows:

Brown	Phase	~
Blue	Neutral	0
Yellow/Green	Ground	⏏

- 4 Verify that the POWER LED located on the front panel is lit, indicating that the unit is supplying power to the radio port.
- 5 Configure the basic parameters and align the antenna as described in the applicable sections of [Chapter 3 – Commissioning](#).
- 6 Connect the 10/100 Base-T ETHERNET connector(s) to the data equipment. The cable connection should be a crossed Ethernet if connecting to a hub/switch and a straight cable if connecting directly to a PC Network Interface Card (NIC).

**NOTE**

The length of the Ethernet cable connecting CPE-IDU-1D to the user's equipment, together with the length of the IDU-ODU cable, should not exceed 100 meters.

- 7 Verify proper operation as described in the applicable section of [Chapter 3 – Commissioning](#).

Chapter 3 - Commissioning

In This Chapter:

- Base Station and Micro Base Station Commissioning
 - ◇ Configuring Basic Parameters of Base Station and Micro Base Station, page 70
 - ◇ Operation Verification – Base Station and Micro Base Station, page 72
- SU Commissioning
 - ◇ Configuring Basic Parameters in SUs, page 77
 - ◇ Aligning the Subscriber Unit Antenna, page 79
 - ◇ Operation Verification - SU, page 80

3.1 Base Station and Micro Base Station Commissioning

3.1.1 Configuring Basic Parameters of Base Station and Micro Base Station

After completing the installation process, as described in the preceding chapter, some basic parameters must be configured using the Monitor application via the MON port of the NPU/Micro Base Station. These parameters are necessary to enable remote management using SNMP or Telnet.

The basic parameters are listed in Table 3-1. Refer to Chapter 4 – Operation and Administration for detailed information on the applicable parameters.

Table 3-1: Basic NPU/Micro Base Station Parameters	
Management Option	Parameters
MGMT port	<ul style="list-style-type: none"> ■ Management Port IP address ■ Management Port Subnet Mask ■ Management Port Gateway ■ Management Port Destination Subnet ■ Management Port Destination Subnet Mask ■ Management Port Auto Negotiation Option (μBST) ■ Management Port Speed and Duplex (μBST, if Auto Negotiation Option is disabled)
DATA port	<ul style="list-style-type: none"> ■ Data Port IP address ■ Data Port Subnet Mask ■ Data Port Gateway ■ Data Port Management VLAN ID ■ Data Port Speed (NPU) ■ Data Port Auto Negotiation Option (μBST) ■ Data Port Speed and Duplex (μBST, if Auto Negotiation Option is disabled)
Authorized Managers (per manager)	<ul style="list-style-type: none"> ■ IP Address ■ Send Traps ■ Read Community ■ Write Community

The following are the guidelines for configuring the basic parameters:

- All parameters of both ports should be configured. Otherwise, default values shall be used.
- If remote OOB management via a router connected to the MGMT port is used, the parameters should be configured to ensure different subnets for the Data port, the Management port (local OOB management) and the Management Port Destination. The Management Port Destination Subnet is the subnet behind a router connected to the MGMT port.
- Authorized Manager(s) must be configured properly to enable remote management using AlvariSTAR (or another SNMP based application).

Once the basic parameters have been configured, additional parameters and services can be remotely configured using either SNMP management or the Monitor application via Telnet. Alternatively, it is possible to continue the configuration process using the Monitor application via the MON port.

Refer to Chapter 4 – Operation and Administration for information on how to access the Monitor application either via the MON port or via Telnet and how to use it.

NOTE

The default password is “admin”.



3.1.2 Operation Verification – Base Station and Micro Base Station

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

3.1.2.1 AU-ODU LEDs

To verify the correct operation of the AU-ODU, examine the LED indicators located on the bottom panel of the outdoor unit.

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

NOTE



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

Table 3-2: AU-ODU LEDs		
Name	Description	Functionality
PWR	Power indication	<ul style="list-style-type: none"> ■ Off – ODU is not powered ■ Green – ODU power is OK
ALARM	Not Used	(Red – blinks shortly during ODU power up)
ETH (WLNK)	Wireless link status indication	<ul style="list-style-type: none"> ■ Off – No SU is associated ■ Green – At least one SU is associated

3.1.2.2 Base Station LEDs

To verify the correct operation of the Base Station equipment, examine the LED indicators located on the front panels of the modules. The following tables list the LEDs of the Base Station modules and their associated indications.

Table 3-3: AU-IDU LEDs		
Name	Description	Functionality
PWR	Power indication	<ul style="list-style-type: none"> ■ Off – AU-IDU is not powered ■ Red – AU-IDU power supply failed (low power) ■ Green – AU-IDU power is OK
ALARM	Alarm indication	<ul style="list-style-type: none"> ■ Off – AU-IDU is OK ■ Red – AU-IDU failure
WLINK	Wireless link status indication	<ul style="list-style-type: none"> ■ Off – No SU is associated ■ Green – At least one SU is associated
WACT	IDU transmission indication	<ul style="list-style-type: none"> ■ Off – No IDU transmission ■ Green – IDU transmission OK
SP	Spare	Not Used
IP	IP activity indication	<ul style="list-style-type: none"> ■ Off – No downlink (AU to SU) IP activity ■ Green (blinking) – Downlink (AU to SU) IP activity
ODU1/ODU2 PWR	IDU to ODU Power Indication	<ul style="list-style-type: none"> ■ Off – No IDU to ODU power output ■ Red – IDU to ODU power output failed ■ Green – IDU to ODU power output OK
ODU1/ODU2 ALRM		<ul style="list-style-type: none"> ■ Off – IDU-ODU communication OK ■ Red - IDU-ODU communication failure

Table 3-4: NPU LEDs		
Name	Description	Functionality
PWR	Power indication	<ul style="list-style-type: none"> ■ Off – NPU is not powered ■ Red – NPU power failure ■ Green – NPU power is OK
ALRM	NPU Alarm indication	<ul style="list-style-type: none"> Off – NPU is OK Red – NPU failure
BST ALRM	Base Station chassis alarm indication	<ul style="list-style-type: none"> Off – All Base Station modules are OK Red – Failure in one (or more) Base Station modules
EXT ALRM	External alarm indication	<ul style="list-style-type: none"> Off – No alarm received via the AL IN connector Red – Alarm received via the AL IN connector
MASTER	Master/Slave (primary/secondary) operation indication	<ul style="list-style-type: none"> ■ Off – Secondary NPU (backup) ■ Green – Primary NPU
GPS/SYNC	GPS/IF clock synchronization functionality indication	<ul style="list-style-type: none"> ■ Off – GPS/IF clock synchronization is disabled ■ Green – GPS/IF clock synchronization is enabled

Table 3-5: PIU LEDs		
LED Status		Description
PWR	MASTER	
Off	Off	Chassis is not connected to power.
Red	Off	Power is not connected or power input is out of range or PIU card is damaged. Chassis is powered by the redundant PIU.
Red	Green	Power input is out of range or PIU card damaged. Chassis is powered by the PIU
Green	Off	Power to PIU is OK. PIU is in redundant mode and the chassis is powered from the other PIU.
Green	Green	Power to PIU is OK. The chassis is powered from the PIU.

Table 3-6: PSU LEDs		
LED Status		Description
PWR	ALRM	
Off	Off	No power or fatal damage
Off	Red	Power input is out of range or PSU is damaged or PSU is inhibited by NPU.
Green	Off	Power is OK and PSU operates properly.

Table 3-7: AVU LEDs		
LED Status		Description
PWR	ALRM	
Off	Off	No 5V power input
Red	Red	12V power failed
Green	Red	One or more fans have failed
Green	Off	AVU operates properly

3.1.2.3 Micro Base Station LEDs

To verify the correct operation of the Micro Base Station equipment, examine the LED indicators located on the front panel of the unit. The following table lists the LEDs of the Micro Base Station and their associated indications.

Table 3-8: Micro Base Station LEDs		
Name	Description	Functionality
PWR	Power indication	<ul style="list-style-type: none"> ■ Off – Micro Base Station is not powered ■ Red – Input power failure ■ Green – Micro Base Station power is OK
ALRM	Micro Base Station alarm indication	<ul style="list-style-type: none"> Off – Micro Base Station is OK Red – Micro Base Station failure
SP	Spare	Not Used
EXT ALRM	External alarm indication	Red – External alarm (received via the ALRM IN port). Not applicable in the current release.
WACT	IDU transmission indication	<ul style="list-style-type: none"> ■ Off – No IDU transmission ■ Green – IDU transmission OK
WLINK	Wireless link status indication	<ul style="list-style-type: none"> ■ Off – No SU is associated ■ Green – At least one SU is associated
ODU1/ODU2 PWR	IDU to ODU Power Indication	<ul style="list-style-type: none"> ■ Off – No IDU to ODU power output ■ Red – IDU to ODU power output failed ■ Green – IDU to ODU power output OK
ODU1/ODU2 ALRM	IDU-ODU communication status	<ul style="list-style-type: none"> ■ Off – IDU-ODU communication OK ■ Red - IDU-ODU communication failure

3.1.2.4 Verifying the Ethernet Connection

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

3.2 SU Commissioning

3.2.1 Configuring Basic Parameters in SUs

After completing the installation process, as described in the preceding chapter, the basic parameters must be configured to ensure that the unit operates correctly and can communicate with the AU. Once the basic parameters have been configured, additional parameters can be remotely configured via the wireless link.



To configure the SU's basic parameters:

- 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 IP address of the Monitor program port is 192.168.254.251. The Subnet Mask is 255.255.255.0. The recommended IP address for the PC is 192.168.254.250, as this is also the default TFTP Sever IP Address (required for downloading SW versions and for downloading/uploading configuration files)
- 3 Run the Telnet program connecting to 192.168.254.251. The *Enter the password* prompt is displayed. Enter the password and press the Enter key.

NOTE

The default password is "installer".



- 4 The Main menu of the SU Installer Monitor program is displayed, enabling you to access the required parameters configuration and performance monitoring options. Refer to [Appendix B](#) for instructions on using the SU Installer Monitor program and detailed information on the various parameters and other features supported by the program.
- 5 Configure the basic parameters listed in Table 3-9 on page 78.
- 6 Reset the unit (use the Reset option in the Unit Control menu) to apply the new settings and enable synchronization with the AU.

Table 3-9: SU's Basic Parameters		
Parameter	Default Value	Comment
Ethernet Port Operation Mode	Auto Negotiation	
Common Name		Must be supplied by administration to ensure uniqueness in the entire network
Organization Name		Optional – according to administrator policy.
Address		Optional– according to administrator policy.
Country Code		Optional– according to administrator policy.
Operator ID	186.190.0	
Cell ID	0.0	
Sector ID	0	
Base Sector ID Mask	255.255.255.0	
Bandwidth	3.5 MHz	
Uplink (Tx) Frequency	3451.75 MHz	

NOTE

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

3.2.2 Aligning the Subscriber Unit Antenna

The LINK QUALITY bar display is located on the bottom panel of the outdoor unit. LED 1 (WLNK) indicates that the wireless link is active, and is lit when the SU has completed the Network Entry process. LEDs 2 to 9 indicate the quality of the received signal. The higher the number of LEDs that are on, the better the quality of the received signal.

The link quality can be estimated more accurately using the Link Quality Display option in the SU Installer Monitor program. Refer to [Start Link Quality Display](#) on page 217 for more details on this option.

This section describes how to align the Subscriber Unit antenna using the LINK QUALITY bar display or the Start Link Quality Display option of the Monitor program.



To align the Subscriber Unit antenna:

- 1 Point the antenna towards the general direction of the Base Station.
- 2 Verify that the power indication of the unit is on.
- 3 Verify that at least one LED (LED 2) of the LINK QUALITY bar display is on, indicating that the unit is synchronized with the AU. If the SU is not synchronized with the AU, ensure that all parameters are configured properly. If the unit is still not synchronized with the AU, improve the quality of the link by changing the direction of the antenna or by placing the antenna at a higher or alternate location.
- 4 Rotate the antenna until the maximum Link Quality reading is achieved. If you encounter prolonged difficulty in achieving the expected link quality, try to improve the reception quality by placing the antenna at a higher point or in an alternate location.



NOTE

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

- 5 Secure the unit firmly to the pole.



CAUTION

In some cases, the antenna may need to be tilted to ensure that the level at which the SU receives transmissions from the AU (and vice versa) is not too high. When all LINK QUALITY LEDs are on, including LED 10. This indicates that the received signal level is too high (saturation). This must be avoided, preferably by up-tilting the antenna. As a rule of thumb, if the SU is located at a distance of less than 300 meters from the AU, it is recommended to up-tilt the antenna by approximately 10° to 15°.

3.2.3 Operation Verification - SU

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

3.2.3.1 CPE-IDU-1D LEDS

Table 3-10: CPE-IDU-1D LEDS		
Name	Description	Functionality
POWER	Power Indication	<ul style="list-style-type: none">■ Off – IDU is not powered or power failed■ Green – IDU power is OK
ETH	Ethernet link status (Ethernet integrity)	<ul style="list-style-type: none">■ Off – No Ethernet connectivity has been detected between the outdoor unit and the device connected to the indoor unit.■ Green – Ethernet connectivity has been detected between the outdoor unit and the device connected to the indoor unit.
WIRELESS	Wireless link status	<ul style="list-style-type: none">■ Off – SU is not associated with an AU/μBST■ Green – SU is connected with an AU/μBST

3.2.3.2 SU – ODU LEDs

To verify the correct operation of the SU – ODU, examine the LED indicators located on the bottom panel of the outdoor unit.

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

NOTE



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

Table 3-11: SU-ODU LEDs		
Name	Description	Functionality
PWR	Power indication	<ul style="list-style-type: none"> ■ Off – ODU is not powered ■ Green – ODU power is OK
ALARM	Alarm indication	<ul style="list-style-type: none"> ■ Off – ODU is OK, diagnostic test passed ■ Red – ODU failure
ETH	Ethernet link status indication (Ethernet integrity)	<ul style="list-style-type: none"> ■ Off – No Ethernet connectivity has been detected between the outdoor unit and the device connected to the indoor unit. ■ Green– Ethernet connectivity has been detected between the outdoor unit and the device connected to the indoor unit
LINK QUALITY bar display	Wireless link status and signal quality Indication	See Table 3-12.

Table 3-12: SU-ODU LINK QUALITY Bar LEDs Functionality	
Bar LEDs	SNR
LED 1 (orange) is On	The SU is connected with and receives services from AU/ μ BST (Network Entry completed)
LED 2 (green) is On	$5\text{dB} \leq \text{SNR} < 10\text{dB}$
LEDs 2-3 (green) are On	$10\text{dB} \leq \text{SNR} < 15\text{dB}$
LEDs 2-4 (green) are On	$15\text{dB} \leq \text{SNR} < 20\text{dB}$
LEDs 2-5 (green) are On	$20\text{dB} \leq \text{SNR} < 24\text{dB}$
LEDs 2-6 (green) are On	$\text{SNR} \geq 24$ and $\text{RSSI} < -75$
LEDs 2-7 (green) are On	$\text{SNR} \geq 24$ and $\text{RSSI} \geq -75$
LEDs 2-8 (green) are On	$\text{SNR} \geq 24$ and $\text{RSSI} \geq -70$
LEDs 2-9 (green) are On	$\text{SNR} \geq 24$ and $\text{RSSI} \geq -60$
LEDs 2-9 (green) and 10 (red) are On	$\text{RSSI} \geq -20$ (saturation)

3.2.3.3 Verifying Data Connectivity

To verify data connectivity, from the end-user's PC or from a portable PC connected to the unit, ping a known device in the network, or try to connect to the Internet. For units with multiple LAN ports, verify proper operation for each of the ports.

Chapter 4 - Operation and Administration

In This Chapter:

- [BreezeMAX System Management](#), page 84
- [The Monitor Program](#), page 85
- [The Micro Base Station's Main Menu](#), page 88
- [Micro Base Station Menu](#), page 89
- [The NPU's Main Menu](#), page 95
- [Base Station Menu](#), page 97
- [NPU Menu](#), page 102
- [AU Menu](#), page 115
- [SU Menu](#), page 132
- [Services Menu](#), page 150
- [NPU/Micro Base Station Parameters Summary](#), page 177

4.1 BreezeMAX System Management

All BreezeMAX system components associated with a modular Base Station are managed via the Base Station's NPU module. The other system components (AUs and SUs) are not accessed directly: each configuration change or status enquiry is sent to the NPU that communicates with other system components. This is true also for a Micro Base station, where all the associated SUs are managed indirectly via the Micro Base Station (μ BST).



NOTE

The SU can also be managed directly from its Ethernet port using the Installer Monitor program. This option is available to support the installation process and enable special tests and performance monitoring at the SU's site.

The following management options are available:

- SNMP based management using AlvariSTAR (or another network management system customized to support management of BreezeMAX)
- Using Telnet to access the embedded Monitor application.
- Accessing the embedded Monitor application locally via the MON port.

Two management access methods are available to support management using SNMP and/or Telnet:

- Out-Of-Band (OOB) management via the dedicated MGMT port.
- In-Band (IB) management via the DATA port.

Typically, BreezeMAX systems will be managed using AlvariSTAR or another SNMP based network management system.

This chapter describes how to manage the system using the Monitor application. For information on managing the system using AlvariSTAR refer to the Applicable AlvariSTAR documentation.



NOTE

To enable remote management (using SNMP and/or Telnet), the parameters of the applicable port (MGMT and/or DATA) must first be configured via the MON port. For details on the applicable parameters refer to [Configuration \(NPU\)](#) on page 107.

4.2 The Monitor Program

4.2.1 Accessing the Monitor Program



To access the Monitor program via the MON connector:

- 1 Use the Monitor cable to connect the MON connector of the NPU/Micro Base Station 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: COM Port Configuration	
Parameter	Value
Baud Rate	9600
Data Bits	8
Stop Bits	1
Parity	None
Flow Control	Xon/Xoff
Port	Connected COM port

- 4 The password prompt is displayed. Enter the password and press the Enter key to get to the Main menu.

NOTE

The default password is "admin".



To access the Monitor program using Telnet:

- 1 The PC used for accessing the Monitor program should be configured according to the parameters configured for the applicable port (MGMT or DATA port).
- 2 If you connect directly to the MGMT or DATA port, use a crossed Ethernet cable.
- 3 Run the Telnet program connecting to the IP address of the connected port.

- 4 The *Enter the password* message is displayed. Enter the password and press the Enter key to get to the Main menu.

**NOTE**

If you forgot the password, type “help” to receive a challenge string consisting of 24 characters. Contact Alvarion’s Customer Service and provide the challenge string (after user identification) to receive a temporary password. You can use this password only once to enter the program. The password must be changed during the session to a different “permanent” password. The administrator should be notified of this new password. Five consecutive errors in entering the temporary password will invalidate it. In this case, repeat this procedure to receive a new challenge string for a new temporary password.

4.2.2 Using the Monitor Program

This section describes the Monitor program structure and navigation rules.

- Each menu or submenu specifies the unit type (BreezeMAX NPU or μ BST), the running SW version and a description of the menu. When accessing the Monitor program using Telnet, the IP address of the applicable port is displayed after the unit type.
- Each menu or submenu displays a list of numbered options. To access an option, enter the number of the required option at the > prompt and press the Enter key.
- At any point in the program, you can use the Esc key to return to the previous menu (one level up) without applying any change.
- The first selectable item in most menus is the Show option, enabling to view the current configuration of the applicable parameters. For some menus some additional status information is displayed.

For certain parameters, an updated value is applied only after reset or after entering a specific command. In these parameters, the configured value may differ from the actual value. If the configured value differs from the actual value both values will be displayed, where the first one is the configured value and the second is the actual value. For example: “Bandwidth (MHz): 1.75, 3.5” means that the configured bandwidth, to be applied after the next reset, is 1.75 MHz, and the current actual bandwidth is 3.5 MHz.

For certain parameters the actual values may not be available (such as when pre-configuring an AU that is not yet installed). For these parameters a value of NA (Not Available) will be displayed.

- The Update/Add options will display all applicable parameters line by line, allowing to conveniently edit all of them. The current value is displayed for each parameter. To keep the current value - press Enter. To change it - enter a new value and press Enter.

- Press the Tab key for context sensitive help text (where applicable).
- If an erroneous value was entered - the reason of the error or help text will be displayed, and the parameter entry text will be displayed again.
- Many menus include a Select By option, enabling to get a sub-menu for a selected entity according to the selection criteria.
- If the Monitor program is not used for 10 minutes, the session will be automatically terminated.
- Select the Exit option in the Main menu to exit the program and terminate the session.

4.3 The Micro Base Station's Main Menu

The Main menu of the Micro Base Station (uBST) Monitor program includes the following options:

```
BreezeMAX uBST
SW Version 1.0.2
Main Menu
=====
1 - Micro Base Station
2 - SU
3 - Services
X - Exit
>
```

Figure 4-1: Micro Base Station Monitor's Main Menu

Following is a description of the menu items and the options available in each of the menu items. Most of the features, parameters and options available in the Micro Base Station menus are identical or very similar to those of the NPU, described in detail in the following sections. In order to avoid duplication of information, references are made to the relevant sections of the NPU Monitor description.

4.3.1 Micro Base Station Menu

The Micro Base Station menu enables viewing general unit's details, viewing and configuring unit's parameters, managing the SW versions and viewing ports traffic counters. For more details refer to [Micro Base Station Menu](#) on page 89.

4.3.2 SU Menu

The SU menu enables viewing summary information of all relevant SUs and configuring the parameters of a selected SU. It also enables managing the selected SU's SW versions and viewing its current status, configuration and performance information. For more details refer to [SU Menu](#) on page 132.

4.3.3 Services Menu

The Service menu enables viewing, updating and adding service profiles and subscribers, and allocating service profiles to subscribers. For more details refer to [Services Menu](#) on page 150.

4.3.4 Exit

Select the Exit option to exit the Monitor program and terminate the Telnet session.

4.4 Micro Base Station Menu

The Micro Base Station menu includes the following options:

- Show
- Unit Control
- Configuration
- Alarms and Traps
- Performance Monitoring

4.4.1 Show

Select this option to view general unit's details as well as the current value/selected option of configurable parameters.

- Unit Details
 - ◇ Serial Number
 - ◇ IDU Serial Number
 - ◇ IDU Main Card HW Revision
 - ◇ IDU Main Card HW Configuration
 - ◇ IDU IF Card HW Revision
 - ◇ IDU IF Card HW Configuration
 - ◇ IDU Boot Version
 - ◇ IDU Temperature (Celsius)
 - ◇ ODU Serial Number
 - ◇ ODU HW Revision
 - ◇ ODU HW Configuration

- ◇ ODU HC08 Version
- ◇ ODU CPLD Version
- ◇ ODU Temperature (Celsius)
- ◇ Status

■ SW Versions

- ◇ Main SW File
- ◇ Main SW Version
- ◇ Shadow SW File
- ◇ Shadow SW Version
- ◇ Running From (Main or Shadow)
- ◇ Boot SW Version

For more details refer to [SW Version Control \(NPU\)](#) on page 105.

■ General Parameters

- ◇ Device Name
- ◇ Device Location

For details refer to [Configuration \(Base Station\)](#) on page 98.

■ Management Port Configuration

- ◇ Management Port MAC Address
- ◇ Management Port IP Address
- ◇ Management Port Subnet Mask
- ◇ Management Port Gateway
- ◇ Management Port Dest Subnet
- ◇ Management Port Dest Subnet Mask

- ◇ Management Port Auto Negotiation
- ◇ Management Port Speed and Duplex
- ◇ Management Port Link Status (Up or Down)

For details refer to [Management Port Parameters](#) on page 108.

■ Data Port Configuration

- ◇ Data Port MAC Address
- ◇ Data Port IP Address
- ◇ Data Port Subnet Mask
- ◇ Data Port Gateway
- ◇ Data Port Management VLAN
- ◇ Data Port Auto Negotiation
- ◇ Data Port Speed and Duplex
- ◇ Data Port Link Status (Up or Down)

For details refer to [Data Port Parameters](#) on page 110.

■ Authorized Managers (per manager)

- ◇ IP Address
- ◇ Send Traps
- ◇ Read Community
- ◇ Write Community

For details refer to [Authorized Managers](#) on page 111.

■ Bridge

- ◇ Bridge Aging Time

For details refer to [Bridge](#) on page 112.

■ MAC Parameters

- ◇ Base Station ID
- ◇ ARQ Enable/Disable
- ◇ Maximum Cell Radius (km)

For details refer to [MAC Parameters \(AU\)](#) on page 121.

■ Phy Parameters

- ◇ Frequency Band
- ◇ Bandwidth (MHz)
- ◇ Downlink (Tx) Frequency (MHz)
- ◇ Tx Power (dBm)

For details refer to [Phy Parameters \(AU\)](#) on page 122.

■ Multirate Parameters

- ◇ Multirate Enable/Disable
- ◇ Uplink Basic Rate
- ◇ Downlink Basic Rate

For details refer to [Multirate Parameters \(AU\)](#) on page 124.

■ ATPC Parameters

- ◇ ATPC Enable/Disable
- ◇ Optimal Uplink RSSI (dBm)

For details refer to [ATPC Parameters \(AU\)](#) on page 126.

■ Voice Parameters:

- ◇ Maximum Number of Voice Calls

For details refer to [Voice Parameters \(AU\)](#) on page 127.

4.4.2 Unit Control

The Unit Control menu enables changing the access password and the Monitor Inactivity Timeout, resetting the unit, setting factory defaults, managing the SW versions of the unit and creating a backup file.

The Unit Control menu includes the following options:

- Change Password
- Reset
- Set Factory Defaults
- SW Versions Control
- Backup
- Monitor Inactivity Timeout

The features and options available in the Unit Control menu of the Micro Base Station are identical to those available in the Unit Control menu of the NPU. For more details refer to [Unit Control \(NPU\)](#) on page 104.

4.4.3 Configuration

The Configuration menu of the Micro Base Station enables to configure various parameters. The parameters available in the Configuration menu of the Micro Base Station are very similar to those available in the Configuration>Update options of the Base Station, NPU and AU menus of the NPU Monitor.

The Configuration menu of the Micro Base Station includes the following options:

- General Parameters (for details refer to [Configuration \(Base Station\)](#) on page 98).
- Management Port (for details refer to [Management Port Parameters](#) on page 108).
- Data Port (for details refer to [Data Port Parameters](#) on page 110).
- Authorized Managers (for details refer to [Authorized Managers](#) on page 111).
- Bridge (for details refer to [Bridge](#) on page 112)
- MAC (for details refer to [MAC Parameters \(AU\)](#) on page 121).

- Phy (for details refer to [Phy Parameters \(AU\)](#) on page 122).
- Multirate (for details refer to [Multirate Parameters \(AU\)](#) on page 124).
- ATPC (for details refer to [ATPC Parameters \(AU\)](#) on page 126).
- Voice Parameters (for details refer to [Voice Parameters \(AU\)](#) on page 127).

4.4.4 Alarms and Traps

The Alarms and Traps menu enables viewing the active alarms or the traps log, filtering the displayed traps and enabling/disabling traps. For details refer to [Alarms and Traps \(Base Station\)](#) on page 98.

4.4.5 Performance Monitoring

The Performance Monitoring menu enables to view and reset the μ BST Ethernet Ports and Wireless Port counters. It also enables to initiate and manage a BER test on the link with a specific SU, and to view or reset the Burst Error Rate counters for the downlink to a selected SU. The Performance Monitoring submenu includes the following options:

- Ports Counters:
 - ◇ Management Port: The functionality is the same as the Management Port counters in the NPU. For details refer to Management Port Counters (NPU) on page 114.
 - ◇ Data and Wireless Ports: The functionality is the same as for the Ethernet and Wireless Ports counters in the AU. For details refer to Ports Counters (AU) on page 127.
- BER Test: The functionality is the same as for the BER Test option in the AU. For details refer to [BER Test \(AU\)](#) on page 130.
- Burst Error Rate Counters: The functionality is the same as for the Burst Error Rate Counters option in the AU. For details refer to [Burst Error Rate Counters \(AU\)](#) on page 131.

4.5 The NPU's Main Menu

The Main menu of the NPU Monitor program includes the following options:

```
BreezeMAX NPU [192.168.254.10]
SW Version 1.5.1
Main Menu
=====
1 - Base Station
2 - NPU
3 - AU
4 - SU
5 - Services
X - Exit
>
```

Figure 4-2: NPU Monitor's Main Menu

4.5.1 Base Station Menu

The Base Station menu enables to view general base station status information, to configure general base station parameters, and to view active alarms or traps log. For details refer to [Base Station Menu](#) on page 97.

4.5.2 NPU Menu

The NPU menu enables configuring the NPU's DATA and MGMT ports, defining authorized managers, managing the NPU's SW versions and viewing current status and configurations. For details refer to [NPU Menu](#) on page 102.

4.5.3 AU Menu

The AU menu enables configuring the MAC and Phy parameters of selected AUs, including pre-configuration of AUs that are not yet installed. It also enables managing AUs SW versions and viewing current status, configurations and performance information. For details refer to [AU Menu](#) on page 115.

4.5.4 SU Menu

The SU menu enables viewing summary information of all relevant SUs and configuring the parameters of a selected SU. It also enables managing the selected SU's SW versions and viewing its current status, configuration and performance information. For details refer to [SU Menu](#) on page 132.

4.5.5 Services Menu

The Service menu enables viewing, updating and adding service profiles and subscribers, and allocating service profiles to subscribers. For details refer to [Services Menu](#) on page 150.

4.5.6 Exit

Select the Exit option to exit the Monitor program and terminate the Telnet session.

4.6 Base Station Menu

The Base Station menu includes the following options:

- Show
- Configuration
- Alarms and Traps

4.6.1 Show

Select this option to view the current value/selected option of configurable parameters. Refer to [Configuration \(Base Station\)](#) on page 98 for more details on these parameters. In addition, some general status information is displayed, as follows:

- Device Name
- Device Location
- Slots status, displaying for each slot (1-9) the following:
 - ◇ Installed module type (or “Not Installed” for an empty slot)
 - ◇ Fault status for an installed module
- Fault status of the AVU module
- PIU slots status, displaying for each PIU slot:
 - ◇ Mode: Master, Redundant or Not Installed
 - ◇ Fault Status
- PSU slots table, displaying the status of each slot: Not installed, OK or Fault.

P I U # 1	P S U # 1	S L O T # 1	S L O T # 2	S L O T # 3	S L O T # 4	S L O T # 5	S L O T # 6	S L O T # 7	S L O T # 8	S L O T # 9	P S U # 3
P I U # 2	P S U # 2										P S U # 4

Figure 4-3: Base Station Chassis Slot Assignments

4.6.2 Configuration

Select this option to view or configure the general Base Station parameters:

4.6.2.1 Device Name

The Device Name parameter provides identification information for the base station equipment.

The device name consists of up to 256 printable characters.

The default Device Name is a null string (empty).

4.6.2.2 Device Location

The Device Location parameter provides location information for the Base Station equipment.

The location name consists of up to 256 printable characters.

The default Device Location is a null string (empty).

4.6.3 Alarms and Traps

The Alarms and Traps menu enables viewing the active alarms or the traps log, filtering the displayed traps and enabling/disabling traps. The available options are:

- Show Active Alarms
- Traps Display Filter
- Show Traps Log
- Trap Configuration

4.6.3.1 Show Active Alarms

Select to view the currently active alarms. For more details on active alarms refer to [Appendix D - Traps and Alarms](#).

4.6.3.2 Traps Display Filter

Select to view/update the filtering criteria for the Traps Log display. The configurable filtering criteria are:

4.6.3.2.1 Minimum Severity

The Minimum Severity parameter enables defining the minimum severity filter. Traps whose severity is below the defined severity will not be displayed.

The options are Critical, Major, Minor, Warning and Info.

The default is Info severity, which means that all the traps in the log will be displayed.

4.6.3.2.2 Days

The Days parameter enables defining the period for which traps will be displayed.

The available options are from 1 to 31 days. Only traps that occurred within the last N days, where N is the value selected for this parameter, will be displayed.

The default is 31 days.

4.6.3.3 Show Traps Log

Select to view the traps log. The traps will be displayed based on the filtering criteria defined by the Minimum Severity and Days parameters in the Traps Display Filtering option, up to a maximum of the last 1000 traps. For more details refer to [Appendix D - Traps and Alarms](#).

4.6.3.4 Trap Configuration

To support simple configuration of traps admin status (enable/disable), the traps are grouped into two groups: Group A Traps and Group B Traps. The Trap Configuration submenu enables viewing the admin status of each trap as well as enabling/disabling the traps in each of the two groups. The available options are:

4.6.3.4.1 Show Traps Admin Status

Select this option to display the Traps Admin Status List. The list includes for each trap the trap ID (Sequential Number), trap name and admin status (Enabled/Disabled).

4.6.3.4.2 Trap Group Enable/Disable

This option allows selecting between Group A and Group B, followed by the option to Enable or Disable the traps in the selected group.

The default for both groups is Enable.

Table 4-2: Group A Traps	
Trap ID	Trap Name
1	ResetOn
2	DiagnosticsHwFaultOn
3	DiagnosticsHwFaultOff
6	AuNetworkEntryStatus
21	ShelfCardExtractionOn
22	ShelfCardInsertionOn
23	ShelfPeripheralEquipmentFaultOn
24	ShelfPeripheralEquipmentFaultOff
25	ShelfEnvParamFaultOn
26	ShelfEnvParamFaultOff
42	ParameterSetFailure
61	OduCrcErrorOn
62	OduCrcErrorOff
63	OduCommErrorOn
64	OduCommErrorOff
114	ServiceGeneralError
128	ColdStart
129	WarmStart
130	LinkDown
131	LinkUp
132	AuthenticationFailure

Table 4-3: Group B Traps	
Trap ID	Trap Name
4	MonitorAccessOn
5	MonitorAccessOff
41	ConfigurationChanged
81	SuMaxTxPowerReached
82	SuMinTxPowerReached
83	SuNetworkEntryStatus
101	SwDownloadStart
102	SwDownloadEnd
103	SwDownloadError
104	SwSwitchFailed
105	SwSwitchSucceed
106	BERTestFinished
107	BERTestStarted
111	IServiceDown
112	ServiceUp
113	ServiceChanged

4.7 NPU Menu

The NPU menu includes the following options:

- Show
- Unit Control
- Configuration
- Performance Monitoring

Following is a detailed description of these options.

4.7.1 Show

Select this option to view the current value/selected option of configurable parameters. Refer to [Configuration \(NPU\)](#) on page 107 for more details on these parameters. In addition, some general status information is shown, as follows:

- General Parameters:
 - ◇ Serial Number
 - ◇ HW Version
 - ◇ HW Configuration
 - ◇ Temperature (Celsius)
- Management Port Parameters:
 - ◇ Management Port MAC Address
 - ◇ Management Port IP Address
 - ◇ Management Port Subnet Mask
 - ◇ Management Port Gateway
 - ◇ Management Port Dest Subnet
 - ◇ Management Port Dest Subnet Mask

- ◇ Management Port Status
- ◇ Management Port Management Traffic (Enabled/Disabled)
- Data Port Parameters:
 - ◇ Data Port MAC Address
 - ◇ Data Port IP Address
 - ◇ Data Port Subnet Mask
 - ◇ Data Port Gateway
 - ◇ Data Port Management VLAN
 - ◇ Data Port Speed
 - ◇ Data Port Status
 - ◇ Data Port Management Traffic (Enabled/Disabled)
- Authorized Managers (per manager):
 - ◇ IP Address
 - ◇ Access Rights
 - ◇ Send Traps
 - ◇ Read Community
 - ◇ Write Community
- Bridge Parameters:
 - ◇ Bridge Aging Time
- SW Files and Versions:
 - ◇ Main SW File
 - ◇ Main SW Version
 - ◇ Shadow SW File

- ◇ Shadow SW Version
- ◇ Running From: The currently running version (Main or Shadow)
- ◇ Boot SW Version

4.7.2 Unit Control

The Unit Control menu of the NPU/ μ BST enables changing the access password and the Monitor Inactivity Timeout, resetting the NPU/ μ BST, setting factory defaults, managing the SW versions of the module and creating backup files.

The Unit Control menu includes the following options:

- Change Password
- Reset
- Set Factory Defaults
- SW Versions Control
- Create Backup
- Monitor Inactivity Timeout

4.7.2.1 Change Password

Select this option to change the password. You will be prompted to enter the new password. After pressing enter, you will be prompted to re-enter the new password.



NOTE

Notify the system administrator of the new password!

Valid passwords: Up to 16 printable characters, case sensitive.

The default password is admin.

4.7.2.2 Reset Unit

Select this option to reset the NPU/ μ BST. To avoid unintentional reset, you will be prompted to confirm the reset request. Changes to some of the configurable parameters are applied only after reset. Refer to [NPU/Micro Base Station Parameters Summary](#) on page 177 for information on which parameters are changeable in run time and which changes are applied only after reset.

4.7.2.3 Set Factory Defaults

Select this option to set the Base Station and NPU (or the Micro Base Station) parameters to their factory default values. Refer to [NPU/Micro Base Station Parameters Summary](#) on page 177 for information on the factory default values of these parameters. The parameters will revert to their default values after the next reset.



NOTE

Setting the parameters of the NPU/ μ BST to their default values will disable remote management of the Base Station.

4.7.2.4 SW Version Control

The NPU/ μ BST can contain two SW versions:

- **Main:** Each time the NPU/ μ BST resets it will reboot using the version defined as Main.
- **Shadow:** Normally the Shadow version is the backup version. Each time a new SW File is downloaded to the NPU/ μ BST, it will be stored as a Shadow version, replacing the previous Shadow Version.

The typical process of upgrading to a new SW version includes the following steps:

- 1 Download the new SW File to the NPU/ μ BST. It will be stored as the Shadow version.
- 2 Reset and run the module from its Shadow version. Note that at this stage, after reset the unit will reboot from its previous Main version.
- 3 If you want to continue using the new version, swap the Shadow and Main versions. The new version is now defined as Main, and will be used each time the module reboots. The previous version is defined now as Shadow.

Each SW version includes two identifiers:

- SW File, which is the name of the downloaded SW file. This name does not necessarily include clear identification of the SW version number.
- SW Version, which provides unambiguous identification of the SW version.

The SW Version Control submenu includes the following options:

- Show versions
- Run from Shadow

- Set as Main

4.7.2.4.1 Show Versions

Select this option to view the current available versions and the running version:

- Main SW File
- Main SW Version
- Shadow SW File
- Shadow SW Version
- Running From: Main or Shadow
- Boot SW Version

4.7.2.4.2 Run from Shadow

Select the Run from Shadow option to reset the NPU/ μ BST and run the Shadow version after power up. To avoid unintentional actions you will be prompted to confirm the request.

4.7.2.4.3 Set as Main

When the NPU/ μ BST is running the Shadow version (after selecting Reset and Run from Shadow), it will boot from the Main version after the next reset. Select the Set as Main option if you want to swap versions so that the running version will become the Main version and will be the version to be used after reset. To avoid unintentional actions you will be prompted to confirm the request.

4.7.2.5 Create Backup

The Create Backup option enables creating backup files of the Base Station/Micro Base station configuration. The backup file contains copies of all the applicable configuration files and databases in the system.

The following backup file types can be created:

- **Full:** The entire Base Station/Micro Base Station configuration (except to the basic IP parameters of the MGMT and DATA ports - IP Address, Subnet Mask and Default Gateway).
- **Profiles:** All the profiles associated with services (Service Profiles, Forwarding Rules, Priority Classifiers, QoS Profiles).

- **Profiles and Services:** All the profiles and configurations associated with service (General Service parameters, Subscribers, Services, Service Profiles, Forwarding Rules, Priority Classifiers, QoS Profiles)

Upon selecting the backup type option, you will be requested to confirm the request. After confirmation, a message is displayed indicating that the backup file creation is in process. Upon successful completion of the process, a completion message will be displayed.

If a backup file of the same type already exists in the NPU/ μ BST, you will be asked whether to overwrite the existing file. If there was an error in the process of creating a backup file, an error message will be displayed, specifying the reason.



To upload/download the Backup File:

After the backup file has been created, it can be uploaded using a DOS based TFTP Client application to a target directory. To upload the file, use the command:

```
tftp-i <Port IP address> get <file name> <destination address>.
```

The default file name is:

- Full: backup.res.
- Profiles: profiles.res
- Profiles and Services: profiles_srvcs.res

The file is encrypted and cannot be edited. However, it can be downloaded to other NPU(s)/ μ BSTs using a DOS based TFTP Client application with the command: *tftp-i <Port IP address> put <file name>.*

The target NPU/ μ BST will decrypt the backup file, extract all the configuration files and databases and will store them, replacing existing files/databases. The NPU/ μ BST should be reset to apply the downloaded configuration.



NOTE

To avoid loss of connectivity behind a router, the basic IP parameters of the MGMT and DATA ports (IP Address, Subnet Mask, Default Gateway) are not changed when loading a Full backup file to the NPU/ μ BST. The values of these parameters configured in the target NPU/ μ BST before the loading process, are maintained.

4.7.2.6 Monitor Inactivity Timeout

The Monitor Inactivity Timeout 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 60 minutes.

The default value is 10 minutes.

4.7.3 Configuration

The NPU Configuration menu, and the applicable options in the μ BST Configuration menu, enables viewing and updating parameters that define the functionality of the MGMT and DATA ports, the properties of authorized management stations and bridging functionality.

The following are the guidelines for configuring these parameters:

- All IP parameters of both ports should be configured. Otherwise, default values shall be used.
- The Destination Subnet parameters of the MGMT port enable defining an additional subnet of stations that can manage the device when connected via a router to the MGMT port. If OOB management via a router connected to the MGMT port is used, the parameters should be configured to ensure different subnets for the Data port, the Management port and the Management Port Destination Subnet.
- Authorized Manager(s) must be configured properly to enable remote management using AlvariSTAR (or another SNMP based application).

The NPU Configuration menu includes the following options:

- Management Port
- Data Port
- Authorized Managers
- Bridge

4.7.3.1 Management Port Parameters

These parameters define the IP parameters for the MGMT port, when this port is used for Out-Of-Band (OOB) management.

The Ethernet interface of the MGMT port in the NPU operates using Auto Negotiation, enabling communication at either 10 Mbps or 100 Mbps.

The Ethernet interface of the MGMT port in the μ BST can be configured to operate either using Auto Negotiation or at a fixed speed/duplex mode (enabling selection between 10 Mbps Half Duplex, 10 Mbps Full Duplex, 100 Mbps Half Duplex or 100 Mbps Full Duplex).

4.7.3.1.1 Management Port IP Address

The IP address of the MGMT port.

The default is 10.0.0.1.

4.7.3.1.2 Management Port Subnet Mask

The Subnet mask of the MGMT port.

The default is 255.255.255.0.

4.7.3.1.3 Management Port Gateway

The Gateway IP address of the MGMT port.

The default is 0.0.0.0.

4.7.3.1.4 Management Port Dest Subnet **and** Management Port Dest Subnet Mask

The Destination Subnet parameters define the IP subnet of stations that can manage the device when connected via a router to the MGMT port. All management frames destined for addresses belonging to this group will be routed via the MGMT port. All management frames that are not destined for these addresses, or to addresses belonging to the MGMT port local subnet, will be routed via the DATA port.

The default is 0.0.0.0. for both parameters.



NOTE

The Management Port Gateway, Destination Subnet and Destination Subnet Mask are grouped together. Exiting the configuration process (e.g. by pressing the Esc button) after configuring just the first one or two parameters in this group will cancel the changes made.

4.7.3.1.5 Auto Negotiation Option (μBST)

The Management port of the μBST can be configured to operate with Auto Negotiation Option enabled or disabled.

The default is Enabled.

When the Auto Negotiation Option is enabled, the Speed and Duplex parameter in the relevant Show menus displays the detected operation mode. When the Auto Negotiation Option is disabled, the Speed and Duplex parameter in the relevant Show menus displays the configured operation mode. Upon selection of the Disable option, the user is prompted to select the speed and duplex:

4.7.3.1.5.1 Select Link Speed and Duplex

This option is applicable only when the Auto Negotiation Option is disabled. The available options are 10 Mbps Half Duplex, 10 Mbps Full Duplex, 100 Mbps Half Duplex and 100 Mbps Full Duplex.

4.7.3.1.6 Management Port Management Traffic Enable/Disable

The Management Port Management Traffic Enable/Disable parameter allows enabling/disabling the MGMT port.



NOTE

To prevent the undesired situation where management traffic is unintentionally disabled in both the MGMT and DATA ports, the Data Port Management Traffic Enable/Disable parameter will be automatically forced to Enabled upon disabling the Management Port Management Traffic, and vice versa.

4.7.3.2 Data Port Parameters

These parameters define the IP parameters for the Data port connecting the base station to the backbone. The DATA port can also be used for In-Band (IB) management, provided that IB management is enabled. In the current version In-Band management via the DATA port is always enabled.

4.7.3.2.1 Data Port IP Address

The IP address of the DATA port.

The default is 1.1.1.3.

4.7.3.2.2 Data Port Subnet Mask

The subnet mask of the DATA port.

The default is 255.255.255.0.

4.7.3.2.3 Data Port Gateway

The Gateway IP address of the DATA port.

The default is 0.0.0.0.

4.7.3.2.4 Data Port Management VLAN

This parameter defines the VLAN ID for management frames. If a value between 0 to 4094 is configured for the Management VLAN ID, then the device will accept management frames only if their VLAN tag is the same as this value.

Available values are 0-4094 or null (empty) for No VLAN.

The default is null (No VLAN).

4.7.3.2.5 Data Port Speed (NPU)

The speed of the Ethernet interface that operates always in full-duplex mode.

The available options are 100 Mbps and 1 Gbps.

The default speed is 100 Mbps.

4.7.3.2.6 Auto Negotiation Option (μBST)

The Data port of the μBST can be configured to operate with Auto Negotiation Option enabled or disabled.

The default is Enabled.

When the Auto Negotiation Option is enabled, the Speed and Duplex parameter in the relevant Show menus displays the detected operation mode. When the Auto Negotiation Option is disabled, the Speed and Duplex parameter in the relevant Show menus displays the configured operation mode. Upon selection of the Disable option, the user is prompted to select the speed and duplex:

4.7.3.2.6.1 Select Link Speed and Duplex

This option is applicable only when the Auto Negotiation Option is disabled. The available options are 10 Mbps Half Duplex, 10 Mbps Full Duplex, 100 Mbps Half Duplex and 100 Mbps Full Duplex.

4.7.3.2.7 Data Port Management Traffic Enable/Disable

The Data Port Management Traffic Enable/Disable parameter allows enabling/disabling management traffic via the DATA port.



NOTE

To prevent the undesired situation where management traffic is unintentionally disabled in both the MGMT and DATA ports, the Management Port Management Traffic Enable/Disable parameter will be automatically forced to Enabled upon disabling the Data Port Management Traffic, and vice versa.

4.7.3.3 Authorized Managers

The Authorized Managers submenu enables defining the properties of management stations that are allowed to manage the Base Station.

The Authorized Manager submenu includes the following options:

4.7.3.3.1 Show All

Select this option to view the details of all currently defined authorized managers.

4.7.3.3.2 Select

This option enables selecting an existing authorized manager for viewing or updating its properties or for deleting it from the database. The selection is based on the authorized manager's IP address. Refer to the following Add section for details on the configurable parameters.

4.7.3.3.3 Add

Select this option to add a new authorized manager. Up to 10 Authorized Manager can be defined. The following parameters can be configured:

4.7.3.3.3.1 IP Address

The IP address of the Authorized Manager.

4.7.3.3.3.2 Send Traps

The Send Traps parameters whether to enable or disable sending of traps to the Authorized Manager.

4.7.3.3.3.3 Read Community

The SNMP Read Community to be used by the Authorized Manager. A null Read Community means that the read (get) operation can only be performed using the Write Community.

Valid Community strings: Up to 23 printable characters, case sensitive.

4.7.3.3.3.4 Write Community

The SNMP Write Community to be used by the Authorized Manager. A null Write Community means that the Authorized Manager has Read-only access rights.

Valid Community strings: Up to 23 printable characters, case sensitive.

4.7.3.4 Bridge

The Bridge submenu enables configuring the **Bridge Aging Time** parameter, setting the aging time for all addresses in the Forwarding Data Base.

The available values are from 1 to 1440 minutes.

The default is 10 minutes.

4.7.4 Performance Monitoring

The Performance Monitoring option enables to view and reset the NPU Ethernet Ports counters. The Performance Monitoring submenu includes the following options:

- Data Port
- Management Port
- All counters

4.7.4.1 Data Port Counters

The Data Port option enables viewing or resetting the DATA port counters. The information displayed for each counter is the accumulated number since the last time the counters were reset. The counters are reset each time the NPU is reset, or upon activating the Reset Counters option.

The Data Port counters include:

■ Data Port Rx Counters

- ◇ Packets Received from Ethernet
- ◇ Packets Transmitted to Internal
- ◇ Packets Transmitted to Slot 1
- ◇ Packets Transmitted to Slot 2
- ◇ Packets Transmitted to Slot 3
- ◇ Packets Transmitted to Slot 4
- ◇ Packets Transmitted to Slot 7
- ◇ Packets Transmitted to Slot 8
- ◇ Packets Transmitted to Slot 9
- ◇ Packets Received Errors
- ◇ Packets Received Discards

■ Data Port Tx Counters

- ◇ Packets Transmitted to Ethernet
- ◇ Packets Received from Internal
- ◇ Packets Received from Slot 1
- ◇ Packets Received from Slot 2
- ◇ Packets Received from Slot 3

- ◇ Packets Received from Slot 4
- ◇ Packets Received from Slot 7
- ◇ Packets Received from Slot 8
- ◇ Packets Received from Slot 9
- ◇ Packets Transmitted Errors
- ◇ Packets Transmitted Discards

4.7.4.2 Management Port Counters

The Management Port option enables viewing or resetting the MGMT port counters. The information displayed for each counter is the accumulated number since the last time the counters were reset. The counters are reset each time the NPU is reset, or upon activating the Reset Counters option.

The Management Port counters include:

- Management Port Rx Counters
 - ◇ Packets Received from Ethernet
 - ◇ Packets Received Errors
- Management Port Tx Counters
 - ◇ Packets Transmitted to Ethernet
 - ◇ Packets Transmitted Errors

4.7.4.3 All Counters

The All Counters option enables viewing or resetting both the DATA port and the MGMT port counters.

4.8 AU Menu

The AU menu includes the following options:

- Show Summary
- SW Files in NPU
- Select

Following is a detailed description of these options.

4.8.1 Show Summary

Select this option to view the current status of all AUs.

For each applicable slot (1-4, 7-9), the display includes the following information:

- AU Slot ID
- Status: Installed/Not Installed
- Fault Status
- SW File Name: For an installed AU, this is the SW file of the running version. For a “Not Installed” AU, this is the SW file in the NPU to be loaded to the AU when it is installed as well as after each reset (depending on the configured Operation).
- SW Version: For an installed AU, this is the running SW version. For a “Not Installed” AU, this is the SW Version of the SW file in the NPU to be loaded to the AU when it is installed as well as after each reset (depending on the configured Operation).
- Operation: The operation to be performed with the loaded file when the AU is installed, as well as after each reset: Null (do not load), Load (load to Shadow), Run from Shadow or Set as Main.
- SW Download Status: The status of the last SW download operation (or None).
- Maximum Number of Voice Calls: The maximum number of voice calls that can be supported by the AU.

For more details on SW File/Version and Operation refer to [SW Versions Control](#) on page 119.

4.8.2 SW Files in NPU

Up to three AU SW files can be stored in the NPU. Any of the available files can be loaded by the NPU to a selected AU. When three AU files are stored in the NPU, a new file cannot be added until at least one of the existing files is deleted. This menu enables viewing the current AU SW files stored in the NPU and deleting selected file(s).

4.8.2.1 Show Files

Select this option to display the AU SW files currently stored in the NPU. For each available SW file, the file name and the version are shown.

4.8.2.2 Delete a File

Select this option and enter the name of an existing AU SW file to delete it from the NPU's memory.

4.8.3 Select

Use this option and select a slot to access the AU Slot # menu that will enable managing and configuring the AU in the selected slot, or pre-configuring the AU that will be installed in the slot at a later time.

The available AU slot IDs are 1-4, 7-9.

4.8.4 AU Slot # Menu

The AU Slot # menu enables managing and configuring the AU in the selected slot, or pre-configuring the AU that will be installed in the slot at a later time. The AU Slot # menu includes the following options:

- Show
- Unit Control
- Configuration
- Performance Monitoring

4.8.4.1 Show

Select this option to view the current value/selected option of applicable parameters. In addition, some general status information is shown, as follows:

■ General Parameters:

- ◇ IDU Serial Number
 - ◇ IDU IF Card HW Revision
 - ◇ IDU IF Card HW Configuration
 - ◇ IDU Boot Version

 - ◇ ODU Serial Number
 - ◇ ODU HC08 Version
 - ◇ ODU CPLD Version

 - ◇ IDU Main Card HW Revision
 - ◇ IDU Main Card HW Configuration
 - ◇ IDU Temperature (Celsius)

 - ◇ ODU HW Revision
 - ◇ ODU HW Configuration
 - ◇ ODU Temperature (Celsius)
- SW Files and Versions:
- ◇ Main SW File Name
 - ◇ Main SW Version

- ◇ Shadow SW File Name
- ◇ Shadow SW Version
- ◇ Running From (Main or Shadow)

■ MAC Parameters:

- ◇ Base Station ID
- ◇ ARQ Enable/Disable
- ◇ Maximum Cell Radius (km)

■ Phy Parameters:

- ◇ Frequency Band
- ◇ Bandwidth (MHz)
- ◇ Downlink (Tx) Frequency (MHz)
- ◇ Tx Power (dBm)

■ Multirate Parameters:

- ◇ Multirate Enable/Disable
- ◇ Uplink Basic Rate
- ◇ Downlink Basic Rate

■ ATPC Parameters:

- ◇ ATPC Enable/Disable
- ◇ Optimal Uplink RSSI (dBm)

■ Voice Parameters:

- ◇ Maximum Number of Voice Calls

4.8.4.2 Unit Control

The AU Unit Control menu enables resetting the AU and managing the SW versions of the module.

The Unit Control menu includes the following options:

- Reset
- Set Factory Defaults
- SW Version Control

4.8.4.2.1 Reset Unit

Select this option to reset the unit. To avoid unintentional reset, you will be prompted to confirm the reset request. Changes to some of the configurable parameters are applied only after reset. Refer to [NPU/Micro Base Station Parameters Summary](#) on page 177 for information on which parameters are changeable in run time and which changes are applied only after reset.

4.8.4.2.2 Set Factory Defaults

Select this option to set the AU parameters to their factory default values. Refer to [NPU/Micro Base Station Parameters Summary](#) on page 177 for information on the factory default values of these parameters. The parameters will revert to their default values after the next reset.

4.8.4.2.3 SW Versions Control

The AU can contain two SW versions:

- Main: Each time the AU resets it will reboot using the version defined as Main.
- Shadow: Normally, the Shadow version is the backup version. Each time a new SW File is downloaded to the AU, it will be stored as a Shadow version, replacing the previous Shadow Version.

The process of upgrading to a new SW version is controlled by the NPU, and is performed using one of the AU SW files installed in the NPU. If the specified AU SW file does not exist in the AU, it will be downloaded to the AU and the requested operation will be executed, as described below. If it already exists in the AU, then actual loading is not necessary.

The following options are available in the SW Version Control menu:

4.8.4.2.3.1 Show Versions

Select this option to view the following information:

■ Versions in AU:

- ◇ Main SW File Name
- ◇ Main SW Version
- ◇ Shadow SW File Name
- ◇ Shadow SW Version
- ◇ Running From: Main or Shadow

■ Available Versions in NPU: The available AU SW file names and the SW version of each file.

4.8.4.2.3.2 None

Select None to cancel a pending request for another operation (An operation will be executed only after the next reset).

4.8.4.2.3.3 Download

Select this option to download a specified SW file to the Shadow memory of the AU.

If the file already exists in the AU, no action will take place.

4.8.4.2.3.4 Run from Shadow

Select this option to download a specified SW file from the NPU to the Shadow memory of the AU, reset the AU and reboot using the Shadow version. Note that because the process is controlled by the NPU, the AU will continue running from the Shadow version after reset.

If the specified file already exists as the Shadow version (meaning that previously a Download operation was executed for this file name), the only actual operation to take place will be to reset and run from Shadow.

If the specified file already exists as the Main version, no action will take place.

4.8.4.2.3.5 Set as Main

Select this option to download a specified SW file from the NPU to the Shadow memory of the AU, reset the AU and reboot using the Shadow version, and then swap the Main and Shadow SW Version, so that the running version (which was previously the Shadow version) will become the Main version, to be used after next reset.

If the specified file already exists as the running version and it is defined as the Shadow version (meaning that previously a Download and Run from Shadow operation was executed for this file name), the only actual operation to take place

will be to swap the Main and Shadow versions. If it is already defined as the Main version, no action will take place.

4.8.4.3 Configuration

The AU Configuration menu enables viewing and updating the AU's parameters. It is important to note that changes to some parameters take effect only after reset. For these parameters, the applicable Show menus display the Current as well as the Configured value.

The Configuration menu includes the following options:

- MAC
- Phy
- Multirate
- ATPC
- Voice Parameters

4.8.4.3.1 MAC Parameters

The AU MAC menu includes the following options:

4.8.4.3.1.1 Show

Select this option to view the current values/options of the MAC (Media Access Control) parameters.

4.8.4.3.1.2 Update

Select this option to update any of the MAC parameters. The MAC parameters are:

- Base Station ID

The Base Station ID is the unique identifier of the AU/ μ BST. An SU can be authenticated by the AU/ μ BST only if its Base Station ID and Base Station mask match the Base Station ID configured for the AU/ μ BST. A change in the Base Station ID will take effect only after resetting the AU/ μ BST.

The Base Station ID consists of 6 groups of up to three digits each, where the range for each group is 0 to 255. The first 3 groups define the Operator ID, the next two groups define the Cell ID and the sixth group defines the AU/ μ BST ID.

Changes in Base Station ID are applied only after reset

The default Base Station ID is 186.190.0.0.0.0

■ ARQ Enable/Disable

The ARQ Enable/Disable parameter controls whether to use an ARQ algorithm for detecting errors and requesting retransmissions of applicable unicast messages (applicable only for Best Effort and Non Real Time services).

The default is Disable.

■ Maximum Cell Radius

The Maximum Cell Radius is used to adapt various timing parameters of the MAC to the time it takes a message to reach its destination. This time delay is dependent upon the distance between the originating and receiving units. The timing parameters should be adapted to the largest expected delay, which is determined from the distance from the AU/ μ BST of the farthest SU served by it.



NOTE

For Non-Line-Of-Sight (NLOS) links using refractions, the cell distance should be higher than the line-of-sight distance. Typically a 10% margin is a good estimate for the increase in distance due to the NLOS operation.

The basic time element (symbol) used by the system is 68 microseconds. This symbol size is translated to a round trip delay of approximately 20 km, or a cell radius of 10 km. Thus, it is recommended to set the Maximum Cell Radius using a resolution of 10 km: the actual timing of the system is the same for any cell radius larger than $N \times 10$ km and smaller than or equal to $(N+1) \times 10$.



NOTE

An SU located at a distance larger than the Maximum Cell Radius will be rejected during the network entry process.

The values range is from 10 to 100 km. Use 10 km increments (10, 20, 30,100).

The default is 20 km.

4.8.4.3.2 Phy Parameters

The AU Phy Parameters menu includes the following options:

4.8.4.3.2.1 Show

Select this option to view the current values/options of the Phy (Physical Layer) parameters. The radio band of the ODU is also displayed when an AU-IDU connected to an AU-ODU is installed in the slot.

4.8.4.3.2.2 Update

Select this option to update any of the Phy parameters. The Phy parameters are:

■ Bandwidth

The frequency bandwidth used by the radio. A change in the Bandwidth parameter will take effect only after resetting the AU/ μ BST.

The available options are:

1 – 1.75 MHz

2 – 3.5 MHz

The default is 3.5 MHz.

■ Downlink (Tx) Frequency

The frequency used in the downlink (from AU/ μ BST to SU). The frequency in the uplink (SU to AU/ μ BST) is the Uplink frequency minus 100 MHz. A change in the Downlink (Tx) Frequency parameter will take effect only after resetting the AU/ μ BST.

The resolution is in increments of 0.125 MHz. The available values depend on the radio band of the ODU and on the Bandwidth, as follows:

Table 4-4: Range for the Downlink (Tx) Frequency Parameter		
Radio Band	Bandwidth	Downlink (Tx) Frequency Range (MHz)
3.5a	3.5 MHz	3501.25 to 3551.75
	1.75 MHz	3500.375 to 3552.625
3.5b	3.5 MHz	3551.75 to 3598.25
	1.75 MHz	3550.875 to 3599.125



NOTE

If the Radio Band is not known (e.g. the ODU is not installed) then the available range depends only on the Bandwidth, as follows:

For a Bandwidth of 3.5 MHz: 3501.25 to 3598.25.

For a Bandwidth of 1.75 MHz: 3500.375 to 3599.125.

The default is 3551.75 MHz.

■ Tx Power

The Tx Power parameter defines the power level of the transmitted signal at the antenna port of the AU-ODU.

The range is from 13 to 28 dBm using a 0.25 dBm resolution.

The default is 28 dBm.

4.8.4.3.3 Multirate Parameters

BreezeMAX employs a multirate algorithm to dynamically adapt the modulation scheme and Forward Error Correction (FEC) coding to actual link conditions. The algorithm is managed by the AU/ μ BST taking into account also information received from the served SUs, and optimal values are calculated separately for the uplink and downlink for each SU, taking into account also the applicable QoS requirements. MAP messages transmitted to the SUs include information on the uplink rate that should be used by each SU for its next transmission.

The Basic Rate is the minimum rate to be used by the Multirate algorithm. In the downlink, this is also the rate to be used for broadcasts and multicasts.

Broadcasts and multicasts messages are not acknowledged, so that the ARQ mechanism cannot be used and there is no way to guarantee that all intended recipients will receive them properly. In addition, AU's/ μ BST's multicasts and broadcasts are sent to multiple recipients with different link qualities. Therefore, it is preferable to use a relatively low rate for these transmissions, thus reducing the probability of errors and increasing the likelihood that all intended recipients will receive them properly.

In the uplink, this is the rate to be used by SUs for non-scheduled transmissions, such as during the contention period.

The Basic Rate is also the initial rate to be used by the algorithm for each new SU that joins the cell when the Multirate algorithm is enabled.

When the Multirate algorithm is disabled, communication with connected SUs will continue using the last uplink and downlink rates selected by the Multirate algorithm. The Set Rates option in the SU (see [Set Rates](#) on page 143), which becomes available only when the Multirate algorithm is disabled in the AU/ μ BST, enables setting the Uplink Current Rate and the Downlink Current Rate to any of the values listed in Table 4-5.

The multirate algorithm chooses dynamically between 8 rates. These are also the rates that can be configured for the Base Rate and Default Rate parameters.

Table 4-5: Rates (Modulation Schemes and Coding)	
No.	Rate
1	BPSK 1/2
2	BPSK 3/4
3	QPSK 1/2
4	QPSK 3/4
5	QAM16 1/2
6	QAM16 3/4
7	QAM64 2/3
8	QAM64 3/4

4.8.4.3.3.1 Show

Select this option to view the current values/options of the Multirate algorithm parameters.

4.8.4.3.4 Update

Select this option to update any of the Multirate parameters. The Multirate parameters are:

4.8.4.3.4.1 Multirate Enable/Disable

The Multirate Enable/Disable parameter controls whether the multirate algorithm should be used to determine current optimal rates in both the uplinks and the downlinks.

The default is Enable.



NOTE

The multirate algorithm should always be enabled. The option to disable it is available to enable using a fixed rate to support certain tests. After each reset, the AU/ μ BST boots with the multirate enabled, disregarding its status before the device was reset.

4.8.4.3.4.2 Uplink Basic Rate

The Basic Rate for all uplinks.

The available options are listed in Table 4-5 on page 125.

The default rate is the lowest rate BPSK 1/2 (rate 1).

4.8.4.3.4.3 Downlink Basic Rate

The Basic Rate for all downlinks.

The available options are listed in Table 4-5 on page 125.

The default rate is the lowest rate BPSK 1/2 (rate 1).

4.8.4.3.5 ATPC Parameters

BreezeMAX employs an Automatic Transmit Power Control (ATPC) algorithm to dynamically adapt the transmit power of each SU so that it is received by the AU/ μ BST at an optimal level. The algorithm is managed by the AU/ μ BST and optimal values are calculated separately for each SU based on the actual level at which it is received by the AU/ μ BST. MAP messages transmitted to the SUs include information on the estimated up/down power level change required to achieve optimal transmit power level.

4.8.4.3.6 Show

Select this option to view the current values/options of the ATPC algorithm parameters.

4.8.4.3.7 Update

Select this option to update any of the ATPC parameters. The ATPC parameters are:

4.8.4.3.7.1 ATPC Enable/Disable

The ATPC Enable/Disable parameter controls whether the ATPC algorithm should be used to determine current optimal transmit level for each SU served by the AU/ μ BST.

The default is Enable.



NOTE

The ATPC algorithm should always be enabled. The option to disable it is available to enable using a fixed rate to support certain tests. After each reset, the AU/ μ BST boots with the ATPC enabled, disregarding its status before the device was reset.

4.8.4.3.7.2 Optimal Uplink RSSI

The Optimal Uplink RSSI sets the target level at which all transmissions should be received by the AU/ μ BST for optimal performance.

The range is -103 to -60 (dBm).

The default is -69 dBm.

4.8.4.3.8 Voice Parameters

The Voice Parameters option includes a single parameter, Maximum Number of Voice Calls:

4.8.4.3.8.1 Maximum Number of Voice Calls

This parameter sets the upper limit of simultaneous voice calls that will be supported by the AU.

The range is from 0 to 300 Voice Calls.

The default is 50.

4.8.5 Performance Monitoring

The AU Performance menu includes the following options:

- Port Counters
- BER Test
- Burst Error Rate Counters

4.8.5.1 Ports Counters

The Ports Counters option enables viewing or resetting the Ethernet and Wireless ports counters. The information displayed for each counter is the accumulated number since the last time the counters were reset. The counters are reset each time the AU is reset, or upon activating the Reset option.



NOTE

The Ethernet port in the AU is the internal port between the AU and the NPU.

The counters indicate the traffic at the Ethernet and Wireless ports, as described in the following figure:

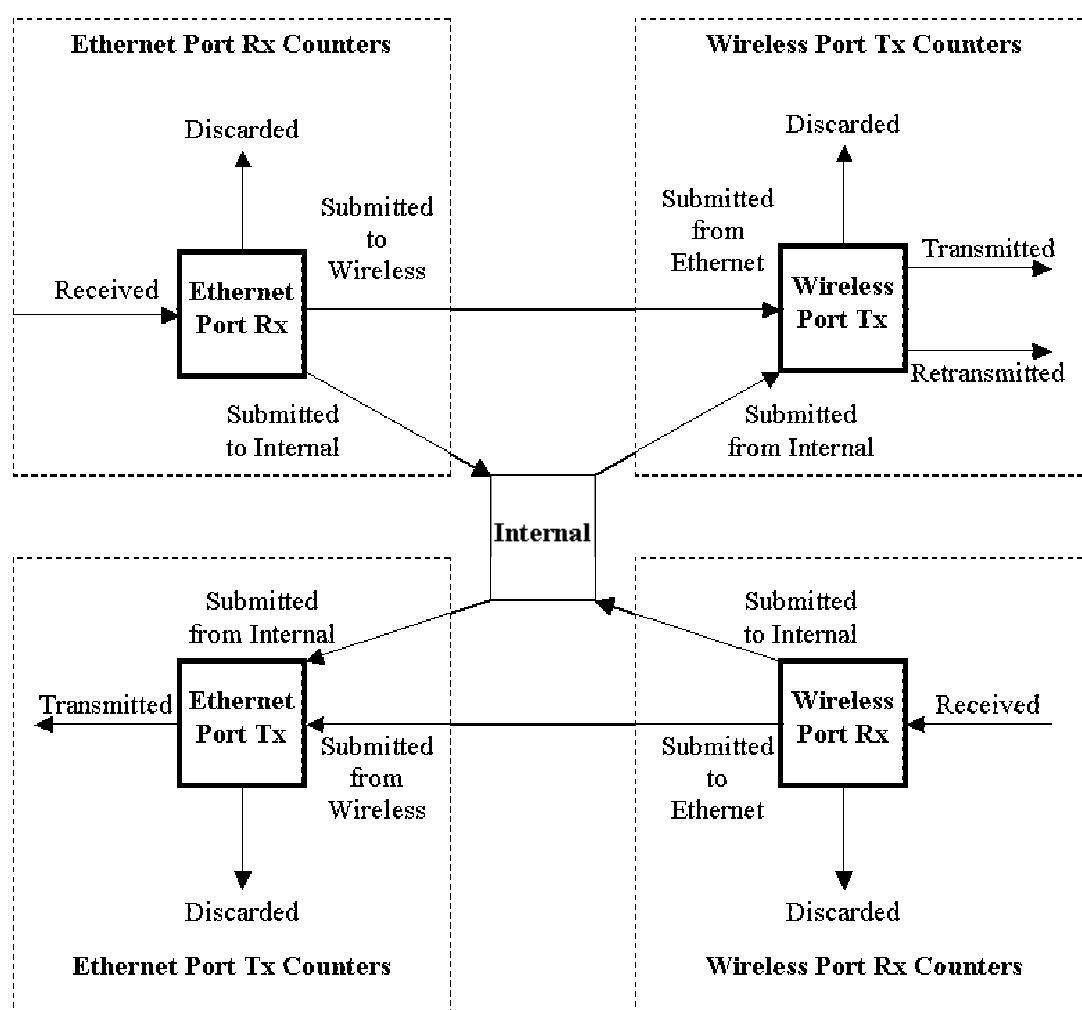


Figure 4-4: Counters Description

For each port, the counters include the frames that were actually transmitted to/received from the port, the frames transferred to/from the other port (submitted), and the frames received from/transmitted to the Internal port. The Internal port refers to the internal management module of the unit that receives and transmits management and control frames to/from both the Ethernet and the Wireless ports.

In addition, for each port, the frames that were discarded for various reasons (errors, overflow etc.) are also counted.

In the Wireless Tx port, the retransmitted frames and the transmitted unicast frames (not shown in the schematic diagram) are also counted. These counters serve for calculating the retransmissions rate, providing some indication on link quality.

The displayed counters include:

■ Ethernet Port Rx Counters

- ◇ Bytes Received from Ethernet
- ◇ Bytes Discarded
- ◇ Bytes Submitted to Wireless
- ◇ Bytes Submitted to Internal
- Ethernet Port Tx Counters
 - ◇ Bytes Submitted from Wireless
 - ◇ Bytes Submitted from Internal
 - ◇ Bytes Transmitted to Ethernet
 - ◇ Bytes Discarded
- Wireless Port Rx Counters
 - ◇ Bytes Received from Wireless
 - ◇ Bytes Submitted to Ethernet
 - ◇ Bytes Submitted to Internal
 - ◇ Bytes Discarded
- Wireless Port Tx Counters
 - ◇ Bytes Submitted from Ethernet
 - ◇ Bytes Submitted from Internal
 - ◇ Bytes Transmitted to Wireless
 - ◇ Bytes Discarded
 - ◇ Unicast Bytes Transmitted
 - ◇ Bytes Retransmitted
 - ◇ Retransmission Rate (%)

**NOTE**

Retransmission Rate is defined as:

$100 \times \text{Bytes Retransmitted} / (\text{Unicast Bytes Transmitted to Wireless})$

Note that unacknowledged bytes are retransmitted only if ARQ is enabled. Retransmission is applicable only for information transmitted using either Best Effort (BE) or Non Real Time (NRT) Quality of Service.

4.8.5.2 BER Test

The BER Test sub-menu enables to initiate a BER test on the link with a specific SU, including definition of test parameters, to terminate a test and to view test results. It includes the following options:

- Start Test
- Stop Test
- Show Test Parameters and Results

4.8.5.2.1 Start Test

Select this option to define the parameters for a Bit Error Rate test and to initiate a test. The test will be initiated after all parameters have been configured. The parameters are:

4.8.5.2.1.1 SU MAC Address

The BER test is performed on a link with a specific SU. This is the MAC address of the applicable SU.

4.8.5.2.1.2 Number of Bytes

The number of BER test bytes to be transmitted. The available range is from 1,000 to 100,000,000 Bytes.

4.8.5.2.1.3 Rate

The rates to be used for the BER test in the uplink and downlink. Refer to Table 4-5 on page 125 for details on the available rates.

4.8.5.2.1.4 Burst Size (Bytes)

The burst size in bytes. The available range is from 500 to 4,000 Bytes.

4.8.5.2.1.5 Test Priority

The service priority of the BER test. Services with higher priority will not be affected by the test. The available options are RT (Real time), NRT (Non Real Time), and BE (Best Effort).

4.8.5.2.2 Stop Test

Select this option to terminate a currently running BER test.

4.8.5.2.3 Show Test Parameters and Results

Select this option to see the parameters of the last BER test and the results. The displayed results include the measured BER in the uplink and downlink.

4.8.5.3 Burst Error Rate Counters

The Burst Error rate Counters option enables selecting a specific SU by its MAC address for viewing or resetting the Burst Error Rate counters for the applicable downlink. The information displayed for each rate in downlink is the accumulated number since the last time the counters were reset. The uplink counters can be viewed in the applicable SU. For each rate the displayed information includes:

- Total Burst
- Error Bursts
- Error Rate

The counters are reset each time the AU is reset, or upon activating the Reset option.

4.9 SU Menu

The SU menu includes the following options:

- Show Summary
- Show Summary by AU
- SW Files in NPU
- Select by Name
- Select by MAC Address
- Add

Following is a detailed description of these options.

4.9.1 Show Summary

Select this option to view summary information and main details for all connected and pre-configured SUs.

- For each SU, the following information is displayed:
 - ◇ MAC Address
 - ◇ SU Name
 - ◇ SU Status (Permanent or Temporary)
 - ◇ Connected AU Slot ID
 - ◇ Registration Status (In Service, Out Of Service)
 - ◇ SW File Name: For a connected SU, this is the SW file of the running version. For an SU that is defined but is not connected, this is the SW file in the NPU/ μ BST to be loaded to the SU when it is connected, as well as after each reset (depending on the configured Operation).
 - ◇ SW Version: For a connected SU, this is the running SW version. For an SU that is defined but is not connected, this is the SW Version of the SW

file in the NPU/ μ BST to be loaded to the SU when it is installed, as well as after each reset (depending on the configured Operation).

- ◇ Operation: The operation to be performed with the loaded file when the SU is connected, as well as after each reset: Null (do not load), Load (load to Shadow), Run from Shadow or Set as Main.
- ◇ SW Download Status: The status of the last SW download operation (or None).
- ◇ SU IDU Type
- ◇ Number of Gateways: The number of Alvarion Gateways connected to the SU IDU.

■ Summary Information:

- ◇ Total Number of SUs: The total number of SUs in the database (including connected and pre-configured SUs)
- ◇ Total Connected SUs
- ◇ SUs Connected to AU Slot N, where N=1-4, 7-9.



NOTE

An SU that is defined as Temporary will be deleted from the database when it is disconnected.

4.9.2 Show Summary by AU

Select this option to view the total number of SUs connected to a specific AU as well as main details on these SUs, as described in [Show Summary \(SU Manu\)](#) on page 132. You will be prompted to select the required AU Slot ID.

4.9.3 SW Files in NPU/ μ BST

Up to three SU SW files can be stored in the NPU/ μ BST. Any of the available files can be loaded by the NPU/ μ BST to a selected SU. When three SU files are stored in the NPU/ μ BST, a new file cannot be added until at least one of the existing files is deleted. This menu enables viewing the current SU SW files stored in the NPU/ μ BST and deleting selected file(s). It also enables defining a Default SU File, which is the file to be loaded to any new temporary SU when the Base Station operates in Quick Mode in order to provide it with the defined Default Service(s). Refer to [Services Menu – General Parameters](#) on page 150 for more information on Quick Mode and Default SU Profiles.

4.9.3.1 Show Files

Select this option to display the SU SW files currently stored in the NPU/μBST. For each available SW file, the file name and the version number are displayed.

In addition, the Default SW File Name and Default Action are also displayed.

4.9.3.2 Default File Name

The Default File Name is the name of the SU file to be used for new temporary SUs when operating in Quick Mode.

4.9.3.3 Default Action

The Default Action is the action to be taken with the Default SU File when a new temporary SU joins the cell when operating in Quick Mode.

The available options are:

- 1 - None
- 2 - Download
- 3 -Run from Shadow
- 4 - Set as Main

4.9.3.4 Delete a File

Select this option and enter the name of an existing SU SW file to delete it from the NPU/μBST Flash memory.

4.9.4 Select by Name

Use this option to select an SU by name to access the SU # menu that will enable managing and configuring the selected SU, viewing its performance information or deleting it from the database.

4.9.5 Select by MAC Address

Use this option to select an SU by its MAC address to access the SU # menu that will enable managing and configuring the selected SU, viewing its performance information or deleting it from the database.

4.9.6 SU # Menu

The SU # menu enables managing and configuring the selected SU. The SU # menu includes the following options:

- Show
- Unit Control

- Configuration
- Performance Monitoring
- Delete

4.9.6.1 Show

Select this option to view the current value/selected option of applicable parameters. In addition, some general status information is displayed, as follows:

- Equipment and Registration Parameters:

- ◇ MAC Address
- ◇ SU Name
- ◇ Organization Name
- ◇ Address
- ◇ Country Code
- ◇ SU Status (Permanent or Temporary)
- ◇ Connected AU Slot ID
- ◇ SU IDU Type
- ◇ Number of Gateways

- Current Link Quality Indicators

- ◇ Uplink RSSI (dBm)
- ◇ Uplink SNR (dB)
- ◇ Uplink Current Rate
- ◇ Downlink RSSI (dBm)
- ◇ Downlink SNR (dB)
- ◇ Downlink Current Rate

■ General ODU Parameters

- ◇ Serial Number
- ◇ RF Card HW Revision
- ◇ RF Card HW Configuration
- ◇ Boot Version
- ◇ Main Card HW Revision
- ◇ Main Card HW Configuration

■ SW Versions information:

- ◇ Main SW File Name
- ◇ Main SW Version
- ◇ Shadow SW File Name
- ◇ Shadow SW Version
- ◇ Running From (Main or Shadow)

■ MAC Parameters

- ◇ Base Station ID
- ◇ Base Station Mask

■ Phy Parameters

- ◇ Bandwidth (MHz)
- ◇ Uplink (Tx) Frequency (MHz)

■ ATPC Parameters

- ◇ ATPC Support
- ◇ TX Power (dBm)

■ Bridging Parameters

- ◇ Enable/Disable Limit on Number of Supported Devices
- ◇ Maximum Number of Supported Devices
- ◇ Bridge Aging Time (minutes)

4.9.6.2 Unit Control

The SU Unit Control menu enables defining the SU's status, resetting the SU and managing the SW versions of the unit.

The Unit Control menu includes the following options:

- Status
- Reset
- Set Factory Defaults
- SW Version Control

4.9.6.2.1 SU Status

The SU Status parameter enables defining the status of the SU, which determines the services it can receive.

The available options are:

- 1 – Permanent
- 2 – Temporary



NOTE

An SU that is defined as Temporary will be deleted from the database when it is disconnected.

4.9.6.2.2 Reset Unit

Select this option to reset the unit. To avoid unintentional reset, you will be prompted to confirm the reset request. Changes to some of the configurable parameters are applied only after reset. Refer to [NPU/Micro Base Station Parameters Summary](#) on page 177 for information on which parameters are changeable in run time and which changes are applied only after reset.

4.9.6.2.3 Set Factory Defaults

Select this option to set the SU parameters to their factory default values. Refer to [SU Parameters Summary](#) on page 152 for information on the factory default

values of these parameters. The parameters will revert to their default values after the next reset.

4.9.6.2.4 SW Versions Control (only for Permanent SUs)

The SU can contain two SW versions:

- Main: Each time the SU resets it will reboot using the version defined as Main.
- Shadow: Normally the Shadow version is the backup version. Each time a new SW File is downloaded to the SU, it will be stored as a Shadow version, replacing the previous Shadow Version.

The process of upgrading to a new SW version is controlled by the NPU/ μ BST, and is performed using one of the SU SW files installed in the NPU/ μ BST. If the specified SU SW file does not exist in the SU, it will be downloaded to the SU and the requested operation will be executed, as described below. If it already exists in the SU, then actual loading is not necessary.

The following options are available in the SW Version Control menu:

- Show SW Versions
- None
- Download
- Run from Shadow
- Set as Main

4.9.6.2.4.1 Show SW Versions

Select this option to view the following information:

- SW Versions in SU:
 - ◇ Main SW File Name
 - ◇ Main SW Version
 - ◇ Shadow SW File Name
 - ◇ Shadow SW Version
 - ◇ Running From: Main or Shadow

- Available Versions in NPU/μBST: The available SU SW file names and the SW Version of each file.

4.9.6.2.4.2 None

Select None to cancel a pending request for another operation (an operations will be executed only after the next reset).

4.9.6.2.4.3 Download

Select this option to download a specified SW file from the NPU/μBST to the Shadow memory of the SU.

If the specified file already exists in the SU, no action will take place.

4.9.6.2.4.4 Run from Shadow

Select this option to download a specified SW file from the NPU/μBST to the Shadow memory of the SU, reset the SU and reboot using the Shadow version. Note that because the process is controlled by the NPU, the SU will continue running from the Shadow version after reset.

If the specified file already exists as the Shadow version (meaning that previously a Download operation was executed for this file name), the only actual operation to take place will be to reset and run from Shadow.

If the specified file is the current Main version, no action will take place.

4.9.6.2.4.5 Set as Main

Select this option to download a specified SW file from the NPU/μBST to the Shadow memory of the SU, reset the SU and reboot using the Shadow version, and then swap the Main and Shadow SW Version, so that the running version (which was previously the Shadow version) will become the Main version, to be used after next reset.

If the specified file already exists as the running version and it is defined as the Shadow version (meaning that previously a Download and Run from Shadow operation was executed for this file name), the only actual operation to take place will be to swap the Main and Shadow versions. If it is already defined as the Main version, no action will take place.

4.9.6.3 Configuration

The SU Configuration menu enables viewing and updating the SU's parameters.

The Configuration menu includes the following options:

- Registration
- MAC

- Phy
- Multirate and ATPC
- Voice/Networking Gateways
- Ethernet Port
- Installer Password
- Bridging Parameters

4.9.6.3.1 Registration Parameters

The SU Registration Parameters option in the NPU/μBST Monitor enables viewing the SU's Registration parameters. The Registration parameters can be configured only locally at the SU (via the Ethernet port).

4.9.6.3.1.1 SU Name

The default SU Name given to a new SU during the definition process (see [Add New SU](#) on page 149) is SU@<SU's MAC Address>.

An SU Name can be configured only for SUs that are not registered. When an SU is registered, it receives services based on its MAC address. When the SU connects and becomes registered, the SU Name in the Base Station/Micro Base Station will be replaced by the name configured in the SU (Common Name).

4.9.6.3.1.2 Organization Name

The Organization Name configured in the SU.

4.9.6.3.1.3 Address

The Address configured in the SU.

4.9.6.3.1.4 Country Code

The Country name configured in the SU.

4.9.6.3.2 MAC Parameters

The SU MAC Parameters menu includes the following options:

4.9.6.3.2.1 Show

Select this option to view the current values/options of the MAC parameters.

4.9.6.3.2.2 Update

Select this option to update any of the MAC parameters. The MAC parameters are:

4.9.6.3.2.2.1 Base Station ID

The Base Station ID is the identifier of the AU/ μ BST to which the SU can connect. An SU can be authenticated by an AU/ μ BST only if the Base Station ID and Base Station ID Mask configured in the SU match the Base Station ID configured for the AU/ μ BST. A change in the Base Station ID and Base Station ID Mask will take effect only after resetting the SU.

The Base Station ID consists of six groups of up to three digits each, where the range for each group is 0 to 255. The first three groups define the Operator ID, the next two groups define the Cell ID and the sixth group defines the Sector (AU) ID.

A change in the Base Station ID is applied only after reset.

The default Base Station ID is 186.190.0.0.0.0

4.9.6.3.2.2.2 Base Station ID Mask

The Base Station ID Mask, together with the Base station ID define the AU(s)/ μ BST(s) that can synchronize with the SU.

The Base Station ID Mask consists of 6 groups of up to 3 digits each, where the range of each group is 0 to 255. The first 3 groups form the mask for the Operator ID. The next 2 groups form the mask for the Cell ID, and the last group forms the mask for the Sector ID.

A change in the Base Station ID Mask is applied only after reset.

The default Base Station ID Mask is 255.255.255.0.0.0.

4.9.6.3.3 Phy Parameters

The SU Phy Parameters menu includes the following options:

4.9.6.3.3.1 Show

Select this option to view the current value/option of the Phy (Physical Layer) parameters.

4.9.6.3.3.2 Update

Select this option to update any of the Phy parameters. The Phy parameters are:

4.9.6.3.3.3 Bandwidth (MHz)

The frequency bandwidth used by the radio. A change in the Bandwidth parameter will take effect only after resetting the SU.

The available options are:

1 – 1.75 MHz

2 – 3.5 MHz

The default is 3.5 MHz.

4.9.6.3.3.4 Uplink (Tx) Frequency (MHz)

The frequency used in the uplink (from SU to AU/ μ BST). The frequency in the downlink (AU/ μ BST to SU) is the Uplink frequency plus 100 MHz.

A change in the Uplink Frequency parameter will take effect only after resetting the SU.

The resolution is in steps of 0.125 MHz. The available values depend on the Bandwidth, as follows:

For a Bandwidth of 3.5 MHz: 3401.25 to 3498.25.

For a Bandwidth of 1.75 MHz: 3400.375 to 3499.125.

The default is 3451.75 MHz.

4.9.6.3.4 Multirate and ATPC Parameters

The Multirate and ATPC mechanism are controlled by the AU/ μ BST (except to the option to temporarily control them locally at the SU for testing purposes). The Show Multirate and ATPC Status and Parameters option enables viewing the current status of the applicable parameters. The Set Rates option can be used to set uplink and downlink rates per SU only when Multirate is disabled.

4.9.6.3.4.1 Show

The Show option enables viewing the current status of the following parameters:

- Uplink RSSI (dBm)

- Uplink SNR (dB)
- Uplink Rate
- Downlink RSSI (dBm)
- Downlink SNR (dB)
- Downlink Rate
- ATPC Support
- Tx Power (dBm)

4.9.6.3.4.2 Set Rates

The Set Rates option is available only when the Multirate algorithm is disabled in the AU/ μ BST (see [Multirate Parameters](#) on page 124), allowing to set the Uplink Current Rate and the Downlink Current Rate to any of the values listed in Table 4-5 on page 125.

The defaults are the last rates used by the Multirate algorithm before it was disabled. For SUs that join the cell when the Multirate algorithm is disabled, the defaults are the applicable Basic Rates.

4.9.6.3.5 Voice/Networking Gateways

The Voice/Networking Gateways option enables viewing details on the Voice/Networking Gateways connected to the SU. This is applicable only for Alvarion's Gateways supporting the DRAP protocol. For each Gateway, the following details are provided:

- Gateway Type
- IP Address
- VLAN ID
- Number Of Active Calls (applicable only for Voice Gateways)

The following gateways are currently available from Alvarion:

- IDU-NG-4D1W: A Networking Gateway that serves also as an SU-IDU, supporting 4 data ports and 1 Wireless LAN port.
- AVG-1D1V: A stand-alone (external) Voice Gateway, supporting 1 data port and 1 POTS port, with advanced routing functionality.

- AVG-1D2V: A stand-alone (external) Voice Gateway, supporting 1 data port and 2 POTS ports, with advanced routing functionality.

4.9.6.3.6 Ethernet Port

The Ethernet Port menu enables configuration of the Ethernet port operation mode (speed and duplex).

4.9.6.3.6.1 Show

The Show option enables viewing the configured and actual operation modes:

- Current Mode: The current operation mode used by the SU.
- Configured Mode: The operation mode to be used by the SU after the next reset.
- Detected Mode: The actual operation mode. When the Current Mode is Auto Negotiation, the Detected Mode displays actual speed/duplex parameters used by the SU as a result of the auto negotiation process.

4.9.6.3.6.2 Update

Select the Update option to configure the **Ethernet Port Configuration** parameter. The available options are 10 Half, 10 Full, 100 Half, 100 Full and Auto Negotiation.

The default is Auto Negotiation.

4.9.6.3.7 Installer Password

The Installer Password option enables viewing the current Installer Password and configuring a new password. The Installer Password is used for accessing the SU's Monitor (Installer) program locally, using Telnet via the SU's Ethernet port.

The Installer Password consists of a string of up to 20 printable characters, case sensitive.

The default Installer Password is installer.

4.9.6.3.8 Bridging Parameters

The Bridging Parameters menu enables setting a limit on the maximum number of Ethernet devices behind the SU and configuring the aging time for devices in the SU's bridging table. The Bridging parameters are:

4.9.6.3.8.1 Enable/Disable Limit on Number of Supported Devices

If the Enable/Disable Limit on Number of Supported Devices parameter is set to Disable, the maximum number of supported devices is 512.

The default is Disable.

4.9.6.3.8.2 Maximum Number of Supported Devices

This parameter is applicable only when the Enable/Disable Limit on Number of Supported Devices parameter is set to Enable.

The available range is from 1 to 512 devices.

The default is 512.

4.9.6.3.8.3 Bridge Aging Time

The Bridge Aging Time sets the aging time for all addresses in the SU's Forwarding Data Base.

The available values are from 1 to 1440 minutes.

The default is 3 minutes.

4.9.6.4 Performance Monitoring

The Performance Monitoring sub-menu provides the following options:

- Ports Counters
- Burst Error Rate Counters

4.9.6.4.1 SU Ports Counters

The SU Ports Counters menu enables viewing or resetting the Ethernet and Wireless ports counters. The information displayed for each counter is the accumulated number since the last time the counters were reset. The counters are reset each time the SU is reset, or upon activating the Reset Counters option.

The counters indicate the traffic at the Ethernet and Wireless ports, as described in the following figure:

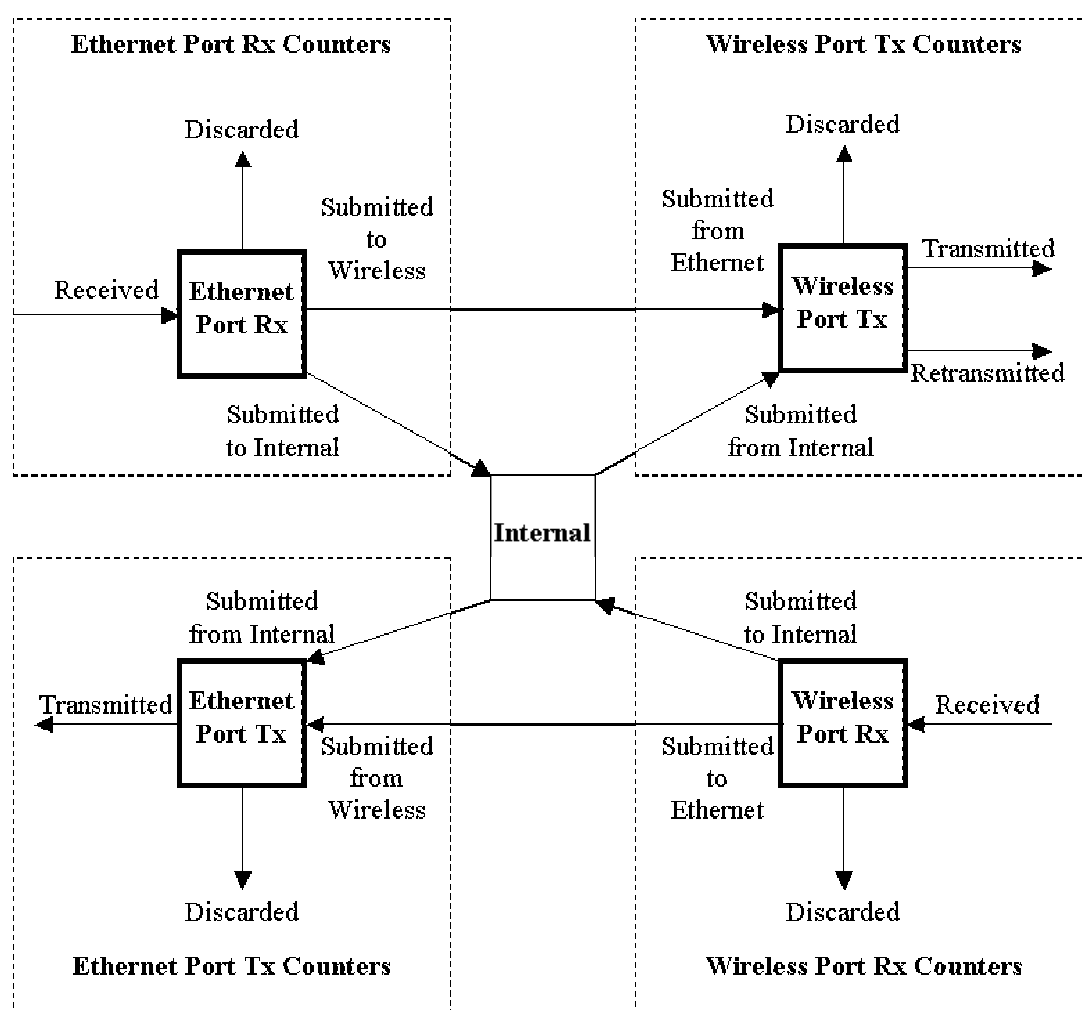


Figure 4-5: Counters Description

For each port, the counters include the frames that were actually transmitted to/received from the port, the frames transferred to/from the other port (submitted), and the frames received from/transmitted to the Internal port. The Internal port refers to the internal management module of the unit that receives and transmits management and control frames to/from both the Ethernet and the Wireless ports.

In addition, for each port, the frames that were discarded for various reasons (errors, overflow etc.) are also counted.

In the Wireless Tx port, the retransmitted frames and the transmitted unicast frames (not shown in the schematic diagram) are also counted. These counters serve for calculating the retransmissions rate, providing some indication on link quality.

The displayed counters include:

■ Ethernet Port Rx Counters

- ◇ Bytes Received from Ethernet
- ◇ Bytes Discarded
- ◇ Bytes Submitted to Wireless
- ◇ Bytes Submitted to Internal
- Ethernet Port Tx Counters
 - ◇ Bytes Submitted from Wireless
 - ◇ Bytes Submitted from Internal
 - ◇ Bytes Transmitted to Ethernet
 - ◇ Bytes Discarded
- Wireless Port Rx Counters
 - ◇ Bytes Received from Wireless
 - ◇ Bytes Submitted to Ethernet
 - ◇ Bytes Submitted to Internal
 - ◇ Bytes Discarded
- Wireless Port Tx Counters
 - ◇ Bytes Submitted from Ethernet
 - ◇ Bytes Submitted from Internal
 - ◇ Bytes Transmitted to Wireless
 - ◇ Bytes Discarded
 - ◇ Unicast Bytes Transmitted
 - ◇ Bytes Retransmitted
 - ◇ Retransmission Rate (%)

**NOTE**

Retransmission Rate is defined as:

$100 \times \text{Bytes Retransmitted} / (\text{Unicast Bytes Transmitted to Wireless})$

Note that unacknowledged bytes are retransmitted only if ARQ is enabled. Retransmission is applicable only for information transmitted using either Best Effort (BE) or Non Real Time (NRT) Quality of Service.

4.9.6.4.2 Burst Error Rate Counters

Data is transmitted in bursts, as described in the following figure, where each burst includes a CRC string.

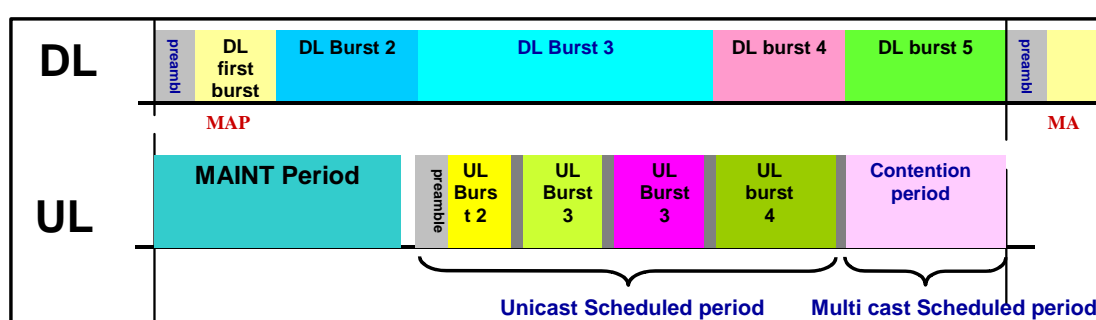


Figure 4-6: Uplink and Downlink Scheduled Transmissions

In the downlink, each burst uses a single rate and may include data intended for several SUs. In the uplink, each burst is from a different SU (also using a single rate).

The Burst Error rate Counters option enables viewing or resetting the uplink Burst Error Rate counters. The information displayed for each rate in uplink is the accumulated number since the last time the counters were reset. For each rate the displayed information includes:

- Total Burst
- Error Bursts
- Error Rate

The counters are reset each time the SU is reset, or upon activating the Reset option.

4.9.6.5 Delete

This option enables deleting the selected SU from the database.

4.9.7 Add New SU

Select the Add New SU option to add a new SU to the database. The Add New SU sub-menu includes the following parameters:

- SU MAC Address
- SW File Name: The SW File to be used by the SU. Should be either a File Name known to exist in the SU or an SU SW File Name in the Micro Base Station/NPU.

A new SU that attempts to communicate with the base station when the base station operates in Advanced Mode will be registered only if its MAC address exists in the database.

4.10 Services Menu

4.10.1 Introduction

4.10.1.1 Services

A Service is a virtual connection between a Subscriber's application and the Network Resource. The Network Resource could be Internet, Content Provider, Corporate Network, etc.

The Services are implemented as IEEE 802.16 connections within the wireless domain. Each Service can include up to 4 uplink and 4 downlink connections. Implementation within the provider's backbone domain depends on the specific backbone network.

A Subscriber is an entity that may be associated with any number of devices connected to any number of SUs. Each Service associates a certain Service Profile with Subscriber's device(s) behind a specific SU.

The Service Profile's properties depend on the Service Type. All data Services have the following properties:

- **VLAN ID based Classification:** Each Service can be associated with up to 16 VLAN IDs, enabling creation of VLANs within the wireless domain and differentiation of services to different end-users behind the same SU based on VLAN ID classification.



NOTE

In the current version, the proper use of VLAN ID based classification for differentiating among several end-users served by the same SU is possible only with a VLAN switch with VLAN Binding capability.

- **Quality of Service (QoS) and Priority based Classification:** Up to 4 uplink and 4 downlink QoS profiles can be assigned to each Service. The data will be mapped onto these connections by either IEEE 802.1p or DSCP priority tags. This will lead to creation of the corresponding number of Uplink and Downlink connections supporting differentiated services to up to 4 applications based on either IEEE 802.1p or DSCP prioritization schemes. In cases where prioritization is not used, a single pair of uplink/downlink connections is created.
- **Forwarding Rules:** A Forwarding Rule is assigned to each Service, defining various features that define the handling of certain message types in the wireless domain. These may include Unicast and Multicast Forwarding rules,

QoS Profile and VLAN ID for Multicasts and Unknown Address Forwarding Policy. The available features depend on the Service Type. The data may be switched only between the Services that share the same Forwarding Rule. In all other respects the service functions as a standard Bridge.

- **Aggregation:** Several Services in the Wireless Domain may be aggregated into a single Virtual Private Link (VPL) in the backbone domain.
- **Priority Marking:** Ethernet frames transmitted to the backbone may be marked with a configurable priority (DSCP or IEEE 802.1p), enabling the upstream network to handle the traffic accordingly.
- **Auto-configuration:** The Ethernet Addresses of the Subscribers' PCs are automatically learnt just as in a standard Bridge. For each Ethernet Address it also learns the VLAN behind the SU it belongs to.

Currently, the following Service types are supported:

- L2 (layer 2) Data Service
- PPPoE Data Service
- Voice Service

4.10.1.2 Service Types

4.10.1.2.1 L2 Service

L2 (Layer 2) service transports Layer 2 (Ethernet) frames between the subscriber's site and the Network Resource located behind the provider's backbone and/or between the subscriber's sites. It is assumed that the backbone either supports encapsulation of the Layer 2 frames (e.g. over ATM) or routes the frames according to the applicable Layer 3 protocol, which could be different from IP. The Network Resource is assumed to be a corporate network.



NOTE

An L2 Service supports also DRAP-based Voice Service, as described in the next page.

4.10.1.2.2 PPPoE Service

PPPoE (Point-to-Point Protocol over Ethernet) Access service provides connectivity between a PPPoE enabled devices at the subscriber's site and a PPPoE aware Access Concentrator behind the Base Station. The frames are forwarded only between the Subscribers' PCs and the PPPoE Access Concentrator. Frames that are not PPPoE Ethertype are discarded. In the uplink, frames are never relayed

but only forwarded to the Access Concentrator. In the downlink, broadcasts are allowed only in cases of unknown addresses.

4.10.1.2.3 Voice Service

The Voice over IP (VoIP) service provides telephony services through an external Voice Gateway connected to the Subscriber Unit's data port. The VoIP service is designed for Alvarion's Voice Gateways, using the proprietary DRAP signaling protocol to identify VoIP sessions and to verify optimal handling of these sessions. Upon provisioning of such a service, the system automatically handles Signaling and RTP connections establishment, including QoS issues.



NOTE

The DRAP-based Voice Service is also available when an L2 Service is provisioned.

DRAP (Dynamic Resources Allocation Protocol) is a protocol between the Gateway (installed behind the Subscriber Unit) and the base station. The protocol provides an auto-discovery mechanism for the Gateway, so that no specific configuration is needed and the Gateway can automatically locate and register with the base station. The protocol uses a few simple messages enabling a Voice Gateway to request resources when calls are made, and the base station to dynamically allocate them.

Using the DRAP solution has the following advantages:

- Maintain telephony toll quality over the wireless network – dynamically allocate Continuous Grant (CG) connections for active calls, maintaining the QoS and low jitter needed for toll-quality voice services.
- Allocate CG bandwidth only for the duration of the call – the air resources are allocated and released according to the DRAP messages, which are based on the VoIP signaling. This dynamic allocation ensures efficient use of the air resources.
- Prevent callers from placing calls if a sector is overloaded – the operator can control and limit the maximum number of concurrent calls per wireless sector and per end user voice gateway. Thus, the operator has complete control of its network and the resources in it.
- Automatic support of Codec changing in a VoIP call – the DRAP messages update the BreezeMAX equipment on any Codec change or subsequent bandwidth allocation change during the call, hence the exact required bandwidth is always provided. This is essential in fax transmissions where the call might begin with one Codec and switch to another to accommodate the fax transmission.

- VoIP stack is always in synch with the wireless transport – as the DRAP is integrated into the VoIP stack all calls are terminated according to the VoIP standard. Even if no resources are available, the voice gateway receives an appropriate message from the BreezeMAX system and sends the required signaling message according to the VoIP standard used.

4.10.1.3 Supporting Generic (3rd Party) VoIP Services

When using VoIP devices that do not support the DRAP protocol, the required service can be provided through a Data (L2) service with a CG QoS (see [QoS Profiles](#) on page 166) that is defined in accordance with the estimated bandwidth required for the service. The required bandwidth depends on several parameters, such as codec type, sample rate and T.38 Fax Relay support. The service parameters depend also on the marking features of the VoIP equipment (the ability to use either DSCP or 802.1p to distinguish between RTP, RTCP and VoIP Signaling, and Data traffic).

The system includes several pre-configured Service Profiles for commonly used VoIP applications. For details on the pre-configured profiles, refer to [Pre-configured Profiles](#) on page 169. For details on defining Service Profiles for generic VoIP devices, refer to [Appendix E - Defining Service Profiles for Generic \(non-DRAP\) VoIP Gateways](#).

4.10.1.4 Advanced and Quick Service Modes

A BreezeMAX Base Station can operate in either Advanced or Quick Mode of service provisioning.

Advanced Mode enables operators to completely deny services to SUs that are not defined in the system. This increases the security of the system but complicates slightly the installation process as an SU must be defined in the system before it can be registered and receive any service.

Quick Mode is intended primarily for scenarios where the operator is not concerned with potentially “stolen” SUs, and wishes to provide basic services also to SUs that are not yet defined in the system. It may also be used as a temporary operation mode during SUs installation phase.

In both modes, defined services are provisioned to defined SUs. The difference between the two modes is in provisioning of services to SUs that are not defined in the system.

In Advanced Mode, an undefined SU that is authenticated by the system will be added to the database of the NPU (NMS) as Temporary. The database will include also its MAC address and the configured registration parameters. No services are provided as long as the SU is defined as Temporary. To receive services, the SU must be defined in the system. When it becomes a Permanent SU, the required services can be assigned to it.

In Quick Mode, an undefined SU that is authenticated by the system will be added to the database of the NPU (NMS) as Temporary. The subscriber will be able to use only services based on the Default Service Profile(s). When the SU is defined as Permanent and services are assigned to it, it will be able to use the defined services.

When changing the status of an SU from Permanent to Temporary, the SU must be reset to perform a new network entry process for getting the correct Default Service.

4.10.1.5 Using VLANs and VPLs

VLANs can be used for creating within the BreezeMAX network virtual groups of multiple end-users (stations) belonging to the same organization (Subscriber). They may also be used to differentiate between different end-users (stations) connected to the same SU.

In the current release, implementation of VLANs necessitates using a VLAN tagging device behind the relevant SUs.

The VLAN functionality of the SU differs from that of the NPU/ μ BST. The SU operates in transparent mode: If no VLAN ID is defined (the VLAN ID List is empty), frames with a VLAN ID tag will pass.

In the backbone, VPL ID (Virtual Private Link ID) is used. VPL is a virtual connection between two points on the network, such as a base station and a service provider or corporate network, identified by the VPL ID, with functionality that is similar to VLAN ID (VLAN on the backbone network). Typically, it is used to separate between different traffic types (e.g. Data and Voice), or traffic to/from different ISPs or different corporate networks.

If the VPL ID is None (No VPL ID), frames with a VLAN ID tag arriving from the downlink (the infrastructure side) will be discarded. Tagged frames arriving from the wireless domain will be forwarded without a VLAN tag, unless 802.1p Priority Marking is used. If 802.1p Priority Marking is used, tagged frames will be forwarded with VPL ID = 0 and the defined Priority Marking Value.

If the VPL ID is other than None, all frames forwarded to the network will be tagged with the VPL ID. The VLAN ID in tagged frames arriving from the wireless network will be replaced by the VPL ID.

The guidelines that should be followed when defining various parameters related to VLAN are:

- Several Service Profiles may share the same VPL ID. However, the following rules must be met:
 - ◇ Any number of L2 and/or VoIP Service Profiles may share the same VPL ID, provided they all use the same Forwarding Rule.

- ◇ Any number of PPPoE Service Profiles may share the same VPL ID, provided they all use the same Forwarding Rule.
- ◇ Any number of L2, VoIP and PPPoE Service Profiles may share the same VPL ID, provided that all L2/Voice Service Profiles use the same Forwarding Rule A, and all PPPoE Service Profiles use the same Forwarding Rule B, where A and B are different.
- A specific VLAN ID behind a certain SU can be associated only with a single Service of a certain Service Type. It is not possible to define two Services of the same Service Type for the same SU and VLAN ID. However, the same SU and VLAN ID can be associated with two Services of different Service Types, excluding the combination of L2 Service and Voice Service.
- The maximum number of VLAN IDs (behind the same SU) that can be associated with a single Service is 16. In the current version, a VLAN switch with VLAN Binding capability must be used to support more than one VLAN ID behind an SU. Otherwise, only a single VLAN ID can be used behind an SU, and this VLAN ID must equal the Multicast VLAN ID in the Forwarding Rule that is used in the applicable Service Profile(s).
- All Services associated with the same SU must use either VLAN ID(s) or No VLAN. It is not possible to define for the same SU one or more Services with VLAN ID(s) together with Service Profile(s) that are not associated with any VLAN.

4.10.2 Common Operations in Services Menu

Except for the General submenu, all submenus available in the Services menu enable viewing, editing, deleting and adding applicable entities, such as Subscribers, Services, Service Profiles, etc.

Some or all of the following options are available in all submenus of the Services menu:

4.10.2.1 Show All

Select this option to see the current details of all entities in the applicable submenu (Subscribers, Services, etc.).

4.10.2.2 Show by

This option enables selecting an entity by a specific identifier such as Name or MAC Address. Select this option and enter the appropriate parameter's value to access the menu for a selected entity. This will enable you to choose from the following options:

- **Show:** Select this option to view the details of the selected entity.
- **Update:** Select this option to edit the details of the selected entity.
- **Delete:** Select this option to remove the selected entity from the database.

4.10.2.3 Show List

Select this option to view all defined entities in the applicable submenu sorted by the entity type ID (Subscriber ID, Service ID, etc). The entity ID is an identifier attached automatically to each new entity. You can select a specific entity by its ID. This will open the Selected Entity menu with the Show, Update and Delete options described above.

4.10.2.4 Select

Select this option to select an entity by its Name. This will open the Selected Entity menu with the Show, Update and Delete options described above.

4.10.2.5 Add

Select this option to add a new entity to the database.

4.10.3 The Services Menu

The Services menu includes the following options:

- General
- Subscribers
- Service
- Service Profile
- Forwarding Rules
- Priority Classification
- QoS Profile

4.10.3.1 General

The General menu includes parameters that are common to all Subscribers. It includes the following options:

4.10.3.1.1 Show

Select this option to view the current values/options of the General parameters.

4.10.3.1.2 Update

Select this option to update any of the General parameters. The General parameters are:

4.10.3.1.2.1 Service Mode

The Service Mode of the base station.

The available options are:

1 – Advanced

2 – Quick

For more information on Service Modes refer to [Advanced and Quick Service Modes](#) on page 152.

The default Service Mode is Quick (2).

4.10.3.1.2.2 Default Data Service Profile

The default data Service Profile to be used by temporary SUs in Quick Mode.

Available profiles – any of the Data Service Profiles existing in the database.

4.10.3.1.2.3 Default VoIP Service Profile

The default Voice Service Profile to be used by temporary SUs in Quick Mode.

Available profiles – any of the Voice Service Profiles existing in the database.

4.10.3.2 Subscribers

The Subscribers menu enables defining new Subscribers, viewing or editing details of previously defined Subscribers and removing Subscribers from the database.

The configurable Subscriber's parameters are:

4.10.3.2.1 Subscriber Name

This is the name of the subscriber, which must be unique for the entire network.

A Subscriber Name consists of up to 32 printable characters.

4.10.3.2.2 First Name

An optional parameter for information purposes.

A First Name consists of up to 50 printable characters.

4.10.3.2.3 Last Name

An optional parameter for information purposes.

A Last Name consists of up to 50 printable characters.

4.10.3.2.4 Description

An optional parameter for information purposes.

A Description consists of up to 50 printable characters

4.10.3.2.5 Admin Status

The administrative status of the Subscriber can be either Enabled or Disabled. Select Disabled to disable all services to the Subscriber.

4.10.3.3 Services

Each Service defines the Service Profile for a specific Subscriber's station(s) behind a specific SU.

The Services menu enables defining new Services, viewing or editing details of previously defined Services and removing Services from the database.

The Services menu also enables viewing and resetting the Service counters.

4.10.3.3.1 Service Parameters

The Service's parameters are:

4.10.3.3.1.1 Name

A Service Name consists of up to 32 printable characters.

4.10.3.3.1.2 Subscriber Name

The Subscriber to which the Service is allocated.

The Subscriber Name must be one of the names that exist in the database after being defined using the Subscribers menu.

4.10.3.3.1.3 Service Profile Name

The Service Profile to be used in the Service.

The Service Profile Name must be one of the names that exist in the database after being defined using the Service Profile menu.

4.10.3.3.1.4 SU MAC Address

The MAC Address of the SU associated with the Service.

The SU MAC Address must be one of the addresses that exist in the database after being defined as a Permanent SU in the SU menu.

The MAC Address can be changed (in Update option) only if the Admin status of the Service is set to Disabled.

4.10.3.3.1.5 VLAN List

A list of VLAN IDs listing the VLAN IDs behind the SU associated with the applicable Subscriber.

The list includes VLAN IDs, each one in the range of 0 to 4094, separated by commas. Select null (empty string) for No VLAN. The VLAN List is not displayed in Show menus if the list is empty.

Refer to [Using VLANs](#) on page 154 for guidelines regarding VLAN ID configuration.

4.10.3.3.1.6 Admin Status

The administrative status of the Service can be either Enabled or Disabled. Select Disabled to disable the Service.

4.10.3.3.1.7 Operation Status

A read-only display of the operational status that is available in the Show menus only. Up means that the Service is currently in use.

4.10.3.3.2 Performance

The Performance sub-menu enables viewing and resetting the connections' counters of the Service. For each connection in each direction the following information is displayed:

- Connection ID and direction
- Bytes Submitted
- Bytes Transmitted
- Bytes Retransmitted
- Bytes Dropped
- Bytes Discarded
- Packets Submitted
- Packets Transmitted
- Packets Dropped
- Packets Discarded

- Average Delay (microseconds)
- Delay Variance (microseconds)
- Maximum Delay (microseconds)
- CIR Performance (%)
- Data Loss Indicator (%)
- MIR Performance (%)
- Average Throughput (bits/s)

4.10.3.4 Service Profile

Each Service Profile defines the properties of the defined service. Each Service Profile is associated with specific Forwarding Rule and Priority Classifier.

The Service Profile menu enables defining new Service Profiles, viewing or editing details of previously defined Service Profiles and removing Service Profiles from the database.

The configurable Service Profile's parameters are:

4.10.3.4.1 Service Profile Name

A Service Profile Name consists of up to 32 printable characters.

4.10.3.4.2 Service Type

The Service Type of the Service Profile. The Service Type parameter is configurable only when defining a new Service Profile (Add). It is not changeable.

The currently available Service Type options are:

- 1 – L2
- 2 – PPPoE
- 3 – Voice

For more details refer to [Service Types](#) on page 151.

4.10.3.4.3 VPL ID

A Virtual Private Link ID to be used in the backbone behind the Base Station.

Available values are in the range of 0 to 4094 or null (empty string) for No VPL ID. A value of 4095 is displayed for No VPL ID.

Refer to [Using VLANs](#) on page 154 for guidelines regarding VPL ID configuration.

4.10.3.4.4 Priority Marking Mode

In some cases, the network operator may want to use the BreezeMAX system for marking QoS classes, in order to provide network-wide QoS and enable the upstream network to handle the traffic accordingly. Within the BreezeMAX system, frames can be classified to QoS classes using Priority Classifiers, based on either a DSCP header or 802.1p tag. This applies only in cases where an external networking device marks the applicable fields. BreezeMax also enables marking data transmitted to the backbone network with either DSCP or 802.1p values, where the marking is done per Service Profile. This marking overrides marking performed by external devices behind the SU. Typically, Priority Marking by the NPU/μBST will be used in the following cases:

- The external networking equipment behind the SU does not use priority marking.
- The service provider does not trust the priority marking defined by the user's equipment.
- The service provider uses a priority marking type (DSCP or 802.1p) that differs from the one used by the user's networking equipment.

The system supports three marking modes:

- 1 **Transparent Marking Mode** (No Priority Marking): In this case, the system should forward the frames to the uplink network without any changes.

If 802.1p classification is used at the SU, the frames will be transmitted to the operator's network with their original 802.1p value and the configured VPL ID. If no VPL ID is configured (VPL ID = Null), the 802.1p tags will not be forwarded.

For DSCP classification at the SU, if the VPL ID is configured, the NPU/Micro Base Station adds an 802.1Q header with the configured VPL ID and 802.1p=0. Note that there may be a disparity between the DSCP values and the default 802.1p = 0 value.

- 2 **802.1p Marking Mode:** All frames are marked with the configured VPL ID and 802.1p Marking Value. If no VPL ID is configured (VPL ID = None), the 802.1Q header will include a VLAN ID = 0.

If 802.1p classification is used at the SU, the original 802.1p tags are replaced by the configured 802.1p Marking Value.

If DSCP classification is used at the SU, an 802.1Q header is added, with the configured VPL ID and 802.1p Marking Value, and the original DSCP bits are kept.

3 DSCP Marking Mode: All frames are marked with the configured DSCP Marking Values.

If 802.1p classification is used at the SU, the frames will be transmitted to the operator's network with their original 802.1p value and the configured VPL ID. If no VPL ID is configured (VPL ID = Null), the original 802.1p tags will not be forwarded.

If DSCP classification is used at the SU, the original DSCP bits will be replaced by the configured DSCP Marking Value.

NOTE



- PPPoE frames can be marked only with 802.1p. DSCP marking for PPPoE services is not supported.
- In L2 Services, many protocols may be carried over Ethernet. As BreezeMAX bridges all these protocols, there's no way to know what protocol type is encapsulated in Ethernet beforehand. Consequently, if DSCP Marking is configured for L2, the BreezeMAX system uses DSCP marking only for IP packets (e.g. Ethertype 0x0800). If 802.1p Marking is configured, it is used for all frames.

4.10.3.4.5 Priority Marking Value

The Priority Marking Value enables definition of the marking value for data frames transmitted to the backbone, according to the configured Priority Marking Mode:

Table 4-6: Priority Marking Values	
Priority Marking Mode	Priority Marking Values Range
Transparent	Not Applicable
802.1p	0 - 7
DSCP	0 - 63

4.10.3.4.6 Forwarding Rule

The Forwarding Rule to be used by the Service Profile.

The Forwarding Rule must be one of the names that exist in the database after being defined using the Forwarding Rule menu. The Service Type defined in the selected Forwarding Rule must match the one defined for the Service Profile.

4.10.3.4.7 Priority Classifier (L2 and PPPoE Service Type)

The Priority Classifier to be used by the Service Profile. Not applicable for Voice Services.

The Priority Classifier must be one of the names that exist in the database, after being defined using the Priority Classifier menu.

4.10.3.4.8 Maximum Number of Voice Calls (L2 and Voice Service Type)

The Maximum Number of Voice Calls parameter sets the upper limit on the number of simultaneous VoIP calls that can be supported by the Service using the Service Profile. This parameter is applicable only for L2 and Voice Service Profiles.

The available range is from 0 to 10 calls.



NOTE

To properly support Call Waiting, the Maximum Number of Voice Calls should be configured to a value that is twice the number of actual voice sessions that can be supported simultaneously.

4.10.3.5 Forwarding Rule

The Forwarding Rule defines the features that affect forwarding and switching of data. Data in L2 and Voice services may be switched only between the Services that share the same Forwarding Rule. Data in PPPoE service can pass only between the subscriber and an Access Concentrator behind the Base Station.

The Forwarding Rule menu enables defining new Forwarding Rules, viewing or editing details of previously defined Forwarding Rules and removing Forwarding Rules from the database.

The configurable Forwarding Rule's parameters are:

4.10.3.5.1 Forwarding Rule Name

A Forwarding Rule Name consists of up to 32 printable characters.

4.10.3.5.2 Service Type

The Service Type for which the Forwarding Rule is defined. The Service Type parameter is configurable only when defining a new Service Profile (Add). It is not changeable.

The currently available Service Type options are:

- 1 – L2
- 2 – PPPoE
- 3 – Voice

For more details refer to [Service Types](#) on page 151.

4.10.3.5.3 Unicast Relaying (L2 and Voice Service Type)

The Unicast Relaying parameter determines whether the AU 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.

4.10.3.5.4 Broadcast Relaying (L2 and Voice Service Type)

The Broadcast Relaying parameter determines whether the AU 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 backbone. If disabled, these packets are sent only to the backbone and are not sent back to the wireless link.

4.10.3.5.5 Unknown Forwarding Policy (L2 and Voice Services Type)

The Unknown Forwarding Policy parameter determines the mode of controlling the flow of information from the backbone to the wireless media. Select from the following options:

- 1 – Reject: The AU will transmit packets only to those addresses that the AU knows to exist on the wireless link side.
- 2 – Forward: Enables the transmission of all packets, except those sent to addresses that the AU recognizes as being on its wired backbone side.

4.10.3.5.6 Multicast VLAN ID

The VLAN ID to be attached to multicast messages in order to enable full support of the VLAN feature.

Available values are in the range of 0 to 4094 or null (empty string) for No Multicast VLAN ID.

Refer to [Using VLANs](#) on page 154 for guidelines regarding configuration of Multicast VLAN ID.

4.10.3.5.7 Multicast QoS Profile

The QoS Profile to be used for multicast and broadcast messages.

The QoS Profile must be one of the names that exist in the database after being defined using the QoS Profile menu.

4.10.3.6 Priority Classifier (L2 and PPPoE Service Type)

The Priority Classifier defines the QoS Profiles to be allocated to users/sessions differentiated by DSCP or 802.1p priority classifiers. Priority Classifiers are not applicable to Voice Service Profiles.

Each Priority Classifier can define up to 4 uplink and 4 downlink QoS profiles.

**NOTE**

DSCP based Priority Classifiers are applicable only to IP or ARP traffic. It is not applicable to PPPoE and other Ethernet type traffic.

If a Priority Classifier is not applicable for a certain traffic (e.g. DSCP based profile with PPPoE traffic or 802.1p based profile with traffic that do not use VLAN tags), no prioritization scheme will be in effect and quality of service will be determined by the first QoS Profile in the applicable lists.

The Priority Classifier menu enables defining new Priority Classifiers, viewing or editing details of previously defined Priority Classifiers and removing Priority Classifiers from the database.

The configurable Priority Classifier's parameters are:

4.10.3.6.1 Priority Classifier Name

A Priority Classifier Name consists of up to 32 printable characters.

4.10.3.6.2 Priority Type

The prioritization mechanism used by the Priority Classifier.

The available options are:

1 – DSCP

2 – 802.1p

4.10.3.6.3 Uplink Upper Priority Limits

The Uplink Upper Priority Limits parameter enables to define up to four ranges, where each range may be assigned a different QoS Profile for uplink communication. The list includes up to 4 numbers separated by commas, where each number must be higher than its predecessor and the last number must be the highest available for the applicable priority type (7 for 802.1p, 63 for DSCP).

Examples for acceptable lists:

DSCP Priority: [10,30,50,63]; [21,42,63]; [20,63]; [63].

802.1p Priority: [2,4,6,7]; [1,5,7]; [6,7]; [7].

A ranges list of 21,42,63 means that packets with a priority from 0 to 21 will be transmitted using the first QoS Profile defined in the Uplink QoS Profiles list (see below), packets with a priority from 22 to 42 will be transmitted using the second QoS Profile defined in the Uplink QoS Profiles list and packets with a priority higher than 42 (43-63) will be transmitted using the third Uplink QoS Profile.

A ranges list that includes a single entry (63 for DSCP and 7 for 802.1p) means that priority based classification is not used.

4.10.3.6.4 Uplink QoS Profiles

The Uplink QoS Profiles parameter enables to define up to four QoS Profiles, where each entry is the QoS Profile associated with the applicable entry in the Uplink Upper Priority Limits list. The list includes up to four QoS Profile Names, where each name must be one of the names that exist in the database after being defined using the QoS Profile menu. Each entry in the Uplink QoS Profiles list is associated with the applicable entry in the Uplink Priority Ranges list.

4.10.3.6.5 Downlink Upper Priority Limits

The DownLink Upper Priority Limits list functionality is the same as that of the Uplink Upper Priority Limits list, except that the ranges are defined for downlink communication.

4.10.3.6.6 Downlink QoS Profiles

The Downlink QoS Profiles list functionality is the same as that of the Uplink QoS Profiles list, except that the QoS Profiles are associated with the entries in the Downlink Upper Priority Limits list.

4.10.3.7 QoS Profile

The QoS Profile defines the Quality of Service parameters that are applicable when the QoS Profile is used.

Different QoS Profile Types are available to support different service requirements:

- **Real-Time (RT):** The Real-Time polling service is designed to meet the needs of Real Time Variable Bit Rate like services characterized by requirements for guaranteed rate and delay such as streaming video or audio. These services are dynamic in nature, but offer periodic dedicated requests opportunities to meet real-time requirements. Because the Subscriber Unit issues explicit requests, the protocol overhead and latency is increased, but capacity is granted only according to the real needs of the connection. QoS Profile parameters include Committed Information Rate (CIR) and Committed Time (CT).
- **Non-Real-Time (NRT):** Non-Real-Time polling service is very similar to the Real-Time polling service except that connections may utilize random access transmit opportunities for sending bandwidth requests. These Non Real Time Variable Bit Rate services, such as file transfer and Internet access with a minimum guaranteed rate, are characterized by requirement for a guaranteed rate, but can tolerate longer delays and are rather insensitive to jitter. QoS Profile parameters include Committed Information Rate (CIR), Committed Time (CT) and Maximum Information Rate (MIR) that limits the rate so that bandwidth_intensive services will not expand to occupy the full bandwidth.

- **Best Effort (BE)** service is for services where neither throughput nor delay guarantees are provided. The Subscriber Unit sends requests for bandwidth in either random access slots or dedicated transmission opportunities. The occurrence of dedicated opportunities is subject to network load, and the Subscriber Unit cannot rely on their presence. Service parameters include Committed Time (CT) and Maximum Information Rate (MIR).
- **Continuous Grant (CG)** service is tailored for carrying constant bit-rate (CBR) real-time services characterized by fixed size data packets on a periodic basis such as VoIP or E1/T1. The Base Station schedules regularly, in a preemptive manner, grants of the size defined at connection setup, without an explicit request from the Subscriber Unit. This eliminates the overhead and latency of bandwidth requests in order to meet the delay and jitter requirements of the underlying service. Service parameters include Packet Size (unsolicited grant size) and Sampling Rate (grant interval).

The QoS Profile menu enables defining new QoS Profiles, viewing or editing details of previously defined QoS Profiles and removing QoS Profiles from the database.

The available QoS Profile parameters depend on the QoS Type. The configurable QoS Profile's parameters are:

4.10.3.7.1 QoS Profile Name

A QoS Profile Name consists of up to 32 printable characters.

4.10.3.7.2 QoS Type

The QoS Type that defines the QoS parameters that are applicable to the service. The available options are:

- 1 – CG (Continuous Grant)
- 2 – RT (Real Time)
- 3 – NRT (Non real time)
- 4 – BE (Best Effort)

4.10.3.7.3 CT (RT, NRT and BE QoS Types)

The CT (Committed Time) parameter defines the time window over which the information rate is averaged to ensure compliance with the CIR or MIR parameter.

The available options are:

- 1 – Short
- 2 – Medium

3 – Long

The actual value in milliseconds for each of the three options varies according to the QoS type.

Table 4-7: CT values			
CT	BE	NRT	RT
Short	50mS	50mS	50mS
Medium	100mS	100mS	100mS
Long	1sec	1Sec	200mS

4.10.3.7.4 CIR (RT and NRT QoS Types)

CIR is the information transfer rate that the system is committed to transfer under normal conditions. The rate is averaged over a minimum increment of time, which is defined by the CT parameter.

The range is from 0 to 12,000 Kbps.

4.10.3.7.5 MIR (NRT and BE QoS Types)

MIR is the maximum information rate that the system will allow for the connection. The rate is averaged over a minimum increment of time, which is defined by the CT parameter.

The range is from 1 to 12,000 Kbps.

MIR cannot be lower than CIR (applicable to NRT QoS type).

4.10.3.7.6 Packet Size (CG QoS Type)

The Packet Size parameter defines the amount of data in Bytes that is expected for each grant.

4.10.3.7.7 Sampling Rate (CG QoS Type)

The Sampling Rate parameter defines the time in milliseconds between two successive grants (inter arrival time).

NOTE

Packet Size (in bits) x Sampling Rate (in seconds) should not exceed 12 Mbps.



4.10.4 Defining Services

The process of defining completely new Services should be done “from bottom up”, as each entity in the process is defined using one or more “lower level” entities.



To define a new Service “from scratch”:

- 1 Define the QoS profiles that should be available for the required Priority Classifiers (Uplink/Downlink QoS Profiles) and for the required Forwarding Rules (Multicast QoS Profile).
- 2 Define the Priority Classifiers that should be available for the required Service Profiles. All QoS Profiles required for the Uplink/Downlink QoS profiles list must be defined in advance.
- 3 Define the Forwarding Rules that should be available for the required Service Profiles. The QoS Profiles required for the Multicast QoS Profile parameter must be defined in advance.
- 4 Define the Service Profiles that should be available for the required Services. All required Priority Classifiers and Forwarding Rules must be defined in advance.
- 5 Define the relevant Subscribers.
- 6 Verify that all applicable SUs are defined.
- 7 Use existing Subscriber Name, SU MAC Address and Service Profile Name to define the required Service.

Once there are various QoS Profiles, Priority Classifiers, Forwarding Rules, Service Profiles, Subscribers and SUs in the database, you can skip one or more of the steps 1 to 6.

4.10.5 Pre-configured Profiles

At manufacturing stage, each NPU is configured with a set of pre-configured Profiles. Certain parameters of these Profiles may be modified to reflect specific implementation requirements. When the software version is upgraded, these pre-configured Profiles will not be installed again in the NPU. This is to prevent configuration problems from occurring if the modified Profiles differ from the factory loaded Profiles.

Note that upon resetting to NPU/μBST to its default configuration (Set Factory Defaults), pre-configured Profiles that were modified are not affected.

The pre-configured Service Profiles are:

- **Basic L2 Internet Access** – for basic Internet Access service with Best Effort QoS, utilizing L2 Service Type. This is the recommended Default Service Profile for Quick Mode.
- **Basic PPPoE Internet Access** - for basic Internet Access service with Best Effort QoS, utilizing PPPoE Service Type.
- **Gold, Silver and Bronze Teleworking** – for teleworking applications with different QoS requirements. The pre-configured Teleworking Services are asymmetric: DL Rate > UL Rate.
- **Gold, Silver and Bronze LAN-to-LAN** – for LAN-to LAN applications with different QoS requirements. The pre-configured LAN-to-LAN Services are symmetric: DL rate = UL rate.
- **VoIP Service Profiles** – for DRAP-based gateways. Two pre-configured VoIP service Profiles are defined; VoIP 1V for gateways with a single POTS interface, and VoIP 2V for fully supporting gateways for 2 POTS interfaces.
- **Service Profiles for Generic (non-DRAP) VoIP Devices:**
 - ◇ 1 POTS Basic VoIP G.729: 1 POTS, no Fax, G.729 codec with a 20 milliseconds sample interval, no priority marking.
 - ◇ 1 POTS Advanced VoIP G.729: 1 POTS, T.38 Fax, G.729 codec with a 20 milliseconds sample interval, DSCP priority marking.
 - ◇ 1 POTS Basic VoIP G.711: 1 POTS, no Fax, G.711 codec with a 20 milliseconds sample interval, no priority marking.
 - ◇ 1 POTS Advanced VoIP G.711: 1 POTS, T.38 Fax, G.729 codec with a 20 milliseconds sample interval, DSCP priority marking.

For more details of defining Service Profiles for Generic (3rd party) VoIP devices, refer to [Appendix E - Defining Service Profiles for Generic \(non-DRAP\) VoIP Gateways](#).

Except for the Basic PPPoE Internet Access pre-configured Service Profiles, all pre-configured Data Service Profiles use L2 Service Type to ensure transport of all L2 and L3 protocol.

It is recommended to use the L2 Best Effort Internet Access pre-configured Service Profile as the Default Data Service Profile in Quick Mode.

The following tables provide details on the pre-configured Service Profiles, Forwarding Rules, Priority Classifiers and QoS Profiles.

Table 4-8: Pre-Configured Data Service Profiles				
Name	Service Type	VPL ID*	Forwarding Rule	Priority Classifier
Internet Access L2	L2	Null	Internet Access L2	BE Asymmetric
Internet Access PPPoE	PPPoE	11	Internet Access PPPoE	BE Asymmetric
Gold Teleworking	L2	12	Gold Teleworking	Gold Asymmetric
Silver Teleworking	L2	13	Silver Teleworking	Silver Asymmetric
Bronze Teleworking	L2	14	Bronze Teleworking	Bronze Asymmetric
Gold LAN-to-LAN	L2	15	Gold LAN-to-LAN	Gold Symmetric
Silver LAN-to-LAN	L2	16	Silver LAN-to-LAN	Silver Symmetric
Bronze LAN-to-LAN	L2	17	Bronze LAN-to-LAN	Bronze Symmetric

In all pre-configured Data Service Profiles, the **Priority Marking Mode** is set to Transparent and the **Maximum Number of Voice Calls** is 0.

* VPL IDs are assigned arbitrary values and should be configured in accordance with specific network implementation, taking into account the considerations described in [Using VLANs](#) on page 154.

As Internet Access L2 is the recommended Default Data Service Profile, a VPL ID = None is used to ensure availability of basic data services in Quick Mode.

Table 4-9: Pre-Configured Forwarding Rules for Data Service						
Name	Service Type	Unicast relaying	Broadcast Relaying	Unknown forwarding Policy	Multicast QoS	Multicast VLAN*
Internet Access L2	L2	Disable	Disable	Forward	BE 750	Null
Internet Access PPPoE	PPPoE	Disable (hard coded)	Disable (hard coded)	Forward (hard coded)	BE 750	Null
Gold Teleworking	L2	Disable	Disable	Forward	NRT 1500/1750	Null
Silver Teleworking	L2	Disable	Disable	Forward	NRT 1000/1150	Null
Bronze Teleworking	L2	Disable	Disable	Forward	NRT 750/850	Null
Gold LAN-to-LAN	L2	Enable	Enable	Forward	NRT 1500/1750	Null
Silver LAN-to-LAN	L2	Enable	Enable	Forward	NRT 1000/1150	Null
Bronze LAN-to-LAN	L2	Enable	Enable	Forward	NRT 750/850	Null

* Multicast VLANs are assigned arbitrary values and should be configured in accordance with specific network implementation, taking into account the considerations described in [Using VLANs](#) on page 154.

Table 4-10: Pre-Configured Priority Classifiers for Data Services

Name	Type	Uplink Priority ranges	Uplink QoS Profiles	Downlink Priority ranges	Downlink QoS Profiles
BE Asymmetric	802.1p	7	BE 96	7	BE 750
Gold Asymmetric	802.1p	7	NRT 128/192	7	NRT 1500/1750
Silver Asymmetric	802.1p	7	NRT 96/128	7	NRT 1000/1150
Bronze Asymmetric	802.1p	7	NRT 96/128	7	NRT 750/850
Gold Symmetric	802.1p	7	NRT 1500/1750	7	NRT 1500/1750
Silver Symmetric	802.1p	7	NRT 1000/1150	7	NRT 1000/1150
Bronze Symmetric	802.1p	7	NRT 750/850	7	NRT 750/850

Table 4-11: Pre-Configured QoS Profiles for Data Services

Name	Type	CIR (Kbps)	MIR (Kbps)	CT
BE 96	Best Effort	NA	96	Medium
BE 750	Best Effort	NA	750	Medium
NRT 96/128	Non Real Time	96	128	Medium
NRT 128/192	Non Real Time	128	192	Medium
NRT 750/850	Non Real Time	750	850	Medium
NRT 1000/1150	Non Real Time	1000	1150	Medium
NRT 1500/1750	Non Real Time	1500	1750	Medium

Table 4-12: Pre-Configured Voice Service Profiles (for DRAP-based Gateways)					
Name	Service Type	VPL ID*	Priority Marking Mode	Maximum Number of Voice Calls**	Forwarding Rule
VoIP 1V	Voice	18	Transparent	2	VoIP
VoIP 2V	Voice	18	Transparent	4	VoIP

* VPL IDs are assigned arbitrary values and should be configured in accordance with specific network implementation, taking into account the considerations described in [Using VLANs](#) on page 154.

** To properly support Call Waiting, an additional connection must be available. Thus, the Maximum Number of Voice Calls is twice the maximum expected number of actual voice sessions.

Table 4-13: Pre-Configured Service Profiles for Generic (non-DRAP) VoIP Services				
Name	Service Type	VPL ID*	Forwarding Rule	Priority Classifier
1 POTS Basic VoIP G.729	L2	19	VoIP	1 POTS Basic VoIP G.729
1 POTS Advanced VoIP G.729	L2	19	VoIP	1 POTS Advanced VoIP G.729
1 POTS Basic VoIP G.711	L2	19	VoIP	1 POTS Basic VoIP G.711
1 POTS Advanced VoIP G.711	L2	19	VoIP	1 POTS Advanced VoIP G.711

In all pre-configured Service Profiles for generic VoIP services, the **Priority Marking Mode** is set to Transparent and the **Maximum Number of Voice Calls** is 0.

* VPL IDs are assigned arbitrary values and should be configured in accordance with specific network implementation, taking into account the considerations described in [Using VLANs](#) on page 154.

Table 4-14: Pre-Configured Forwarding Rule for Voice Services						
Name	Service Type	Unicast Relaying	Broadcast Relaying	Unknown forwarding Policy	Multicast QoS	Multicast VLAN*
VoIP	Voice	Enable (hard coded)	Enable (hard coded)	Forward (hard coded)	BE 128	Null

* Multicast VLANs are assigned arbitrary values and should be configured in accordance with specific network implementation, taking into account the considerations described in [Using VLANs](#) on page 154.

All pre-configured Service profiles for VoIP (DRAP-based Voice Services and Generic (3rd party) VoIP Services share the same pre-configured Forwarding Rule, to enable direct communication between all users of VoIP Services, regardless of the gateway type and other possible differences in the Service Profiles.

Table 4-15: Pre-Configured Priority Classifiers for Generic (non-DRAP) VoIP Services					
Name	Type	Uplink Priority Ranges	Uplink QoS Profiles	Downlink Priority Ranges	Downlink QoS Profiles
1 POTS Basic VoIP G.729	DSCP	63	CG 47	63	CG 47
1 POTS Advanced VoIP G.729	DSCP	0	BE 64	0	BE 64
		26	RT 6	26	RT 6
		63	CG 38	63	CG 38
1 POTS Basic VoIP G.711	DSCP	63	CG 108	63	CG 108
1 POTS Advanced VoIP G.711	DSCP	0	BE 64	0	BE 64
		26	RT 11	26	RT 11
		63	CG 88	63	CG 88

Table 4-16: Pre-Configured BE and RT QoS Profile for Voice Services

Name	Type	CIR (Kbps)	MIR (Kbps)	CT
BE 64	Best Effort	NA	64	Medium
BE 128	Best Effort	NA	128	Medium
RT 6	Real Time	6	NA	Short
RT 11	Real Time	11	NA	Short

Table 4-17: Pre-Configured CG QoS Profile for Generic (non-DRAP) VoIP Services

Name	Type	Packet Size (Bytes)	Sample Interval (msec)
CG 38	Continuous Grant	94	20
CG 47	Continuous Grant	117	20
CG 88	Continuous Grant	218	20
CG 108	Continuous Grant	270	20

4.11 NPU/Micro Base Station Parameters Summary

Table 4-18: NPU/μBST Monitor Parameters Summary			
Parameter	Range	Default	Run-Time Updated
Base Station/μBST Configuration Parameters			
Device Name	Up to 256 printable characters	Null	Yes
Device Location	Up to 256 printable characters	Null	Yes
Base Station/μBST Alarms and Traps			
Minimum Severity	1 – Critical 2 – Major 3 – Minor 4 – Warning 5 – Info	Info	Yes
Days	1 – 31 days	31 days	Yes
Traps Group Enable/Disable	Per Group (A, B): 1 – Disable 2 – Enable	Group A: Enable Group B: Enable	Yes
NPU/μBST Parameters			
Password	Up to 16 printable characters, case sensitive	admin	Yes
Monitor Inactivity Timeout	1 – 60 minutes	10 minutes	Yes
Management Port IP Address	IP address	10.0.0.1	No
Management Port Subnet Mask	IP address	255.255.255.0	No

Table 4-18: NPU/μBST Monitor Parameters Summary

Parameter	Range	Default	Run-Time Updated
Management Port Gateway	IP address	0.0.0.0	No
Management Port Destination Subnet	IP address	0.0.0.0	No
Management Port Destination Subnet Mask	IP address	0.0.0.0	No
Management Port Auto negotiation Option (μBST)	1 – Disable 2 – Enable	Enable	No
Management Port Speed and Duplex (μBST)	1 – 10 Mbps Half Duplex 2 – 10 Mbps Full duplex 3 – 100 Mbps Half Duplex 4 – 100 Mbps Full Duplex		No
Management Port Management Traffic Enable/Disable	1 – Disable 2 – Enable	Enable	No
Data Port IP Address	IP address	1.1.1.3	No
Data Port Subnet Mask	IP address	255.255.255.0	No
Data Port Gateway	IP address	0.0.0.0	No
Data Port Management VLAN ID	0-4094 or Null for No VLAN	Null	No
Data Port Speed (NPU)	1 – 100 Mbps 2 – 1 Gbps	100 Mbps	No

Table 4-18: NPU/μBST Monitor Parameters Summary			
Parameter	Range	Default	Run-Time Updated
Data Port Auto Negotiation Option (μBST)	1 – Disable 2 – Enable	Enable	No
Data Port Speed and Duplex (μBST)	1 – 10 Mbps Half Duplex 2 – 10 Mbps Full duplex 3 – 100 Mbps Half Duplex 4 – 100 Mbps Full Duplex		No
Data Port Management Traffic Enable/Disable	1 – Disable 2 – Enable	Enable	No
Authorized Manager IP Address	IP address	NA	Yes
Authorized Manager Send Traps	1 – Disable 2 – Enable	NA	Yes
Authorized Manager Read Community	Up to 23 printable characters, case sensitive	NA	Yes
Authorized Manager Write Community	Up to 23 printable characters, case sensitive	NA	Yes
Bridge Aging Time	1 – 1440 minutes	10 minutes	Yes
AU/μBST MAC Parameters			
Base Station ID	X.X.X.X.X.X X: 0-255	186.190.0.0.0.0	No
ARQ Enable/Disable	1 – Disable 2 – Enable	Disable	No

Table 4-18: NPU/μBST Monitor Parameters Summary			
Parameter	Range	Default	Run-Time Updated
Maximum Cell Radius (km)	10 –100 km using 10 km steps	20 km	No
AU/μBST Phy Parameters			
Bandwidth (MHz)	1 – 1.75 2 – 3.5	3.5	No
Downlink (Tx) Frequency (MHz)	For Band 3.5a and a Bandwidth of 3.5 MHz: 3501.25 to 3551.75 in increments of 0.125 MHz. For Band 3.5a and a Bandwidth of 1.75 MHz: 3500.375 to 3552.625 in increments of 0.125 MHz. For Band 3.5b and a Bandwidth of 3.5 MHz: 3551.75 to 3598.25 in increments of 0.125 MHz. For Band 3.5b and a Bandwidth of 1.75 MHz: 3550.875 to 3599.125 in increments of 0.125 MHz.	3551.75	No
Tx Power (dBm)	13 – 28 (dBm, in increments of 0.25 dBm)	28	Yes
AU/μBST Multirate Parameters			
Multirate Enable/Disable	1 – Disable 2 – Enable Disable is temporary until next reset	Enable	Yes

Table 4-18: NPU/μBST Monitor Parameters Summary			
Parameter	Range	Default	Run-Time Updated
Uplink Basic Rate	1 – BPSK 1/2 2 – BPSK 3/4 3 – QPSK 1/2 4 – QPSK 3/4 5 – QAM16 1/2 6 – QAM16 3/4 7 – QAM64 2/3 8 – QAM64 3/4	BPSK 1/2	Yes
Downlink Basic Rate	1 – BPSK 1/2 2 – BPSK 3/4 3 – QPSK 1/2 4 – QPSK 3/4 5 – QAM16 1/2 6 – QAM16 3/4 7 – QAM64 2/3 8 – QAM64 3/4	BPSK 1/2	Yes
AU/μBST ATPC Parameters			
ATPC Enable/Disable	1 – Disable 2 – Enable Disable is temporary until next reset	Enable	Yes
Optimal Uplink RSSI (dBm)	-103 to -50	-69	Yes
AU/μBST Voice Parameters			
Maximum Number of Voice Calls	0 – 300	50	Yes

Table 4-18: NPU/ μ BST Monitor Parameters Summary			
Parameter	Range	Default	Run-Time Updated
AU/μBST BER Test Parameters			
SU MAC Address	MAC address	NA	Yes
Number of Bytes	1,000 – 100,000,000	NA	Yes
Rate	1 – BPSK 1/2 2 – BPSK 3/4 3 – QPSK 1/2 4 – QPSK 3/4 5 – QAM16 1/2 6 – QAM16 3/4 7 – QAM64 2/3 8 – QAM64 3/4	NA	Yes
Burst Size	500 – 4000 Bytes	NA	Yes
Test Priority	1 – RT 2 – NRT 3 – BE	NA	Yes
SU Control Parameters			
SU Status	1 – Permanent 2 – Temporary	Permanent	Yes
SU Registration Parameters			
Name	Read-only		NA
Organization Name	Read-only		NA
Address	Read-only		NA
Country Code	Read-only		NA

Table 4-18: NPU/μBST Monitor Parameters Summary			
Parameter	Range	Default	Run-Time Updated
SU MAC Parameters			
Base Station ID	X.X.X.X.X.X X: 0 – 255		No
Base Station ID Mask	X.X.X.X.X.X X: 0 – 255		No
SU Phy Parameters			
Bandwidth (MHz)	1 – 1.75 2 – 3.5		No
Uplink (Tx) Frequency (MHz)	BW 3.5 MHz: 3401.25 to 3498.25 BW 1.75 MHz: 3400.375 to 3499.125 Resolution: increments of 0.125 MHz		No
SU Multirate and ATPC Parameters			
Uplink Rate	Applicable only if Multirate in AU is disabled: 1 – BPSK 1/2 2 – BPSK 3/4 3 – QPSK 1/2 4 – QPSK 3/4 5 – QAM16 1/2 6 – QAM16 3/4 7 – QAM64 2/3 8 – QAM64 3/4	New SU: Uplink Basic Rate. Connected SU: Last used rate.	Yes

Table 4-18: NPU/μBST Monitor Parameters Summary			
Parameter	Range	Default	Run-Time Updated
SU Ethernet Port Parameters			
Ethernet Port Configuration	1 – 10 Mbps Half Duplex 2 – 10 Mbps Full duplex 3 – 100 Mbps Half Duplex 4 – 100 Mbps Full Duplex 5 – Auto Negotiation	Auto Negotiation	No
SU Password			
Password	Up to 20 printable characters, case sensitive	installer	Yes
SU Bridging Parameters			
Enable/Disable Limit on Number of Supported Devices	1 – Disable 2 – Enable	Disable	Yes
Maximum Number of Supported Devices	1 – 512	512	Yes
Bridge Aging Time	1 – 1440 minutes	3 minutes	Yes
Service General Parameters			
Service Mode	1 – Advanced 2 – Quick	Quick	Yes
Default Data Service Profile	Name of an existing profile or None.	Internet Access L2	Yes
Default Voice Service Profile	Name of an existing profile or None.	None	Yes

Table 4-18: NPU/μBST Monitor Parameters Summary			
Parameter	Range	Default	Run-Time Updated
Service Subscribers Parameters			
Subscriber Name	Up to 32 printable characters. Must be unique in the network.		Yes
First Name	Up to 50 printable characters.		Yes
Last Name	Up to 50 printable characters.		Yes
Description	Up to 50 printable characters.		Yes
Admin Status	1 – Disabled 2 – Enabled		Yes
Service Parameters			
Service Name	Up to 32 printable characters.		Yes
Subscriber Name	A Subscriber Name (up to 32 printable characters) that exists in the database		Yes
SU MAC Address	MAC Address of an SU that exists in the database		Yes
Service Profile Name	A Service Profile Name (up to 32 printable characters) that exists in the database		Yes
VLAN List	A list of different numbers separated by commas where each entry is from 1 to 4094. Null is for No VLAN.		Yes
Admin Status	1 – Disabled 2 – Enabled		Yes

Table 4-18: NPU/μBST Monitor Parameters Summary			
Parameter	Range	Default	Run-Time Updated
Service Profile Parameters			
Service Profile Name	Up to 32 printable characters.		Yes
Service Type	Applicable only for new Service Profiles (Add): 1 – L2 2 – PPPoE 3 - Voice		Yes
VPL ID	0 – 4094 or null for No VPL ID.		Yes
Priority Marking Mode	1 – Transparent 2 – 802.1p 3 - DSCP		
Priority Marking Value	802.1p: 0 – 7 DSCP: 0 - 63		
Forwarding Rule	A Forwarding Rule Name (up to 32 printable characters) that exists in the database		Yes
Priority Classifier	A Priority Classifier Name (up to 32 printable characters) that exists in the database		Yes
Maximum Number of Voice Calls	0 – 10		Yes
Forwarding Rule Parameters			
Forwarding Rule Name	Up to 32 printable characters		Yes

Table 4-18: NPU/μBST Monitor Parameters Summary			
Parameter	Range	Default	Run-Time Updated
Service Type	Applicable only for new Service Profiles (Add): 1 – L2 2 – PPPoE		Yes
Unicast Relaying	Applicable only for L2 Service type: 1 – Disabled 2 – Enabled		Yes
Broadcast Relaying	Applicable only for L2 Service type: 1 – Disabled 2 – Enabled		Yes
Unknown Forwarding Policy	Applicable only for L2 Service type: 1 – Reject 2 – Forward		Yes
Multicast VLAN ID	0 – 4094 or null for No Multicast VLAN.		Yes
Multicast QoS Profile	A QoS Profile Name (up to 32 printable characters) that exists in the database		Yes
Priority Classifier Parameters			
Priority Classifier Name	Up to 32 printable characters		Yes
Priority Type	1 – DSCP 2 – 802.1p		Yes

Table 4-18: NPU/μBST Monitor Parameters Summary

Parameter	Range	Default	Run-Time Updated
Uplink Priority Ranges	Up to 4 numbers separated by commas, where each number must be higher than its predecessor and the last number must be the highest available for the applicable priority type (7 for 802.1p, 63 for DSCP).		Yes
Uplink QoS Profiles	Up to four QoS Profile Names separated by commas, where each name (up to 32 printable characters) is a name of a QoS Profile that exists in the database. The number of entries in the list must be identical to number of entries in Uplink Priority Ranges list.		Yes
Downlink Priority Ranges	Up to 4 numbers separated by commas, where each number must be higher than its predecessor and the last number must be the highest available for the applicable priority type (7 for 802.1p, 63 for DSCP).		Yes
Downlink QoS Profiles	Up to four QoS Profile Names separated by commas, where each name (up to 32 printable characters) is a name of a QoS Profile that exists in the database. The number of entries in the list must be identical to number of entries in Downlink Priority Ranges list.		Yes

Table 4-18: NPU/μBST Monitor Parameters Summary			
Parameter	Range	Default	Run-Time Updated
QoS Profile Parameters			
QoS Profile Name	Up to 32 printable characters		Yes
QoS Type	2 – RT 3 – NRT 4 – BE		Yes
CT	1 – Short 2 – Medium 3 – Long		Yes
CIR (Kbps)	Applicable to RT and NRT: 0 – 12,000		Yes
MIR (Kbps)	Applicable to NRT and BE: 1 – 12,000. MIR cannot be lower than CIR (NRT)		Yes
Packet Size (Bytes)	Applicable to CG		Yes
Sample Interval (msec)	Applicable to CG		Yes



A

Appendix A - Preparing the SU IDU-ODU Cable



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

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

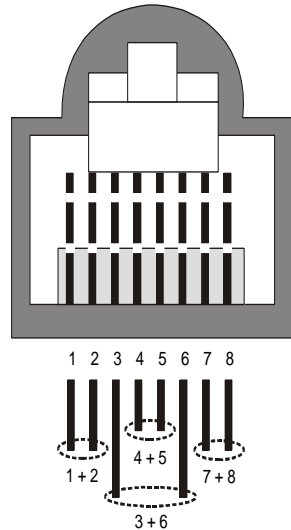


Figure A-1: Ethernet Connector Pin Assignments

The color codes used in cables supplied by Alvarion with crimped connectors are as listed in Table A-1:

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

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

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



B

Appendix B - Using the SU Installer Monitor Program

In This Appendix:

- [The SU Installer Monitor Program](#), page 196
- [Using the Monitor Program](#), page 197
- [The Main Menu](#), page 199
- [Unit Control Menu](#), page 201
- [Registration Parameters Menu](#), page 210
- [Base Station ID Parameters Menu](#), page 212
- [Radio Parameters Menu](#), page 215
- [Performance Monitoring Menu](#), page 217
- [Multirate and ATPC Parameters Menu](#), page 221
- [SU Parameters Summary](#), page 223

B.1 The SU Installer Monitor Program

The SU Installer Monitor program enables configuration of basic parameters during installation to facilitate communication with the AU, including all parameters required for completion of the Network Entry process. It also enables downloading of SW files, control of the running SW version, and downloading/uploading of the configuration file, enabling simplified and faster configuration process.

The SU Installer Monitor program also provides a selection of performance monitoring capabilities, allowing installers and technicians to view information on link quality and traffic counters. These monitoring capabilities enable performance verification and problem identification.

To further support local testing, the program also enables temporary control of the ATPC and Multirate mechanisms.

B.2 Using the Monitor Program

B.2.1 Accessing the Monitor Program



To access the Monitor program:

- 1 The Monitor program uses the fixed IP address 192.168.254.251. with the subnet mask 255.255.255.0. The PC used for accessing the Monitor program should be configured accordingly. It is recommended to set the PC's IP address to 192.168.254.250, which is the default TFTP Server IP address (required for downloading SW versions and for downloading/uploading configuration files).



NOTE

The IP address 192.168.254.251 is used only for the Monitor program. This is not the IP address used by the unit for other purposes. The IP parameters for management purposes are allocated by the NPU during the Network Entry process.

- 2 Connect the PC to the Ethernet port, using a straight cable.
- 3 Run the Telnet program connecting to 192.168.254.251. The *Enter the password* prompt is displayed. Enter the password and press the Enter key.



NOTE

Following three consecutive failures to enter the correct password, access to the Monitor program will be blocked for 5 minutes.

The factory default password is "installer".

If you forgot the password, type "help" to receive a challenge string consisting of 24 characters. Contact Alvarion's Customer Service and provide the challenge string (after user identification) to receive a temporary password. You can use this password only once to enter the program. The password must be changed during the session to a different "permanent" password. The administrator should be notified of this new password. Five consecutive errors in entering the temporary password will invalidate it. In this case, repeat this procedure to receive a new challenge string for a new temporary password.

- 4 The Main menu of the SU Installer Monitor program is displayed, enabling you to access the required parameters configuration and performance monitoring options.

B.2.2 Using the Program

This section describes the Monitor program structure and navigation rules.

- Each menu or submenu displays a list of numbered options. To access an option, enter the number of the required option at the > prompt and press the Enter key.
- The header of each displayed item includes the unit identification (MAC Address), the running SW version and the name of the current item.

- The first selectable item in each menu is the Show option, enabling to view the current configuration of the applicable parameters. For some menus some additional status information is displayed.
- At any point in the program, you can use the Esc key to return to the previous menu (one level up) without applying any change.
- Configurable parameter's menu displays the current value/status of the parameter and provides instructions related to configuration changes. These instructions may include the permitted value range for the parameter, the permitted format or the selectable options.
- Each change in a parameter's configuration must be confirmed using the Enter key. If the new value/option is a valid one, the program will return to the previous menu. Entry of a wrong value will be indicated by an appropriate error message, and the configuration change text will be displayed again.
- Changes to certain parameters are applied only after reset. For these parameters, the applicable Show menus display both Current and Configured values.
- If the Monitor program is not used for 10 minutes, the session will be terminated automatically.
- Select the Exit option in the Main menu to exit the program and terminate the session.

B.3 The Main Menu

The Main menu of the SU Installer Program includes the following options:

- Show All Parameters and Status
- Unit Control
- Registration Parameters
- Base Station ID Parameters
- Radio Parameters
- Performance Monitoring
- Multirate and ATPC Parameters
- Exit

B.3.1 Show All Parameters and Status

Select this option to view the current values/selected option of all parameters as well as additional status information. The display includes all the items listed in the descriptions of the Show option in the sections explaining the Unit Control, Registration Parameters, Base Station ID Parameters, Radio Parameters and Multirate and ATPC Parameters menus.

B.3.2 Unit Control

The Unit Control menu enables resetting the unit, reverting to the default configuration, changing the password, configuring the operation mode of the Ethernet port, and selecting the running SW version. It also enables to download a new SW version.

B.3.3 Registration Parameters

The Registration Parameters menu enables configuring registration parameters that are required for services provisioning to the unit.

B.3.4 Base Station ID Parameters

The Base Station ID Parameters menu enables to configure the parameters that define the AU(s) with which the unit can synchronize.

B.3.5 Radio Parameters

The Radio Parameters menu enables configuring the basic radio parameters necessary to facilitate communication with the Base Station.

B.3.6 Performance Monitoring

The Performance Monitoring menu enables viewing continuously updated link quality parameters and traffic counters.

B.3.7 MultiRate and ATPC Parameters

The Multirate and ATPC Parameters menu enables temporary control on the transmitted signal for testing purposes.

B.3.8 Exit

Select the Exit option to exit the Monitor program and terminate the Telnet session.

B.4 Unit Control Menu

The Unit Control menu includes the following options:

- Show
- Reset Unit
- Change Password
- SW Versions Control
- Configuration Control
- Ethernet Port Operation Mode

B.4.1 Show

Select this option to view the current values/selected option of applicable parameters as well as general status information, as follows:

- SW Versions:
 - ◇ Main SW File Name
 - ◇ Main SW Version
 - ◇ Shadow SW File Name
 - ◇ Shadow SW Version
 - ◇ Running from: indicates whether the unit is running now the Main or the Shadow version.
- Upload/Download Parameters:
 - ◇ TFTP Server IP address: the IP address of the TFTP server used for SW version download and for Configuration File Download/Upload.
 - ◇ SW File Name: the name in the TFTP server of the SW version to be downloaded to the unit.
 - ◇ Configuration File Download Name: the name in the TFTP server of the configuration file to be downloaded to the unit.

- ◇ Configuration File Upload Name: the name in the TFTP server of the configuration file to be uploaded from the unit.

■ Ethernet Port Operation Mode parameters and status:

- ◇ Current Eth Mode: the actual operation mode of the Ethernet port.
- ◇ Configured Eth Mode: the configured operation mode of the Ethernet port.
- ◇ Detected Eth Mode: the actual speed and duplex parameters of the Ethernet port.

■ HW Versions:

- ◇ ODU HW Version: The version of the ODU's digital module
- ◇ ODU HW Configuration
- ◇ ODU RF Version: The version of the ODU's radio module

■ Unit Status: the connectivity status of the unit. Possible statuses are:

- ◇ Searching for Base Station
- ◇ Base Station Found
- ◇ Not Authorized
- ◇ Not Registered
- ◇ Registered

B.4.2 Reset Unit

Select this option to reset the unit. To avoid unintentional reset, you will be prompted to confirm the reset request. Changes to most of the configurable parameters are applied only after reset. Refer to [SU's Parameters Summary](#) on page 152 for information on which parameters are changeable in run time and which changes are applied only after reset.

B.4.3 Change Password

Select this option to change the password. You will be prompted to enter the new password. After pressing enter, you will be prompted to re-enter the new password.

**NOTE**

Notify the administrator of the new password!

Valid passwords: Up to 20 printable characters.

Default password: installer

B.4.4 SW Versions Control

The SU can contain two SW versions:

- Main: Each time the SU resets it will reboot using the version defined as Main.
- Shadow: Normally, the Shadow version is the backup version. Each time a new SW File is downloaded to the SU, it will be stored as a Shadow version, replacing the previous Shadow version.

The typical process of upgrading to a new SW version includes the following steps:

- 1 Download the new SW File to the SU. It will be stored as the Shadow version.
- 2 Reset and run the unit from its Shadow version. Note that at this stage, after reset the unit will reboot from its previous Main version.
- 3 If you want to continue using the new version, swap the Shadow and Main versions. The new version is now defined as Main, and will be used each time the unit reboots. The previous version is defined now as Shadow.

The SU functions as a TFTP client, enabling loading of SW files from a TFTP server.

The SW Versions Control submenu includes the following options:

- Show
- Reset and Run from Shadow
- Set Running Version as Main
- SW Download Parameters
- Perform SW Download

B.4.4.1 Show

Select this option to view the current available versions and the running version as well as the TFTP parameters:

■ SW Versions:

- ◇ Main SW File Name
- ◇ Main SW Version
- ◇ Shadow SW File Name
- ◇ Shadow SW Version
- ◇ Running from: indicates whether the unit is running now the Main or the Shadow version.

■ Download/Upload Parameters:

- ◇ TFTP Server IP address: the IP address of the TFTP server used for SW version download and for Configuration File Download/Upload.
- ◇ SW File Name: the name in the TFTP server of the SW version to be downloaded to the unit.

B.4.4.2 Reset and Run from Shadow

Select this option to reset the unit and run the Shadow version after power up. To avoid unintentional actions you will be prompted to confirm the request.

B.4.4.3 Set Running Version as Main

When the unit is running the Shadow version (after selecting Reset and Run from Shadow), it will boot from the Main version after the next reset. Select this option if you want to swap versions so that the running version will become the Main version and will be the version to be used after reset. To avoid unintentional actions you will be prompted to confirm the request.

B.4.4.4 SW Download Parameters

This submenu enables viewing or defining the parameters to be used for downloading a new SW version from a TFTP server. It includes the following options:

■ Show

- TFTP Server IP Address

- SW File Name

B.4.4.4.1 Show

Select this option to view the current SW Download parameters:

- TFTP Server IP address: the IP address of the TFTP server used for SW version download.
- SW File Name: the name in the TFTP server of the SW version to be downloaded to the unit.

B.4.4.4.2 TFTP Server IP Address

Select this option to change the IP address of the TFTP server.

The default TFTP Server IP address is 192.168.254.250.



NOTE

1. When the SU is synchronized with a base station, it receives the TFTP Server IP Address from the base station during the network entry process. This address is 1.7.1.1 for a Base Station (NPU) and 1.1.1.1 for a Micro Base Station. This will be the TFTP Server IP Address after each reset, as long as the SU is associated with a base station.
2. The same TFTP Server IP Address parameter is used in the SW Download, Configuration File Download and Configuration File Upload processes.

B.4.4.4.3 SW File Name

Select this option to enter the name in the TFTP server of the required SW file.

B.4.4.5 Perform SW Download

Select this option to execute the SW download operation. To avoid unintentional actions you will be prompted to confirm the request.



To perform SW download:

- 1 The required SW file should be available in the TFTP Server directory in a PC connected to the unit.
- 2 Typically it is recommended to configure the IP address of the PC to 192.168.154.250, which is the default TFTP Server IP address of the unit. If a different IP address is configured in the PC with the TFTP server, configure the TFTP Server IP address to the same address.
- 3 Enter the name of the SW file (as called in the TFTP server) as the SW File Name.

- 4 Select Perform SW Download and confirm the download request. Wait to receive a success/failure message.
- 5 Following a successful download, the loaded SW version becomes the Shadow version in the unit.

B.4.5 Configuration Control

The Configuration Control Submenu includes the following options:

- Set Factory Defaults
- Configuration File Download Control
- Configuration File Upload Control

B.4.5.1 Set Factory Defaults

Select this option to reset the unit and revert to the default configuration. To avoid unintentional actions you will be prompted to confirm the request. All parameters except the Password will revert to the factory default values.

B.4.5.2 Configuration File Download Control

The Configuration File Download Control submenu enables to define parameters related to downloading a configuration file from a TFTP server to the SU, and to initiate the download operation. It includes the following options:

- Show
- TFTP Server IP Address
- Configuration File Download Name
- Perform Configuration Download

B.4.5.2.1 Show

Select this option to view the current Configuration File Download parameters:

- TFTP Server IP address: the IP address of the TFTP server used for configuration file download.
- Configuration File Download Name: the name in the TFTP server of the configuration file to be downloaded to the unit.

B.4.5.2.2 TFTP Server IP Address

Select this option to change the IP address of the TFTP server.

The default TFTP Server IP address is 192.168.254.250.



NOTE

1. When the SU is synchronized with a base station, it receives the TFTP Server IP Address from the base station during the network entry process. This address is 1.7.1.1 for a Base Station (NPU) and 1.1.1.1 for a Micro Base Station. This will be the TFTP Server IP Address after each reset, as long as the SU is associated with a base station.
2. The same TFTP Server IP Address parameter is used in the SW Download, Configuration File Download and Configuration File Upload processes.

B.4.5.2.3 Configuration File Download Name

Select this option to enter the name in the TFTP server of the required configuration file. A Configuration File Download Name consists of up to 50 characters.

The default Configuration File Download Name is SU_DOWNLOAD_CFG.

B.4.5.2.4 Perform Configuration Download

Select this option to execute the configuration file download operation. To avoid unintentional actions you will be prompted to confirm the request.



To perform configuration file download:

- 1 The required configuration file should be available in the TFTP Server directory in a PC connected to the unit.
- 2 Typically it is recommended to configure the IP address of the PC to 192.168.154.250, which is the default TFTP Server IP address of the unit. If a different IP address is configured in the PC with the TFTP server, configure the TFTP Server IP address to the same address.
- 3 Enter the name of the configuration file (as called in the TFTP server) as the Configuration File Download Name.
- 4 Select Perform Configuration Download and confirm the download request. Wait to receive a success/failure message.
- 5 Following a successful download, reset the unit to apply the new configuration.

B.4.5.3 Configuration File Upload Control

The Configuration File Upload Control submenu enables to define parameters related to uploading the configuration of the SU to a file in the TFTP server directory, and to initiate the upload operation. It includes the following options:

- Show

- TFTP Server IP Address
- Configuration File Upload Name
- Perform Configuration Upload

B.4.5.3.1 Show

Select this option to view the current Configuration File Upload parameters:

- TFTP Server IP address: the IP address of the TFTP server used for configuration file upload.
- Configuration File Upload Name: the name in the TFTP server directory of the configuration file to be uploaded.

B.4.5.3.2 TFTP Server IP Address

Select this option to change the IP address of the TFTP server.

The default TFTP Server IP address is 192.168.254.250.



NOTE

1. When the SU is synchronized with a base station, it receives the TFTP Server IP Address from the base station during the network entry process. This address is 1.7.1.1 for a Base Station (NPU) and 1.1.1.1 for a Micro Base Station. This will be the TFTP Server IP Address after each reset, as long as the SU is associated with a base station.
2. The same TFTP Server IP Address parameter is used in the SW Download, Configuration File Download and Configuration File Upload processes.

B.4.5.3.3 Configuration File Upload Name

Select this option to enter the name in the TFTP server directory of the configuration file to be uploaded. A Configuration File Upload Name consists of up to 50 characters.

The default Configuration File Upload Name is SU_UPLOAD_CFG.

B.4.5.3.4 Perform Configuration Upload

Select this option to execute the configuration file upload operation. To avoid unintentional actions you will be prompted to confirm the request.



To perform configuration file upload:

- 1 Typically it is recommended to configure the IP address of the PC to 192.168.154.250, which is the default TFTP Server IP address of the unit. If a different IP address is configured in the PC with the TFTP server, configure the TFTP Server IP address to the same address.

- 2 Enter the name of the configuration file (as will be called in the TFTP server) as the Configuration File Upload Name.
- 3 Select Perform Configuration Upload and confirm the dupload request. Wait to receive a success/failure message.

B.4.6 Ethernet Port Operation Mode

The Ethernet Port Control parameter enables viewing and defining the operation mode of the Ethernet port

The available options are:

- Show Ethernet Mode
- Auto Negotiation
- 100 Mbps, Full-Duplex
- 100 Mbps, Half-Duplex
- 10 Mbps, Full-Duplex
- 10 Mbps, Half-Duplex

The default is Auto-Negotiation.

Upon selecting the Show Ethernet Mode option, the configured and actual values are displayed:

- Current Eth Mode: the actual operation mode of the Ethernet port.
- Configured Eth Mode: the configured operation mode of the Ethernet port.
- Detected Eth Mode: the actual speed and duplex parameters of the Ethernet port.

B.5 Registration Parameters Menu

The Registration Parameters menu includes the following options:

- Show
- Common Name
- Organization
- Address
- Country Code

B.5.1 Show

Select this option to view the registration parameters:

- Common Name: the unique common name of the unit. Changes to the Common Name parameter are applied only after reset. Therefore, the actual value may differ from configured value. Both the actual and configured values are displayed.
- Organization: the name of the organization (customer) using the unit.
- Address: the location of the unit.
- Country Code: the ISO 3166 3-digit country code.

B.5.2 Common Name

Select this option to enter the Common Name of the unit. This is the name used for provisioning of services to the unit, and it must be unique in the entire network. The administrator should maintain a central database to ensure name uniqueness throughout the entire network.

The Common Name consists of up to 32 printable characters.

The default Common Name is an empty string (no name). This is a mandatory parameter - the Common Name must be defined during the installation process.

B.5.3 Organization Name

Select this option to enter the name of the organization (customer) using the unit. This parameter is optional, and is intended for optional use by the Network management System.

The Organization Name consists of up to 64 printable characters.

The default Organization Name is an empty string (no Organization name).

B.5.4 Address

Select this option to enter the location of the unit. This parameter is optional, and is intended for optional use by the Network management System.

The Address consists of up to 64 printable characters.

The default Address is an empty string (no address).

B.5.5 Country Code

Select this option to enter the ISO 3166 3-digit code of the country where the unit is located. This parameter is optional, and is intended for optional use by the Network management System.

- The Country Code consists of up to 12 printable characters.
- The default Country Code is an empty string (no Country Code).

B.6 Base Station ID Parameters Menu

Each AU (sector) in the network is configured with a unique Base Station ID that consists of Operator ID, Cell ID and Sector ID. The Base Station ID parameters in the SU define the AU(s) that can synchronize with the SU. These parameters include the 3 components of a base ID for the Base Station (Operator ID, Cell ID, Sector ID and Base Station ID), and a Base Station ID Mask. The SU can synchronize only with AUs with a Base Station ID that is included in the IDs range defined by the applicable parameters in the SU (base ID of the Base Station that consists of Operator ID, Cell ID and Sector ID, and the Base Station ID Mask).

The Base Station ID Parameters menu includes the following options:

- Show
- Operator ID
- Cell ID
- Sector ID
- Base Station ID Mask

B.6.1 Show

Select this option to view the base station ID parameters and the ID of the connected AU (if applicable). The Base Station ID parameters are applied only after reset. Therefore, actual values may differ from configured values. For each parameter both the actual and configured values are displayed:

- Operator ID: the base ID of the operator. The unit can synchronize only with AUs with an Operator ID in the range defined by this Operator ID and the Operator ID part of the Base Station ID Mask.
- Cell ID: the base ID of the cell. The unit can synchronize only with AUs with a Cell ID in the range defined by this Cell ID and the Cell ID part of the Base Station ID Mask.
- Sector ID: the base ID of the sector. The unit can synchronize only with AUs with a Sector ID in the range defined by this Sector ID and the Sector ID part of the Base Station ID Mask.

- Base Station ID Mask: used with the Operator ID, Cell ID and Sector ID to define the range of AU Base Station ID(s) with which the unit can synchronize.
- Connected Base Station ID: the Base Station ID of the AU with which the unit is synchronized. If the unit is not synchronized with any AU, an empty string is displayed.

B.6.2 Operator ID

Select this option to define the Operator ID. This is the base Operator ID used together with the Operator ID part of the Base Station ID Mask to define the range of Operator IDs of the AUs that can synchronize with the unit.

The Operator ID comprises 3 groups of up to 3 digits each, where the range of each group is 0 to 255. Typically the same Operator ID will be used throughout the entire network. The Operator ID serves also for preventing SUs from synchronizing with AUs belonging to a different operator.

The default Operator ID is 186.190.0.

B.6.3 Cell ID

Select this option to define the Cell ID. This is the base Cell ID used together with the Cell ID part of the Base Station ID Mask to define the range of Cell IDs of the AUs that can synchronize with the unit.

The Cell ID comprises 2 groups of up to 3 digits each, where the range of each group is 0 to 255.

The default Operator ID is 0.0.

B.6.4 Sector ID

Select this option to define the Sector ID. This is the base Sector ID used together with the Sector ID part of the Base Station ID Mask to define the range of Sector IDs of the AUs that can synchronize with the unit.

The Sector ID comprises up to 3 digits in the range 0 to 255.

The default Sector ID is 0.

B.6.5 Base Station ID Mask

Select this option to define the Base Station ID Mask. The Base Station ID Mask, together with the Operator ID, Cell ID and Sector ID, define the range of Base Station IDs of AUs that can synchronize with the SU.

The Base Station ID Mask comprises 6 groups of up to 3 digits each, where the range of each group is 0 to 255. The first 3 groups form the mask for the

Operator ID. The next 2 groups form the mask for the Cell ID, and the last group forms the mask for the Sector ID.

The default Base Station ID Mask is 255.255.255.0.0.0.

B.7 Radio Parameters Menu

The Radio Parameters menu includes the following options:

- Show
- Bandwidth
- Uplink (Tx) frequency

B.7.1 Show

Select this option to view the radio parameters. The Base Station ID parameters are applied only after reset. Therefore, actual values may differ from configured values. For each parameter both the actual and configured values are displayed:

- Bandwidth: The bandwidth in MHz used by the radio.
- Tx Central Frequency: The central transmit frequency in MHz.
- Rx Central Frequency: The central receive frequency in MHz. This is not a configurable parameter – the Rx frequency is calculated as the configurable Uplink (Tx) Frequency plus 100 MHz.

B.7.2 Bandwidth

Select this option to define the bandwidth of the signal.

The available options are 1.75 MHz and 3.5 MHz.

The default Bandwidth is 3.5 MHz.

B.7.3 Uplink (Tx) Frequency

Select this option to define the transmit frequency of the SU.

The available options are:

- For a Bandwidth of 3.5 MHz: 3401.25 to 3498.25 MHz
- For a Bandwidth of 1.75 MHz: 3400.375 to 3499.125 MHz

For both options the resolution is 0.125 MHz.



NOTE

Some frequencies are available only with a Bandwidth of 1.75 MHz (3400.375-3401.125, 3498.375-3499.125). Prior to selecting any of these frequencies the Bandwidth must be configured to 1.75 MHz.

B.8 Performance Monitoring Menu

The Performance Monitoring menu includes the following options:

- Start Link quality Display
- Counters

B.8.1 Start Link Quality Display

Select this option to get a continuously updated display of link quality indicators. Each displayed line includes:

- SNR (dB): The average Signal to Noise Ratio of the received signal
- RSSI (dB): The average level of the received signal
- Optimal Rx Rate: The optimal Rx rate calculated by the SU and requested from the AU
- Last Rx Rate
- Last Tx Power (dBm)

B.8.2 Counters

The Counters menu includes the following options:

- Display Counters
- Reset Counters

B.8.2.1 Display Counters

Select this option to display the current status of the traffic counters. The counts are the accumulated number of relevant Bytes since the last unit reset or the last Counters Reset.

The counters indicate the traffic at the Ethernet and Wireless ports, as described in Figure B-1.

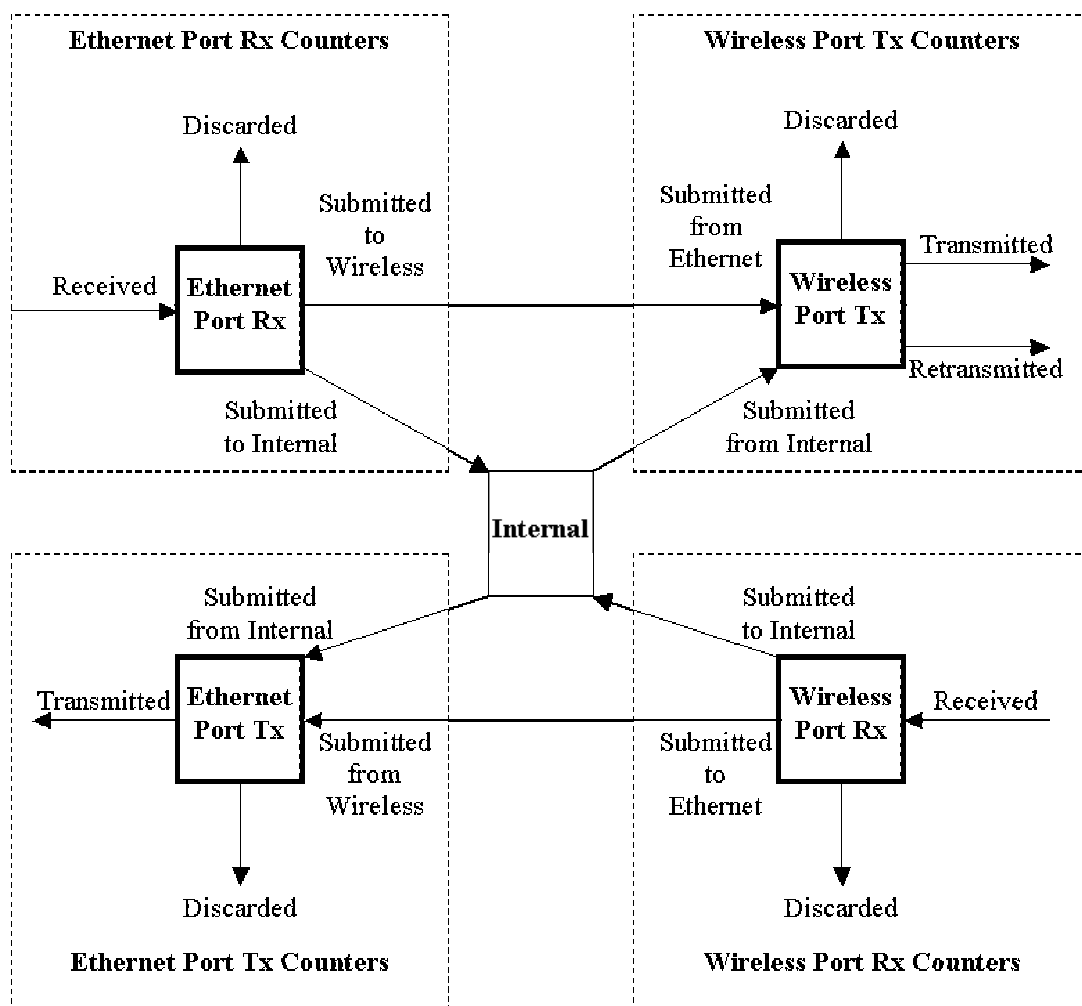


Figure B-1: Counters Description

For each port, the counters include the frames that were actually transmitted to/received from the port, the frames transferred to/from the other port (submitted), and the frames received from/transmitted to the Internal port. The Internal port refers to the internal management module of the unit that receives and transmits management and control frames to/from both the Ethernet and the Wireless ports.

In addition, for each port, the frames that were discarded for various reasons (errors, overflow etc.) are also counted.

In the Wireless Tx port, the retransmitted frames and the transmitted unicast frames (not shown in the schematic diagram) are also counted. These counters serves for calculating the retransmissions rate, providing some indication on link quality.

The displayed counters include:

- Ethernet Port Rx Counters

- ◇ Bytes Received from Ethernet
- ◇ Bytes Discarded
- ◇ Bytes Submitted to Wireless
- ◇ Bytes Submitted to Internal
- Ethernet Port Tx Counters
 - ◇ Bytes Submitted from Wireless
 - ◇ Bytes Submitted from Internal
 - ◇ Bytes Transmitted to Ethernet
 - ◇ Bytes Discarded
- Wireless Port Rx Counters
 - ◇ Bytes Received from Wireless
 - ◇ Bytes Submitted to Ethernet
 - ◇ Bytes Submitted to Internal
 - ◇ Bytes Discarded
- Wireless Port Tx Counters
 - ◇ Bytes Submitted from Ethernet
 - ◇ Bytes Submitted from Internal
 - ◇ Bytes Transmitted to Wireless
 - ◇ Bytes Discarded
 - ◇ Unicast Bytes Transmitted to Wireless
 - ◇ Bytes Retransmitted
 - ◇ Retransmission Rate (%)



NOTE

Retransmission Rate is defined as:

$100 \times \text{Bytes Retransmitted} / (\text{Unicast Bytes Transmitted to Wireless})$

Note that unacknowledged bytes are retransmitted only if ARQ is enabled. Retransmission is applicable only for information transmitted using either Best Effort (BE) or Non Real Time (NRT) Quality of Service.

B.8.2.2 Reset Counters

Select this options to reset all the counters.

B.9 Multirate and ATPC Parameters Menu

In regular operation the transmitted signal is controlled by the ATPC mechanism. The ATPC mechanism in the SU is controlled by the Base Station.

The Multirate and ATPC Parameters menu enable temporary control of the signal transmitted by the SU. It is intended for test purposes only, when it may be necessary to force the unit to transmit at a certain fixed power level. It also enables a continuous transmission of an OFDM signal at a configurable power level.

These settings will not be saved and will automatically return to original values as received from the Base Station when the units resets or upon exiting the program (or upon termination).

The Multirate and ATPC Parameters menu includes the following options:

- Show
- Enable ATPC
- Disable ATPC and Set Tx Power
- Transmit Continuous OFDM

B.9.1 Show

Select this option to view the current Multirate and ATPC parameters:

- Last Tx Rate
- Optimal Rx Rate: The current optimal rate for received signals.
- ATPC: The current status current status (Enabled/Disabled) of the ATPC mechanism
- Tx Power: The current Tx power.

B.9.2 Enable ATPC

Select this option to enable the ATPC mechanism after disabling it temporarily for testing purposes.

B.9.3 Disable ATPC and Set Tx Power

Select this option to temporarily disable ATPC for testing purposes. You will be prompted to enter the requested Tx Power. The available values for the Tx Power are from -20 dBm to 20 dBm using a 1 dBm resolution.

The default Tx Power is the last power level used before the ATPC algorithm was disabled.

Upon finishing the test, enable ATPC to resume normal operation. If not enabled manually, ATPC will be enabled automatically after the next reset or following termination of the Telnet session.

B.9.4 Transmit Continuous OFDM

Select this option to transmit a continuous OFDM signal. This is possible only when the unit is not connected (does not receive MAPs). You will be prompted to enter the requested Tx Power. The available values for the Tx Power are from -20 dBm to 20 dBm using a 1 dBm resolution.

The default Tx Power is the last power level used before the ATPC algorithm was disabled.

Continuous OFDM transmission will continue until the next reset.

B.10 SU Parameters Summary

Table B-1: SU's Parameters Summary			
Parameter	Range	Default	Run-Time Updated
Unit Control Parameters			
Password	Up to 20 printable characters, case sensitive	installer	No
TFTP Server IP Address	IP address	192.168.254.250 (1.7.1.1 if associated with an AU, 1.1.1.1 if associated with a μ BST)	Yes
SW File Name			Yes
Configuration File Download Name	Up to 50 characters	SU_DOWNLOAD_CFG	Yes
Configuration File Upload Name	Up to 50 characters	SU_UPLOAD_CFG	Yes
Ethernet Port Operation Mode	<ul style="list-style-type: none"> ■ Auto Negotiation ■ 10 Mbps, Half-Duplex ■ 10 Mbps, Full-Duplex ■ 100 Mbps, Half-Duplex ■ 100 Mbps, Full-Duplex 	Auto Negotiation	Yes
Registration Parameters			
Common Name	Up to 32 printable characters	Empty	No
Organization Name	Up to 64 printable characters	Empty	Yes
Address	Up to 64 printable characters	Empty	Yes
Country Code	The ISO 3166 3-digit country code	Empty	Yes

Table B-1: SU's Parameters Summary			
Parameter	Range	Default	Run-Time Updated
Base Station ID Parameters			
Operator ID	3 groups of up to 3 digits each. Each group range is 0-255.	186.190.0	No
Cell ID	2 groups of up to 2 digits each. Each group range is 0-255.	0.0	No
Sector ID	A groups of up to 3 digits in the range 0-255.	0	No
Base Station ID Mask	6 groups of up to 3 digits each. Each group range is 0-255.	255.255.255.0.0.0	No
Radio Parameters			
Bandwidth	1.75 MHz or 3.5 MHz	3.5 MHz	No
Uplink (Tx) Frequency	BW=3.5 MHz:3401.25 to 3498.25 BW=1.75 MHz:3400.375 to 3499.125 Resolution: steps of 0.125	3451.75 MHz	No
Multirate and ATPC Parameters			
Set Tx Power	-20 to 20 dBm using a 1 dBm resolution.	Last power used by ATPC	Yes



Appendix C - Software Upgrade

In This Appendix:

- [Before you Start](#), page 226
- [File Loading Procedure](#), page 227
- [Completing the Software Upgrade \(Switching Versions\)](#), page 228

C.1 Before you Start



NOTE

This section describes software upgrades using the Monitor program. The upgrade procedure can also be performed using AlvariSTAR. For instructions on using AlvariSTAR for software upgrade, refer to "The Software Upgrade Manager" section in the AlvariSTAR User Manual.

Loading of new SW files to the unit's FLASH memory can be performed by a simple loading procedure using a TFTP application. Upgrade packages can be obtained from the Technical Support section of Alvarion's web site,

<http://www.alvarion.com/>.

Before performing an upgrade procedure, be sure you have the most recent instructions, and that the correct SW files are available in your computer.

If you are loading new SU/AU SW files, verify that no more than two SU/AU SW files exist in the NPU/ μ BST. If there are three SU/AU SW files in the unit, one of them must be deleted before loading a new SU/AU SW file.



To view the current SU/AU SW files in NPU/ μ BST:

Select *SU/AU > SW Files in NPU/ μ BST > Show Files*.



To delete an SU/AU SW file from NPU/ μ BST:

Select *SU/AU > SW Files in NPU/ μ BST > Delete a File* and enter the name of the file to be deleted.

C.2 File Loading Procedure



To load software files:

- 1 Verify that you have IP connectivity from your computer to the NPU/Micro Base Station (either the MGMT or the DATA port). To verify the connection, ping the unit's IP address and verify that PING replies are being received.
- 2 To perform the upgrade, use a DOS TFTP utility with the following syntax: *tftp -i hostaddress put sourcefile*

where *-i* stands for binary mode and *hostaddress* is the IP address of the unit to be upgraded (NPU/ μ BST). The *put* command instructs the PC client to send a file to the *hostaddress*. *sourcefile* is the name of the SW file in the PC Client.

For example, to load the file *np1_0_2_15* to the NPU whose IP address is 172.17.31.215, use the following command:

```
tftp -i 172.17.31.215 put np1_0_2_15
```



NOTE

It is recommended to upgrade all system elements with the latest software version. Nevertheless, it is possible to upgrade each unit separately and independently.

- 3 Following a successful completion of the file loading process, the **Transfer successful** DOS message is displayed.
- 4 The unit decompresses the loaded file and checks the integrity of the new version. The new version replaces the previous shadow version only after verification. If verification tests fail, the loaded version will be rejected. The unit will reject a file if either the file name or the version number matches the current Main versions.
- 5 Check that the loaded versions exist in the unit:



To view the current NPU/ μ BST SW Versions in the unit:

Select *Unit Control>SW Versions Control>Show Versions*.



To view the current SU/AU SW files in NPU/ μ BST:

Select *SU/AU>SW Files in NPU/ μ BST>Show Files*.

C.3 Completing the Software Upgrade (Switching Versions)

After verifying successful upload of all software files, set the new version as the main version in each one of the upgraded system elements:

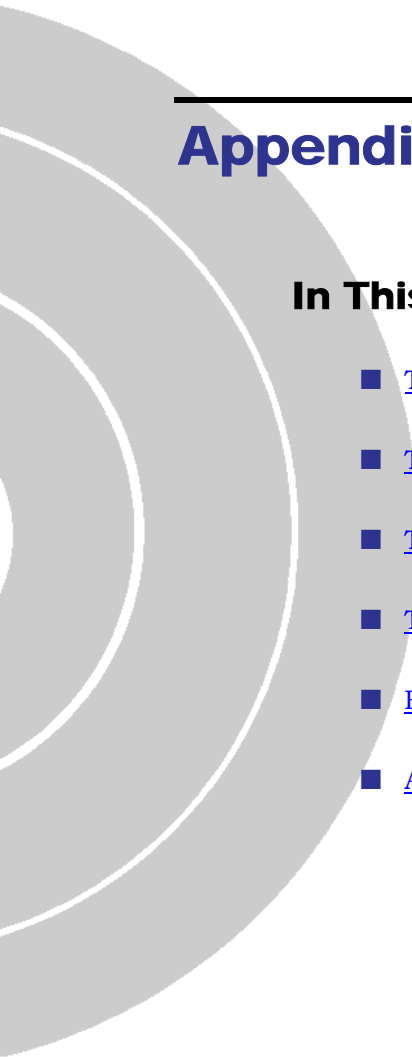
- **SU(s):** Select the SU that should be upgraded. Select *Unit Control > SW Versions Control > Set as Main*, and enter the name of the new SU SW file. The unit will reset automatically and will use the new version after power-up. Repeat the process for all SUs that should be upgraded.
- **AU(s):** Select the AU that should be upgraded. Select *Unit Control > SW Versions Control > Set as Main*, and enter the name of the new AU SW file. The unit will reset automatically. After power-up, the unit will use the new version. Repeat the process for all AUs that should be upgraded.
- **NPU/μBST:** Select *Unit Control > SW Versions Control > Run from Shadow*. The system will reset automatically. After power-up, the NPU/μBST will run from the new version, that at this stage is still marked as the Shadow Version. To switch versions, select *Unit Control > SW Versions Control > Set as Main*.



D

Appendix D - Traps and Alarms

In This Appendix:

- [Traps and Alarms Structure](#), page 230
 - [Traps and Alarms Sources](#), page 231
 - [Traps and Alarms Severities](#), page 232
 - [Trap/Alarm Categories](#), page 233
 - [BreezeMAX Traps](#), page 234
 - [Active Alarms](#), page 261
- 

D.1 Traps and Alarms Structure

A BreezeMAX trap/alarm includes the following variables:

Table D-1: BreezeMAX Trap/Alarm Variables		
Trap Variable	Alarm Variable	Description
rbTrapSeqNumber	ID	Trap/Alarm Number: A sequential number identifying the trap/alarm.
rbTrapSource	src	Trap/Alarm Source: The device that is associated with the trap/alarm. For more information refer to Traps and Alarms Sources on page 231.
rbTrapSeverity	sev	Trap/Alarm Severity: The severity of the trap/alarm. For more details refer to Traps and Alarms Severities on page 232.
rbTrapCategory	cat	Trap/Alarm Category: The category of the trap/alarm. For more details refer to Traps and Alarms Categories on page 233.
rbTrapAdditionalInfo	<Reason String>	Trap/Alarm Additional Info: Optional information on the reason for the trap/alarm, if applicable.

D.2 Traps and Alarms Sources

The trap/alarm source indicates the device that originated the trap/alarm. Each trap/alarm message should include the full hierarchy of its source.

Possible sources and associated information are:

- NPU: Slot #.
- AU: Slot #.
- SU: AU slot #, SU's MAC address.
- PSU: PSU #.
- PIU: PIU #.
- AVU
- Micro Base Station
- Service: Service Index, Service Name, Subscriber Index, Subscriber ID.

P I U # 1	P S U # 1	S L O T # 1	S L O T # 2	S L O T # 3	S L O T # 4	S L O T # 5	S L O T # 6	S L O T # 7	S L O T # 8	S L O T # 9	P S U # 3
P I U # 2	P S U # 2										P S U # 4

Figure D-1: Base Station's Chassis Slots Assignment

D.3 Traps and Alarms Severities

The trap/alarm severity level indicates how the capability of the managed object has been affected. It represents the severity of the alarm, as perceived by the managed object.

The default severity levels defined in the system, ordered from most severe to least severe, are:

Table D-2: Trap/Alarm Severities	
Severity	Description
Critical	Indicates that a service affecting condition has occurred and an immediate corrective action is required (e.g. when a managed object becomes completely out of service and its capability must be restored).
Major	Indicates that a service affecting condition has developed and an urgent corrective action is required (e.g. when there is severe degradation in the capability of the managed object and its full capability must be restored).
Minor	Indicates the existence of a non-service affecting fault condition and that a corrective action should be taken in order to prevent a more serious (for example, service affecting) fault.
Warning	Indicates the detection of a potential or impending service-affecting fault, before any significant effects have been felt. Action should be taken to further diagnose (if necessary) and correct the problem in order to prevent it from becoming a more serious service-affecting fault.
Info	Indicates a non service-affecting event, which doesn't require any further actions.

The severity of the alarm affects also the following:

- **Unit Fault Status:** The summarized severity of the unit's fault status. It reflects the severity of the alarm with the highest severity that is ON at a specific time. For a Base Station, this is the summarized severities of the NPU, AUs, PIUs, PSUs and AVU.
- **System Fault Status:** The summarized severity of the entire system fault status.

D.4 Trap/Alarm Categories

The type of trap/alarm categorizes it into one of the following five basic categories (as stated in ITU - CCITT Rec. X.733):

Table D-3: Trap/Alarm Categories		
Category	Denoting String	Description
Communications	COMM	Associated with the procedures and/or processes required to convey information from one point to another.
Quality of service	QoS	Associated with degradation in the quality of a service.
Processing Error	PROC	Associated with software or processing fault.
Equipment	EQU	Associated with an equipment fault.
Environmental	ENVR	Associated with a condition relating to an enclosure in which the equipment resides.

D.5 BreezeMAX Traps

BreezeMAX traps include the following trap groups:

- [General Traps](#) on page 234.
- [Chassis/μBST Related Traps](#) on page 239.
- [NPU/μBST Related Traps](#) on page 242.
- [AU/μBST Related Traps](#) on page 245.
- [SU Related Traps](#) on page 247.
- [Software Download and BER Test Related Traps](#) on page 248.
- [Service Related Traps](#) on page 254.
- [MIB II Traps](#) on page 257.

D.5.1 General Traps

D.5.1.1 rbResetOn Trap

rbResetOn Trap Variables	
Variable	Description
Sequential Number	1
Description	The device/card is about to perform reset.
Trap Source	μBST/NPU/AU/SU
Trap Severity	Info
Trap Category	Equipment
Additional Info	1, 2 (see details in the following table)

rbResetOn Trap Additional Info	
No.	Description
1	External Reset
2	Internal Fault Reset

D.5.1.2 rbDiagnosticsHwFaultOn Trap

rbDiagnosticsHwFaultOn Trap Variables	
Variable	Description
Sequential Number	2
Description	The device/card has detected a hardware fault.
Trap Source	μBST/NPU/AU/SU
Trap Severity	Major
Trap Category	Equipment
Additional Info	3...8, 23...27 (see details in the following table)

rbDiagnosticsHwFaultOn Trap Additional Info	
No.	Description
3	SU HW fault. Manta's (ASIC) PLL is not locked for more than 5 msec.
4	SU HW fault. Manta's (ASIC) PLL is not locked in steady state.
5	SU HW fault. Host failed to download Manta's firmware (complete with CRC errors, or handshake error).
6	SU HW fault. Radio's PLL is not locked after power up sequence.
7	SU HW fault. Radio's PLL is not locked in steady state.
8	SU, AU, NPU or μBST HW fault. A Built In Test (BIT) has failed.
23	μBST/AU HW fault. Output Tx Power exceeds P _{MAX} +5dB for more than 5 minutes.

rbDiagnosticsHwFaultOn Trap Additional Info	
No.	Description
24	μBST/AU HW fault. When a process to burn IDU table fails (CRC check on finish fails, FTP session failed, no place in FFS).
25	μBST/AU HW fault. IF synthesizer failed to lock on the frequency set on the synthesizer.
26	μBST/AU HW fault. μBST/AU detected an error while downloading the ODU table. The string includes also the byte number of the ODU table where the error was detected.
27	μBST/AU HW fault. Connection between μBST/AU and ODU has been lost.

D.5.1.3 rbDiagnosticsHwFaultOff Trap

rbDiagnosticsHwFaultOff Trap Variables	
Variable	Description
Sequential Number	3
Description	A previously detected hardware fault has been fixed.
Trap Source	μBST/NPU/AU/SU
Trap Severity	Equipment
Trap Category	Info
Additional Info	3...8, 23...27. For details see Additional Info in rbDiagnosticsHwFaultOn Trap Additional Info table above.

D.5.1.4 rbMonitorAccessOn Trap

rbMonitorAccessOn Trap Variables	
Variable	Description
Sequential Number	4
Description	The device is accessed via LCI (Monitor port) or Telnet.
Trap Source	μBST/NPU/SU
Trap Severity	Info
Trap Category	Equipment
Additional Info	140, 141. For details see the following table.

rbMonitorAccessOn Trap Additional Info	
No.	Description
140	LCI (Monitor port) access has been detected.
141	Telnet access has been detected.

D.5.1.5 rbMonitorAccessOff Trap

rbMonitorAccessOff Trap Variables	
Variable	Description
Sequential Number	5
Description	LCI (Monitor port) or Telnet access to the device has been terminated.
Trap Source	μBST/NPU/SU
Trap Severity	Info
Trap Category	Equipment
Additional Info	140, 141. For details see rbMonitorAccessOn Trap Additional Info table above.

D.5.1.6 rbAuNetworkEntryStatus Trap

rbAuNetworkEntryStatus Trap Variables	
Variable	Description
Sequential Number	6
Description	μBST/AU Network Entry status has been changed
Trap Source	μBST/AU
Trap Severity	Info
Trap Category	Communication
Additional Info	135...139

rbAuNetworkEntryStatus Trap Additional Info	
No.	Description
135	μBST/AU DHCP process failed
136	μBST/AU configuration download failed
137	μBST/AU set parameters failed
138	μBST/AU firmware download failed
139	μBST/AU is in service

D.5.2 Chassis/ μ BST Related Traps



NOTE

In μ BST, Slot# will always be 1, and PSU# will always be 1.

D.5.2.1 rbShelfCardExtractionOn Trap

rbShelfCardExtractionOn Trap Variables	
Variable	Description
Sequential Number	21
Description	The card is being extracted from the chassis.
Trap Source	NPU/AU/PIU/PSU/AVU
Trap Severity	Info
Trap Category	Equipment

D.5.2.2 rbShelfCardInsertionOn Trap

rbShelfCardInsertionOn Trap Variables	
Variable	Description
Sequential Number	22
Description	The card is being inserted into the chassis.
Trap Source	NPU/AU/PIU/AU/AVU
Trap Severity	Info
Trap Category	Equipment

D.5.2.3 rbShelfPeripheralEquipmentFaultOn Trap

rbShelfPeripheralEquipmentFaultOn Trap Variables	
Variable	Description
Sequential Number	23
Description	A fault has been detected in a peripheral unit or a μ BST component.
Trap Source	μ BST/PIU/PSU/AVU
Trap Severity	Minor
Trap Category	Equipment
Additional Info	53...55

rbShelfPeripheralEquipmentFaultOn Trap Additional Info	
No.	Description
53	A fault has been detected in a PSU, or μ BST has detected a power supply failure.
54	A fault has been detected in a PIU (not applicable to μ BST).
55	A fault has been detected in the AVU, or the μ BST has detected a problem in at least one of its fans.

D.5.2.4 rbShelfPeripheralEquipmentFaultOff Trap

rbShelfPeripheralEquipmentFaultOff Trap	
Variable	Description
Sequential Number	24
Description	A fault in a peripheral unit has been corrected.
Trap Source	μ BST/PIU/PSU/AVU
Trap Severity	Info
Trap Category	Equipment
Additional Info	53...55. See details in the following table.

rbShelfPeripheralEquipmentFaultOff Trap Additional Info	
No.	Description
53	NPU/μBST has detected that the faulty PSU/power supply has become fully operational.
54	NPU has detected that the faulty PIU has become fully operational.
55	NPU/μBST has detected that the faulty AVU/fan has become fully operational

D.5.2.5 rbShelfEnvParamFaultOn Trap

rbShelfEnvParamFaultOn Trap Variables	
Variable	Description
Sequential Number	25
Description	A fault has been detected in a chassis environmental parameter.
Trap Source	μBST/NPU
Trap Severity	Info
Trap Category	Equipment
Additional Info	73...76. For details see the following table.

rbShelfEnvParamFaultOn Trap Additional Info	
No.	Description
73	A fault has been detected in the dry contacts of NPU/μBST.
74	An NPU/μBST temperature fault has been detected.
75	An AU-IDU temperature fault has been detected.
76	An AU-ODU temperature fault has been detected.

D.5.2.6 rbShelfEnvParamFaultOff Trap

rbShelfEnvParamFaultOff Trap	
Variable	Description
Sequential Number	26
Description	A previously detected fault in a chassis environmental parameter has been fixed.
Trap Source	NPU
Trap Severity	Equipment
Trap Category	73...76. For details see rbShelfEnvParamFaultOn Trap Additional Info table above.

D.5.3 NPU/μBST Related Traps

D.5.3.1 rbConfigurationChanged Trap

rbConfigurationChanged Trap Variables	
Variable	Description
Sequential Number	41
Description	A configuration change has been detected.
Trap Source	μBST/NPU
Trap Severity	Info
Trap Category	Equipment
Additional Info	33: A Management Port parameter has been changed.

D.5.4 rbParameterSetFailure Trap

rbParameterSetFailure Trap Variables	
Variable	Description
Sequential Number	42
Description	An error in configuration change has been detected.
Trap Source	μBST/NPU/AU/SU
Trap Severity	Info
Trap Category	Equipment
Additional Info	Provided in rbTrapSetFailureReason. See below.

rbTrapSetFailureReason	
No.	Description
1	General Error
2	Failed to update parameters CRC
3	Set defaults to unknown type (internal error)
4	Failed to set defaults (internal error)
5	Log prefix is too long
6	Failed to set Log Prefix (internal error)
7	Cell Radius is invalid
8	Failed to set Cell Radius
9	Failed to set Base Station ID (internal error)
10	Failed to set Base Station Mask (internal error)
11	Failed to set ARQ mode (internal error)
12	Failed to set Band (internal error)
13	Tx Frequency is out of calculated limited range
14	Tx frequency is invalid

rbTrapSetFailureReason	
No.	Description
15	Tx frequency is out of maximum permitted range
16	Tx Frequency set failed (internal error)
17	Tx Power value is invalid
18	Set Tx Power Failed (internal error)
19	UL Basic rate is invalid
20	Failed to set Uplink Basic Rate (internal error)
21	DL Basic rate is invalid
22	Failed to set Downlink Basic Rate (internal error)
23	It is forbidden to set SU rate while Multirate is enabled
24	Invalid Downlink rate
25	Invalid Uplink rate
26	Invalid Optimal RSSI
27	Set Optimal RSSI failed (internal error)
28	BER Test data size is less than minimum allowed
29	BER Test data size is higher than the maximum allowed
30	BER Test is already running
31	Invalid BER Test Rate
32	Invalid BER Test Priority
33	Failed to set Test Priority for BER Test (internal error)
34	Invalid BER Test packet size
35	Failed to set BER Test packet size (internal error)
36	Failed to create connection for the BER test
37	Failed to disconnect Telnet session
38	Invalid Ethernet Port configuration mode
39	Set Ethernet Port mode failed (internal error)

rbTrapSetFailureReason	
No.	Description
40	SU Installer password is too long
41	Set SU Installer password failed (internal error)
42	Invalid Band
43	Invalid Aging Time or internal error
44	Invalid Limit of Supported devices or internal error
45	Failed to set Limit mode - invalid value or internal error

D.5.5 AU/μBST Related Traps

D.5.5.1 rbOduCrcErrorOn Trap

rbOduCrcErrorOn Trap Variables	
Variable	Description
Sequential Number	61
Description	A CRC error has been detected in the AU-ODU table.
Trap Source	μBST/AU
Trap Severity	Warning
Trap Category	Communication

D.5.5.2 rbOduCrcErrorOff Trap

rbOduCrcErrorOff Trap Variables	
Variable	Description
Sequential Number	62
Description	A previously detected CRC error in the AU-ODU table has been fixed.
Trap Source	μBST/AU
Trap Severity	Info
Trap Category	Communication

D.5.5.3 rbOduCommErrorOn Trap

rbOduCommErrorOn Trap Variables	
Variable	Description
Sequential Number	63
Description	An error has been detected in the communication with the AU-ODU.
Trap Source	μBST/AU
Trap Severity	Minor
Trap Category	Communication

D.5.5.4 rbOduCommErrorOff Trap

rbOduCommErrorOff Trap Variables	
Variable	Description
Sequential Number	64
Description	A previously detected error in the communication with the AU-ODU has been fixed.
Trap Source	μBST/AU
Trap Severity	Info
Trap Category	Communication

D.5.6 SU Related Traps

D.5.6.1 rbSuMaxTxPowerReached Trap

rbSuMaxTxPowerReached Trap Variables	
Variable	Description
Sequential Number	81
Description	The SU has reached the maximum allowed output power.
Trap Source	SU
Trap Severity	Info
Trap Category	PROC

D.5.6.2 rbSuMinTxPowerReached Trap

rbSuMinTxPowerReached Trap Variables	
Variable	Description
Sequential Number	82
Description	The SU has reached the minimum allowed output power.
Trap Source	SU
Trap Severity	Info
Trap Category	PROC

D.5.6.3 rbSuNetworkEntryStatus Trap

rbSuNetworkEntryStatus Trap Variables	
Variable	Description
Sequential Number	83
Description	SU's network entry status has been changed.
Trap Source	SU
Trap Severity	Info
Trap Category	PROC
Additional Info	132...134. For details see the following table.

rbSuNetworkEntryStatus Trap Additional Info	
No.	Description
132	Authentication process failed
133	Registration process failed
134	Registration process completed successfully

D.5.7 Software Download and BER Test Related Traps

D.5.7.1 rbSwDownloadStart Trap

rbSwDownloadStart Trap Variables	
Variable	Description
Sequential Number	101
Description	SW download process has started.
Trap Source	μBST/NPU/AU/SU
Trap Severity	Info
Trap Category	PROC

D.5.7.2 rbSwDownloadEnd Trap

rbSwDownloadEnd Trap Variables	
Variable	Description
Sequential Number	102
Description	SW download process has finished.
Trap Source	μBST/NPU/AU/SU
Trap Severity	Info
Trap Category	PROC

D.5.7.3 rbSwDownloadError Trap

rbSwDownloadError Trap Variables	
Variable	Description
Sequential Number	103
Description	An error has been detected in the SW download process.
Trap Source	μBST/NPU/AU/SU
Trap Severity	Minor
Trap Category	PROC
Additional Info	100...103, 150..181. See details in the following table.

NOTE

Additional Info 150...181 details reasons for AU/SU SW download failures.



rbSwDownloadError Trap Additional Info	
No.	Description
100	Unsupported Software version has been detected. This trap is generated by a μ BST/NPU when there is no compatibility between versions (μ BST/NPU, AU or SU). It is generated by AU and SU when there is no compatibility with corresponding SU or AU versions.
101	The requested SW version is not available at μ BST/NPU site. This trap is generated only by μ BST/NPU.
102	SW download process failed.
103	No space available in disk. There are already 3 SW versions in μ BST/NPU for AU/SU, and another version is being downloaded.
150	Download is aborted by an external event.
151	Header's "HW Version" is not compatible with the real unit's HW
152	Header's "HW Config" is not compatible with the real unit's HW
153	Failure to create a new file on Flash
154	Failure to open file on Flash
155	Failure to get file statistics (size..)
156	Failure to read from file
157	Failure to write to file
158	Failure to write information about SW file to the "Info" file
159	Can not Access Flash using File System
160	Old Shadow file is not accessible and can not be removed
161	NPU/ μ BST File Signature is not recognized
162	File does not contain header
163	File's header is too long
164	Some header's field title or format is not recognized
165	Header's "Unit Type" field does not match current Unit (Trying to Download wrong SW)
166	RF Version should be checked but is not found in header

rbSwDownloadError Trap Additional Info	
No.	Description
167	Header's "RF Revision" is not compatible with the real unit's RF
168	CRC calculation failed
169	Calculated CRC does not match CRC in the header
170	Calculated file size does not match file size in the header
171	Failure to start TFTP client
172	Error is received during TFTP
173	Failure to read received data from TFTP data socket
174	TFTP data socket is empty
175	Another TFTP session is already in process
176	File name is not set properly
177	File size exceeds the maximum size that can be downloaded to AU/SU
178	Files with extension other than ".bz" can not be downloaded to AU/SU.
179	File exists as Main and can not be removed
180	File is not available
181	Communication timeout

D.5.7.4 rbSwSwitchFailed Trap

rbSwSwitchFailed Trap Variables	
Variable	Description
Sequential Number	104
Description	Software switch-over failed
Trap Source	μBST/NPU/AU/SU
Trap Severity	Minor
Trap Category	PROC
Additional Info	104, 105. See details in the following table

rbSwSwitchFailed Trap Additional Info	
No.	Description
104	Run from shadow action
105	Set as Main action

D.5.7.5 rbSwSwitchSucceed Trap

rbSwSwitchSucceed Trap Variables	
Variable	Description
Sequential Number	105
Description	Software switch-over succeeded
Trap Source	μBST/NPU/AU/SU
Trap Severity	Info
Trap Category	PROC
Additional Info	105 (Set as Main action)

D.5.7.6 rbBERTestFinished Trap

rbBERTestFinished Trap Variables	
Variable	Description
Sequential Number	106
Description	BER Test finished
Trap Source	SU
Trap Severity	Info
Trap Category	PROC

D.5.7.7 rbBERTestStarted Trap

rbBERTestStarted Trap Variables	
Variable	Description
Sequential Number	107
Description	BER Test has started
Trap Source	SU
Trap Severity	Info
Trap Category	PROC

D.5.8 Service Related Traps

D.5.8.1 rbServiceDown Trap

rbServiceDown Trap Variables	
Variable	Description
Sequential Number	111
Description	The Service is down
Trap Source	SU, ServiceID
Trap Severity	Major
Trap Category	QoS

D.5.8.2 rbServiceUp Trap

rbServiceUp Trap Variables	
Variable	Description
Sequential Number	112
Description	The service has become operational
Trap Source	SU, ServiceID
Trap Severity	Info
Trap Category	QoS

D.5.8.3 rbServiceChanged Trap

rbServiceChanged Trap Variables	
Variable	Description
Sequential Number	113
Description	The Service properties have been modified
Trap Source	SU, ServiceID
Trap Severity	Info
Trap Category	QoS
Additional Info	119...122. See details in the following table.

rbServiceChanged Trap Additional Info	
No.	Description
119	Service Admin Status has been changed
120	Service SU MAC Address has been changed
121	Service VLAN List has been changed
122	Service Profile has been changed (implies that another Service Profile has been set)

D.5.8.4 rbServiceGeneralError Trap

rbServiceGeneralError Trap Variables	
Variable	Description
Sequential Number	114
Description	A Service error has been detected
Trap Source	SU, ServiceID
Trap Severity	Minor
Trap Category	QoS
Additional Info	111...118. See details in the following table.

rbServiceGeneralError Trap Additional Info	
No.	Description
111	The maximum allowed number of Subscribers has been reached
112	The maximum allowed number of Service configurations has been reached
113	The maximum allowed number of Service Profile configurations has been reached
114	The maximum allowed number of Forwarding Rules configurations has been reached
115	The maximum allowed number of Policy Rules configurations has been reached
116	The maximum allowed number of QoS Profiles configurations has been reached
117	The maximum allowed number of calls has been reached
118	There is no available bandwidth to allocate to a new VoIP call

D.5.9 MIB II Traps

D.5.9.1 coldStart Trap

coldStart Trap Variables	
Variable	Description
Sequential Number	128
Description	The device is rebooting itself and may change its configuration or the SNMP agent's configuration
Trap Source	μBST/NPU
Trap Severity	Info
Trap Category	Equipment

D.5.9.2 warmStart Trap

warmStart Trap Variables	
Variable	Description
Sequential Number	129
Description	The device is rebooting itself but neither the device's nor the SNMP agent's configuration will change
Trap Source	μBST/NPU
Trap Severity	Info
Trap Category	Equipment

D.5.9.3 linkDown Trap

linkDown Trap Variables	
Variable	Description
Sequential Number	130
Description	A communication link failure
Trap Source	μBST/NPU/AU/SU
Trap Severity	Info
Trap Category	Communication
Additional Info	127...131. See details in the following table.

linkDown Trap Additional Info	
No.	Description
127	The Ethernet connection to the backbone has been found to be down. A μBST/NPU trap.
128	The Management connection has been found to be down. A μBST/NPU trap.
129	The communication to an AU has failed. An AU trap.
130	Radio link has failed completely (loss of communication to all SUs). A μBST/AU trap.
131	Radio link to a specific SU has failed. An SU trap.

D.5.9.4 linkUp Trap

linkUp Trap Variables	
Variable	Description
Sequential Number	131
Description	A communication link that previously failed has become operational.
Trap Source	μBST/NPU/AU/SU
Trap Severity	Info
Trap Category	Communication
Additional Info	127...131. See details in the following table.

linkUp Trap Additional Info	
No.	Description
127	The Ethernet connection to the backbone has been found to be active. A μBST/NPU trap.
128	The Management connection has been found to be active. A μBST/NPU trap.
129	The communication to an AU has become active. An AU trap.
130	Radio link has become active (at least one SU is synchronized). A μBST/AU trap.
131	A new SU has become synchronized (not necessarily registered). An SU trap.

D.5.9.5 authenticationFailure Trap

authenticationFailure Trap Variables	
Variable	Description
Sequential Number	132
Description	An authentication process has failed
Trap Source	μBST/NPU/SU
Trap Severity	Warning
Trap Category	Communication
Additional Info	142...143. See details in the following table.

authenticationFailure Trap Additional Info	
No.	Description
142	LCI (Monitor port) authentication failure. A μBST/NPU trap.
143	Telnet authentication failure. A μBST/NPU or SU trap.

D.6 Active Alarms

Active alarms can be viewed in the Alarms Log of NPU/μBST, which includes all the alarms that are currently on.

The alarms are displayed in the format:

ID=<id>,name=<Name>,cat=<Category>,sev=<Severity>,src=<Source>, <Reason String>

Example: ID=21, name=ShelfCardExtractionOn, cat=EQU, sev=Info, src=PIU#1, PIU CARD EXTR

D.6.1 LinkDown Alarm

LinkDown Alarm Variables	
Variable	Description
ID	130
Description	A communication link failure
Source	μBST/NPU/AU
Severity	Info
Category	Communication
Reason String	<p>NPU/μBST ETH CONN: The Ethernet connection to the backbone has been found to be down. A μBST/NPU alarm.</p> <p>NPU/μBST MNG CONN: The Management connection has been found to be down. A μBST/NPU alarm.</p> <p>NPU AU CONN: The communication to an AU has failed. An AU alarm.</p> <p>AU RLNK LOSS: Radio link has failed completely (loss of communication to all SUs). A μBST/AU alarm.</p>

D.6.2 AuthenticationFailure Alarm

AuthenticationFailure Alarm Variables	
Variable	Description
Sequential Number	132
Description	An access authentication process has failed
Source	μBST/NPU
Severity	Warning
Category	Communication
Reason String	NPU LCI UNAUTH ACC: LCI (Monitor port) authentication failure. NPU TELNET UNAUTH ACC: Telnet authentication failure.

NOTE



Authentication Alarms remain on until expiration of the timeout.

D.6.3 DiagnosticsHwFaultOn Alarm

DiagnosticsHwFaultOn Alarm Variables	
Variable	Description
ID	2
Description	The device/card has detected a hardware fault
Source	μBST/NPU
Severity	Major
Category	Equipment
Reason String	BIT Failed

D.6.4 MonitorAccessOn Alarm

MonitorAccessOn Alarm Variables	
Variable	Description
ID	4
Description	The device is accessed via LCI (Monitor port) or Telnet
Source	μBST/NPU
Severity	Info
Category	Equipment
Reason String	NPU/μBST LCI ACCESS: LCI (Monitor port) access has been detected. NPU/μBST TELNET ACCESS: Telnet access has been detected.

D.6.5 SwDownloadStart Alarm

SwDownloadStart Alarm Variables	
Variable	Description
ID	101
Description	SW download process has started
Source	μBST/NPU/AU
Severity	Info
Category	PROC
Reason String	SW DNL START

D.6.6 SwDownloadError Alarm

SwDownloadError Alarm Variables	
Variable	Description
ID	103
Description	An error has been detected in the SW download process
Source	μBST/NPU/AU
Severity	Minor
Category	PROC
Reason String	SW DNL FAIL

D.6.7 rbSwSwitchFailed Alarm

SwSwitchFailed Alarm Variables	
Variable	Description
ID	104
Description	Software switch-over failed
Source	μBST/NPU/AU
Severity	Minor
Category	PROC
Reason String	SW SWITCH

D.6.8 ShelfCardExtractionOn Alarm

ShelfCardExtractionOn Alarm Variables	
Variable	Description
ID	21 (AU),
Description	The card is being extracted from the chassis
Source	NPU/AU
Severity	Info
Category	Equipment
Reason String	AU CARD EXTR NPU CARD EXTR PIU CARD EXTR PSU CARD EXTR AVU CARD EXTR

D.6.9 ShelfPeripheralEquipmentFaultOn Alarm

ShelfPeripheralEquipmentFaultOn Alarm Variables	
Variable	Description
ID	23
Description	A fault has been detected in a peripheral unit or a μ BST components
Source	μ BST/PIU/PSU/AVU
Severity	Minor
Category	Equipment
Reason String	BST PER FAULT

D.6.10 ShelfEnvParamFaultOn Alarm

ShelfEnvParamFaultOn Alarm Variables	
Variable	Description
ID	25
Description	A fault has been detected in a chassis environmental parameter
Source	μBST/NPU
Severity	Info
Category	Equipment
Reason String	BST ENV FAULT

Appendix E - Defining Service Profiles for Generic VoIP Gateways

In this Appendix:

- [Introduction](#), page 268
- [1 POTS Basic VoIP G.729 Service Profile](#), page 270
- [1 POTS Advanced VoIP G.729 Service Profile](#), page 272
- [1 POTS Basic VoIP G.711 Service Profile](#), page 274
- [1 POTS Advanced VoIP G.711 Service Profile](#), page 276

E.1 Introduction

This section describes the method used for defining the pre-configured Service Profiles for Generic (3rd party) VoIP devices that do not use the DRAP protocol. The same principles can be used for modifying the pre-configured profiles or creating new ones for VoIP services that have different characteristics.

E.1.1 Priority Marking

We distinguish between two types of Service Profiles for Generic VoIP devices:

- **Marking is not used:** This scenario is applicable when the VoIP device behind the SU does not support either DSCP or 802.1p marking to distinguish between different VoIP related traffic types, or when such marking is not used for any reason. The implication is that a single Continuous Grant connection should be used for all VoIP traffic.
- **Marking is used:** This scenario is applicable when the VoIP device is capable of marking the different VoIP related traffic types. The assumption is that 3 different priority marks are used: One for RTP traffic, the second for RTCP and VoIP Signaling, and a third one for Data (Device Management).

E.1.2 General Assumptions

- **Protocol Header:** 18 bytes for Ethernet L2 header (including 4 bytes for VLAN), plus 40 bytes of IP/UDP/RTP headers. A total of 58 bytes.
- **RTCP bandwidth:** RFC 3556, Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth, states that normally, the amount of bandwidth allocated to RTCP in an RTP session is 5% of the session bandwidth. To be on the safe side allocate 10% of the RTP bandwidth to RTCP.
- **VoIP Signaling:** Cisco states that its IP Phones generate approximately 150 bps signaling traffic (without L2 overhead). To be on the safe side assume 2 Kbps of VoIP Signaling traffic for each POTS interface.
- **Fax:** Fax services are assumed to be based on T.38 Fax Relay. Protocol Header is assumed to be 58 bytes (same as for RTP).
- **Data:** Data traffic may include ARP, DHCP, TFTP, SNMP, HTTP and other management protocols. The recommended default bandwidth value is up to 64 Kbps if a Best Effort connection is used for this traffic. If a Continuous Grant service is used for all VoIP related traffic, a lower bandwidth will be

allocated to Data traffic. Note that the use of bandwidth consuming protocols when an active call is present should be avoided.

E.2 1 POTS Basic VoIP G.729 Service Profile

E.2.1 Service Characteristics

- G.729 codec, 20msec sample interval
- 1 POTS
- No Fax
- Priority marking behind the SU is not used: All VoIP related traffic is classified onto a single Continuous Grant (CG) connection.
- Multiple media streams to support Call-Waiting: If the traffic exceeds the BW allocated to the CG connection, the SU may request to double the allocated BW.

E.2.2 RTP BW Calculation

The required bandwidth for a G.729 call (8 Kbps codec bit rate) with RTP and 20 bytes of voice payload is:

Total packet size (bytes) = (Ethernet of 18 bytes) + (IP/UDP/RTP header of 40 bytes) + (voice payload of 20 bytes) = 78 bytes

Total packet size (bits) = (78 bytes) * 8 bits per byte = 624 bits

PPS (Packets Per Second) = (8 Kbps codec bit rate) / (160 bits) = 50 pps

Note: 160 bits = 20 bytes (voice payload) * 8 bits per byte

Bandwidth per call = Total packet size (624 bits) * 50 pps = 31.2 Kbps

E.2.3 RTCP BW Calculation

RTCP BW is 10% of RTP: 10 % of 31.2 Kbps approximately 3.1 Kbps.

E.2.4 QoS Profile

The calculated bandwidth required for RTP traffic is 31.2 Kbps. To accommodate for other traffic types, such as RTCP (up to 3.1 Kbps), Voice Signaling (up to 2 Kbps) and Data (Device Management), we allocate to it a total bandwidth of $31.2 \times 1.5 = 46.8$ Kbps (equivalent to a Packet Size of 936 bits, or 117 bytes). The SU may request twice this BW so it will be allocated with up to approximately 94 Kbps. This is assumed to be sufficient for all traffic scenarios, including Call Waiting.

Thus, the CG 47 QoS Profile parameters are:

- Packet Size: 117 bytes
- Sample Interval: 20 msec

E.3 1 POTS Advanced VoIP G.729 Service Profile

E.3.1 Service Characteristics

- G.729 codec, 20msec sample interval
- 1 POTS
- T.38 Fax
- DSCP priority marking behind the SU is used, with the following values:
 - ◇ 63: RTP traffic
 - ◇ 26: RTCP and VoIP traffic
 - ◇ 0: Data traffic
- Single media stream to support Call-Waiting

E.3.2 Voice RTP BW Calculation

The required bandwidth for a G.729 call (8 Kbps codec bit rate) with RTP and 20 bytes of voice payload is:

Total packet size (bytes) = (Ethernet of 18 bytes) + (IP/UDP/RTP header of 40 bytes) + (voice payload of 20 bytes) = 78 bytes

Total packet size (bits) = (78 bytes) * 8 bits per byte = 624 bits

PPS (Packets Per Second) = (8 Kbps codec bit rate) / (160 bits) = 50 pps

Note: 160 bits = 20 bytes (voice payload) * 8 bits per byte

Bandwidth per call = Total packet size (624 bits) * 50 pps = 31.2 Kbps

E.3.3 Voice RTCP BW Calculation

RTCP BW is 10% of RTP: 10 % of 31.2 Kbps is 3.12 Kbps.

E.3.4 T.38 14,400 Kbps Fax RTP BW Calculation

The required bandwidth with a 20 msec sample interval is as follows:

Total packet size (bytes) = (Ethernet of 18 bytes) + (IP/UDP/RTP header of 40 bytes) + (voice payload of 36 bytes) = 94 bytes

Total packet size (bits) = (94bytes) * 8 bits per byte = 752 bits

$\text{PPS} = (14.4 \text{ Kbps bit rate}) / (288 \text{ bits}) = 50 \text{ pps}$

Note: $288 \text{ bits} = 36 \text{ bytes (voice payload)} * 8 \text{ bits per byte}$

$\text{Bandwidth per call} = \text{total packet size (752bits)} * 50 \text{ pps} = 37.6 \text{ Kbps}$

Since Fax BW is higher than Voice BW, the Fax BW requirement mandates the CG connection's attributes. This is true for all G.729 and G.723 codecs.

E.3.5 FAX RTCP BW Calculation

RTCP BW is 10% of RTP: 10 % of 37.6 Kbps is 3.76 Kbps.

E.3.6 QoS Profiles

E.3.6.1 CG QoS for RTP traffic

The calculated bandwidth required for RTP traffic is 37.6 Kbps (equivalent to a Packet Size of 752 bits, or 94 bytes). Thus, the CG 38 QoS Profile parameters are:

- Packet Size: 117 bytes
- Sample Interval: 20 msec

E.3.6.2 RT QoS for RTCP and VoIP Signaling

The required bandwidth is 5.76 Kbps (3.76 Kbps for Fax RTCP plus 2 Kbps for VoIP Signaling). We round it up to 6 Kbps. Thus, the required RT 6 QoS Profile parameters are:

- CIR: 6 Kbps
- CT: Short

E.3.6.3 BE QoS for Data

As stated, the recommended QoS Profile for Data is BE 64, with the following parameters:

- MIR: 64 Kbps
- CT: Medium

E.4 1 POTS Basic VoIP G.711 Service Profile

E.4.1 Service Characteristics

- G.711 codec, 20msec sample interval
- 1 POTS
- No Fax
- Priority marking behind the SU is not used: All VoIP related traffic is classified onto a single Continuous Grant (CG) connection.
- Multiple media streams to support Call-Waiting: If the traffic exceeds the BW allocated to the CG connection, the SU may request to double the allocated BW.

E.4.2 RTP BW Calculation

The required bandwidth for a G.711 call (64 Kbps codec bit rate) with RTP and 160 bytes of voice payload is:

Total packet size (bytes) = (Ethernet of 18 bytes) + (IP/UDP/RTP header of 40 bytes) + (voice payload of 160 bytes) = 218 bytes

Total packet size (bits) = (218 bytes) * 8 bits per byte = 1744 bits

PPS = (64 Kbps codec bit rate) / (1280 bits) = 50 pps

Note: 1280 bits = 160 bytes (voice payload) * 8 bits per byte

Bandwidth per call = total packet size (1744 bits) * 50 pps = 87.2Kbps

E.4.3 RTCP BW Calculation

RTCP BW is 10% of RTP: 10 % of 87.2 Kbps approximately 8.7 Kbps.

E.4.4 QoS Profile

The calculated bandwidth required for RTP traffic is approximately 88 Kbps. To accommodate for other traffic types, such as RTCP (up to 8.7 Kbps), Voice Signaling (up to 2 Kbps) and Data (Device Management), we allocate to it a total bandwidth of 108 Kbps (equivalent to a Packet Size of 2160 bits, or 270 bytes). The SU may request twice this BW so it will be allocated with up to approximately 216 Kbps. This is assumed to be sufficient for all traffic scenarios, including Call Waiting.

Thus, the CG 108 QoS Profile parameters are:

- Packet Size: 270 bytes
- Sample Interval: 20 msec

E.5 1 POTS Advanced VoIP G.711 Service Profile

E.5.1 Service Characteristics

- G.729 codec, 20msec sample interval
- 1 POTS
- T.38 Fax
- DSCP priority marking behind the SU is used, with the following values:
 - ◇ 63: RTP traffic
 - ◇ 26: RTCP and VoIP traffic
 - ◇ 0: Data traffic
- Single media stream to support Call-Waiting

E.5.2 Voice RTP BW Calculation

The required bandwidth for a G.711 call (64 Kbps codec bit rate) with RTP and 160 bytes of voice payload is:

Total packet size (bytes) = (Ethernet of 18 bytes) + (IP/UDP/RTP header of 40 bytes) + (voice payload of 160 bytes) = 218 bytes

Total packet size (bits) = (218 bytes) * 8 bits per byte = 1744 bits

PPS = (64 Kbps codec bit rate) / (1280 bits) = 50 pps

Note: 1280 bits = 160 bytes (voice payload) * 8 bits per byte

Bandwidth per call = total packet size (1744 bits) * 50 pps = 87.2 Kbps

E.5.3 Voice RTCP BW Calculation

RTCP BW is 10% of RTP: 10 % of 87.2 Kbps is 8.72 Kbps.

E.5.4 T.38 14,400 Kbps Fax RTP BW Calculation

The required bandwidth with a 20 msec sample interval is as follows:

Total packet size (bytes) = (Ethernet of 18 bytes) + (IP/UDP/RTP header of 40 bytes) + (voice payload of 36 bytes) = 94 bytes

Total packet size (bits) = (94 bytes) * 8 bits per byte = 752 bits

$\text{PPS} = (14.4 \text{ Kbps bit rate}) / (288 \text{ bits}) = 50 \text{ pps}$

Note: $288 \text{ bits} = 36 \text{ bytes (voice payload)} * 8 \text{ bits per byte}$

$\text{Bandwidth per call} = \text{total packet size (752 bits)} * 50 \text{ pps} = 37.6 \text{ Kbps}$

As Fax BW is lower than Voice BW, the Voice BW requirement mandates the CG connection's attributes. This is true for all G.711 codecs.

E.5.5 FAX RTCP BW Calculation

RTCP BW is 10% of RTP: 10 % of 37.6 Kbps is 3.76 Kbps.

E.5.6 QoS Profiles

E.5.6.1 CG QoS for RTP traffic

The calculated bandwidth required for RTP traffic is 87.2 Kbps (equivalent to a Packet Size of 1744 bits, or 218 bytes). Thus, the CG 88 QoS Profile parameters are:

- Packet Size: 218 bytes
- Sample Interval: 20 msec

E.5.6.2 RT QoS for RTCP and VoIP Signaling

The required bandwidth is 10.72 Kbps (8.72 Kbps for Voice RTCP plus 2 Kbps for VoIP Signaling). We round it up to 11 Kbps. Thus, the required RT 11 QoS Profile parameters are:

- CIR: 11 Kbps
- CT: Short

E.5.6.3 BE QoS for Data

As stated, the recommended QoS Profile for Data is BE 64, with the following parameters:

- MIR: 64 Kbps
- CT: Medium



Glossary



AAA

Authentication, Authorization, and Accounting (Pronounced "triple a."). A system (or several systems) that controls what resources users have access to, and keeps track of the activity of users over the network.

ANSI

American National Standards Institute. A voluntary organization composed of corporate, government, and other members that coordinates standards-related activities, approves U.S. national standards, and develops positions for the United States in international standards organizations.

ARP

Address Resolution Protocol. Internet protocol used to map an IP address to a MAC address. Defined in RFC 826.

ARQ

Automatic Repeat reQuest. A communication technique in which the receiving device detects errors and requests retransmissions.

ASCII

American Standard Code for Information Interchange. A code for representing English characters as numbers, with each letter assigned a number from 0 to 127.

ATM

Asynchronous Transfer Mode. A network technology that dynamically allocates bandwidth. ATM uses fixed-size data packets and a fixed channel between two points for data transfer. ATM was designed to support multiple services such as voice, graphics, data, and full-motion video. It allows service providers to dynamically assign bandwidth to individual customers.

ATPC

Automatic Transmit Power Control

AU

Access Unit

AVU

Air Ventilation Unit

BE	Best effort. A service where neither throughput nor delay guarantees are provided. The subscriber unit sends requests for bandwidth in either random access slots or dedicated transmission opportunities. The occurrence of dedicated opportunities is subject to network load, and the subscriber unit cannot rely on their presence. Service parameters include Committed Time (CT) and Maximum Information Rate (MIR).
BER	Bit Error Rate. In a digital transmission, BER is the percentage of bits with errors divided by the total number of bits that have been transmitted, received or processed over a given time period.
BPSK	Binary Phase-Shift Keying. A data transfer technique. BPSK transmits data using two phase modulation signals, one phase representing a binary one, and the other representing a binary zero. The signal is divided into bits; their status is determined by the preceding wave. If the wave changes, for example, the signal is reversed.
BST	Base Station
BW	Bandwidth
BWA	Broadband Wireless Access
CBR	Constant Bit-Rate
CG	Continuous Grant. Also known as Unsolicited Grant Services (UGS), is tailored for carrying constant bit- rate (CBR) real-time services characterized by fixed size data packets on a periodic basis such as VoIP or E1/T1. Service parameters include unsolicited grant size (packet size) and normal grant interval (sample interval).
CIR	Committed Information Rate. The rate (in bits per second) at which a network guarantees to transfer information under normal conditions, averaged over a minimum increment of time.
cPCI	Compact Peripheral Component Interface. a new standard for computer backplane architecture and peripheral integration, defined and developed by the peripheral component interconnect (PCI) industrial computers manufacturers group (PICMG). Designed to provide rugged, high-density systems.
CPE	Customer Premise Equipment. Communications equipment that resides on the customer's premises.

CRC	Cyclical Redundancy Check. A common technique for detecting data transmission errors, in which the frame recipient calculates a remainder by dividing frame contents by a prime binary divisor and compares the calculated remainder to a value stored in the frame by the sending equipment.
CSMA/CD	Carrier Sense Multiple Access with Collision Detection. Media-access mechanisms wherein devices ready to transmit data first check the channel for a carrier. If no carrier is sensed for a specific period of time, a device can transmit. If two devices transmit at once, a collision occurs and is detected by all colliding devices. This collision subsequently delays retransmissions from those devices for some random length of time. Ethernet and IEEE 802.3 use CSMA/CD access.
CT	Committed Time. The time interval used for measuring average information transfer rates.
DHCP	Dynamic Host Configuration Protocol. A protocol for dynamically assigning IP addresses from a pre-defined list to nodes on a network. Using DHCP to manage IP addresses simplifies client configuration and efficiently utilizes IP addresses.
DL	Down Link
DRAP	Dynamic Resources Allocation Protocol
DSCP	Differentiated Service Code Point, AKA DiffServ: An alternate use for the ToS byte in IP packets. Six bits of this byte are being reallocated for use as the DSCP field where each DSCP specifies a particular per-hop behavior that is applied to the packet.
EMC	Electro-Magnetic Compatibility. The capability of equipment or systems to be used in their intended environment within designed efficiency levels without causing or receiving degradation due to unintentional EMI (Electro Magnetic Interference). EMC generally encompasses all of the electromagnetic disciplines.
ETSI	European Telecommunications Standards Institute. A non-profit organization producing voluntary telecommunications standards used throughout Europe, some of which have been adopted by the EC as the technical base for Directives or Regulations.
FCC	Federal Communications Commission. A U.S. government agency that supervises, licenses, and controls electronic and electromagnetic transmission standards.

FDD	Frequency Division Duplex. Full duplex operation by using a pair of frequencies, one for transmission and one for reception.
FEC	Forward Error Correction. A method of communicating data that can correct errors in transmission on the receiving end. Prior to transmission, the data is put through a predetermined algorithm that adds extra bits specifically for error correction to any character or code block. If the transmission is received in error, the correction bits are used to check and repair the data.
FFT	Fast Fourier Transform. An algorithm for converting data from the time domain to the frequency domain; often used in signal processing.
FTP	File Transfer Protocol. A protocol for exchanging files over the Internet. FTP uses the Internet's TCP/IP protocols to enable data transfer.
G.711	A 64 Kbps PCM voice-coding technique. Described in the ITU-T standard in its G-series recommendations.
G.723.1	A compression technique that can be used for compressing speech or audio signal components at a very low bit rate as part of the H.324 family of standards. This codec has two bit rates associated with it: 5.3 and 6.3 Kbps. The higher bit rate provides a somewhat higher quality of sound. The lower bit rate provides system designers with additional flexibility. Described in the ITU-T standard in its G-series recommendations.
G.729	A compression technique where voice is coded into 8 Kbps streams. There are two variations of this standard (G.729 and G.729 Annex A) that differ mainly in computational complexity; both provide speech quality similar to 32-kbps ADPCM. Described in the ITU-T standard in its G-series recommendations.
GPS	Global Positioning System. A system that uses satellites, receivers and software to allow users to determine their precise geographic position.
H.323	A protocol suite defined by ITU-T for voice transmission over internet (Voice over IP or VoIP). In addition to voice applications, H.323 provides mechanisms for video communication and data collaboration, in combination with the ITU-T T.120 series standards.
IB	In-Band
IDU	Indoor Unit

IEEE	Institute of Electrical and Electronics Engineers. IEEE (pronounced I-triple-E) is an organization composed of engineers, scientists, and students. The IEEE is best known for developing standards for the computer and electronics industry. In particular, the IEEE 802 standards for local-area networks are widely followed.
IEEE 802.1p	A QoS method - A three-bit value that can be placed inside an 802.1Q frame tag.
IEEE 802.16	Also known as WiMAX. A group of broadband wireless communications standards for metropolitan area networks (MANs) developed by a working group of the IEEE.
IEEE 802.16a	An extension of IEEE 802.16. 802.16a operates in the 2-11GHz frequency band over a theoretical maximum range of 31 miles with a theoretical maximum data transfer rate of 70Mbps.
IEEE 802.1Q	The IEEE 802.1Q standard defines the operation of VLAN Bridges that permit the definition, operation and administration of Virtual LAN topologies within a Bridged LAN infrastructure. The 802.1Q specification establishes a standard method for inserting VLAN membership information into Ethernet frames. A tag field containing VLAN (and/or 802.1p priority) information can be inserted into an Ethernet frame, carrying VLAN membership information.
IEEE 802.3	A Local Area Network protocol suite commonly known as Ethernet. Ethernet uses Carrier Sense Multiple Access bus with Collision Detection CSMA/CD. This method allows users to share the network cable. However, only one station can use the cable at a time. A variety of physical medium dependent protocols are supported.
IEEE 802.11b	The IEEE 802.11b (also referred to as 802.11 High Rate or Wi-Fi). An extension to 802.11 standard for wireless Ethernet networks, that applies to wireless LANs and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band.
IEEE 802.11g	An extension to 802.11 standard for wireless Ethernet networks, that applies to wireless LANs and provides 20+ Mbps in the 2.4 GHz band.

IETF	Internet Engineering Task Force. One of the task forces of the IAB (Internet Architecture Board), formally called the Internet Activities Board, which is the technical body that oversees the development of the Internet suite of protocols (commonly referred to as "TCP/IP").The IETF is responsible for solving short-term engineering needs of the Internet.
IF	Intermediate Frequency. Radio communications systems modulate a carrier frequency with a baseband signal in order to achieve radio transmission. In many cases, the carrier is not modulated directly. Instead, a lower IF signal is modulated and processed. At a later circuit stage, the IF signal is converted up to the transmission frequency band.
IP	Internet Protocol. The standard that defines how data is transmitted over the Internet. IP bundles data, including e-mail, faxes, voice calls and messages, and other types, into "packets", in order to transmit it over public and private networks.
IPsec	Security Architecture for IP Network. IP Control Protocol (IPCP) and IPv6 Control Protocol IPsec provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithm(s) to use for the service(s), and put in place any cryptographic keys required to provide the requested services. IPsec can be used to protect one or more "paths" between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.
ITU-T	International Telecommunication Union – Telecommunications. An intergovernmental organization through which public and private organizations develop telecommunications. The ITU was founded in 1865 and became a United Nations agency in 1947. It is responsible for adopting international treaties, regulations and standards governing telecommunications. The standardization functions were formerly performed by a group within the ITU called CCITT, but after a 1992 reorganization the CCITT no longer exists as a separate entity.
LAN	Local area Network. A computer network limited to a small geographical area, such as a single building. The network typically links PCs as well as shared resources such as printers.
MAC	Media Access Control. The lower of the two sub-layers of the data link layer defined by the IEEE. The MAC sub-layer handles access to shared media, such as whether token passing or contention will be used.

MAC Address	Standardized data link layer address that is required for every port or device that connects to a LAN. Other devices in the network use these addresses to locate specific ports in the network and to create and update routing tables and data structures. MAC addresses are 6bytes long and are controlled by the IEEE.
MAN	Metropolitan Area Network. A data network designed for a town or city. In terms of geographic breadth, MANs are larger than local-area networks (LANs), but smaller than wide-area networks (WANs).
MIB	Management Information Base. A database of objects that can be monitored by a network management system. SNMP uses standardized MIB formats that allow any SNMP tools to monitor any device defined by a MIB.
MIR	Maximum Information Rate. Specifies the maximum rate of information that can be available to a user. The MIR is used by the traffic policing mechanism to prevent users from sending excess traffic to the network.
NA	Not Available or Not Applicable
NAT	Network Address Translation. Basic Network Address Translation (Basic NAT) is a method by which IP addresses are mapped from one group to another, transparent to end users. Network Address Port Translation, or NAPT is a method by which many network addresses and their TCP/UDP ports are translated into a single network address and its TCP/UDP ports. Together, these two operations, referred to as traditional NAT, provide a mechanism to connect a realm with private addresses to an external realm with globally unique registered addresses.
NIC	Network Interface Card. An expansion board you insert into a computer (or a built-in component) that enables the computer to connect to a network. Most NICs are designed for a particular type of network, protocol, and media, although some can serve multiple networks.
NIU	Network Interface Unit
NLOS	Non Line Of Sight. A term referring to wireless services which don't require a clear open path between sites.

NMS	Network Management System. A system responsible for managing at least part of a network. An NMS is generally a reasonably powerful and well-equipped computer, such as an engineering workstation. NMSs communicate with agents to help keep track of network statistics and resources.
NOC	Network Operations Center. The physical space from which a typically large telecommunications network is managed, monitored and supervised.
NPU	Network Processing Unit
NRT	Non Real Time. is very similar to the Real-Time polling service except that connections may utilize random access transmit opportunities for sending bandwidth requests. These Non Real Time Variable Bit Rate (NRT-VBR) services, such as file transfer and Internet access with a minimum guaranteed rate, are characterized by requirement for a guaranteed rate, but can tolerate longer delays and are rather insensitive to jitter. Service parameters include CIR, Committed Time (CT), and MIR that limit the rate as otherwise bandwidth_intensive services may expand to occupy full bandwidth.
OA&M	Operation, Administration & Maintenance. Provides the facilities and the personnel required to manage a network.
ODU	Outdoor Unit
OFDM	Orthogonal Frequency Division Multiplexing: A method for multiplexing signals, which divides the available bandwidth into a series of frequencies known as tones. Orthogonal tones do not interfere with each other when the peak of one tone corresponds with the null. The rapid switching, frequency-hopping technique is intended to allow more robust data service.
OOB	Out-Of-Band
PER	Packet Error Rate. In a digital transmission, PER is the percentage of packets with errors divided by the total number of packets that have been transmitted, received or processed over a given time period.
PHY	PHYSical Layer. The physical, or lowest, layer of the OSI Network Model. In a wireless network, the PHY defines parameters such as data rates, modulation method, signaling parameters, transmitter/receiver synchronization, etc. Within an actual radio implementation, the PHY corresponds to the radio front end and baseband signal processing sections.

PIU	Power Interface Unit
POTS	Plain Old Telephone System. A basic analog telephone equipment.
PSU	Power Supply Unit
PPPoE	Point-to-Point Protocol over Ethernet. PPPoE relies on two widely accepted standards: PPP and Ethernet. PPPoE is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as a single DSL line, wireless device or cable modem. All the users over the Ethernet share a common connection, so the Ethernet principles supporting multiple users in a LAN combines with the principles of PPP, which apply to serial connections.
QAM	Quadrature Amplitude Modulation. A technique used in wireless applications to double the available bandwidth by combining two amplitude-modulated signals. The two combined signals differ in phase by 90 degrees; this technique doubles the bandwidth by combining the two signals at the source before transmission, transmitting digital data at a rate of 4 bits per signal change.
QoS	Quality of Service. Measure of performance for a transmission system that reflects its transmission quality and service availability.
QPSK	Quadrature Phase Shift Keying. A data transfer technique used in coaxial cable networks that sends data using modulating signals. Four different phases represent data, with each signal's information determined by the signal before it. For example, if a phase stays the same from one signal to the other, the information has not changed.
RF	Radio frequency. An AC signal of high enough frequency to be used for wireless communications.
RSSI	Received Signal Strength Indicator. A signal or circuit that indicates the strength of the incoming (received) signal in a receiver.

RT	Real Time. Real Time service is designed to meet the needs of Real Time Variable Bit Rate (RT-VBR) like services characterized by requirements for guaranteed rate and delay such as streaming video or audio. These services are dynamic in nature, but offer periodic dedicated requests opportunities to meet real-time requirements. Because the subscriber equipment issues explicit requests, the protocol overhead and latency is increased, but capacity is granted only according to the real needs of the connection. Service parameters include CIR and CT.
RTCP	RTP Control Protocol. A protocol that monitors the QoS of an RTP connection and conveys information about the on-going session.
RTP	Real Time Protocol. An Internet protocol for transmitting real-time data such as audio and video. RTP itself does not guarantee real-time delivery of data, but it does provide mechanisms for the sending and receiving applications to support streaming data. Typically, RTP runs on top of the UDP protocol, although the specification is general enough to support other transport protocols.
Rx	Receive
SIP	Session Initiation Protocol. An application-layer control IETF protocol that can establish, modify, and terminate multimedia sessions such as Internet telephony calls (VoIP). SIP can also invite participants to already existing sessions, such as multicast conferences. Media can be added to (and removed from) an existing session. SIP transparently supports name mapping and redirection services, which supports personal mobility - users can maintain a single externally visible identifier regardless of their network location.
SLA	Service Level Agreement. A contract between a service provider and the end user, which stipulates and commits the service provider to a required level of service. An SLA relates to issues such as specified level of service, support options, enforcement or penalty provisions for services not provided, a guaranteed level of system performance as relates to downtime or uptime, a specified level of customer support and what software or hardware will be provided and for what fee.
SME	Small and Medium-sized Enterprises. SMEs are small-scale entrepreneurial private enterprises: they are usually defined as having less than 250 employees, but most have far fewer.

SNMP	Simple Network Management Protocol. A network management protocol that provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.
SNR	Signal to Noise Ratio. The ratio of the amplitude of a desired analog or digital data signal to the amplitude of noise in a transmission channel at a specific point in time. SNR is typically expressed logarithmically in decibels (dB). SNR measures the quality of a transmission channel or a signal over a network channel. The greater the ratio, the easier it is to identify and subsequently isolate and eliminate the effects of noise. SNR also is abbreviated as S/N.
SOHO	Small Office Home Office. A term that refers to the small or home office environment and the business culture that surrounds it. Typically it refers to an office or business with ten or fewer computers and/or employees.
SU	Subscriber Unit
TCP	Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is the part of the TCP/IP suite of protocols that is responsible for forming data connections between nodes that are reliable, as opposed to IP, which is connectionless and unreliable.
TCP/IP	Transmission Control Protocol/Internet Protocol. A set of protocols developed by the U.S. Department of Defense to allow communication between dissimilar networks and systems over long distances. TCP/IP is the de facto standard for data transmission over networks, including the Internet.
TDM	Time Division Multiplexing. Technique in which information from multiple channels can be allocated bandwidth on a single link based on pre-assigned time slots. Bandwidth is allocated to each channel regardless of whether the station has data to transmit.
TFTP	Trivial File Transfer Protocol. Simplified version of FTP that allows files to be transferred from one computer to another over a network, usually without the use of client authentication.
Tx	Transmit

μBST	Micro Base Station
U	A unit for measuring the height in rack cabinets. 1U = 1.75 inches.
UDP	User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768.
UL	Up Link
VLAN	Virtual Local Area Network. A group of devices on one or more LANs that are configured with the same VLAN ID so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Used also to create separation between different user groups.
VLSI	Very Large Scale Integration. The process of placing thousands (or hundreds of thousands) of electronic components on a single chip.
VoIP	Voice over Internet Protocol. Provides an advanced digital communications network that bypasses the traditional public switched telephone system and uses the Internet to transmit voice communication. VoIP enables people to use the Internet as the transmission medium for telephone calls by sending voice data in packets using IP rather than by traditional circuit switched transmissions of the PSTN.
VPL	Virtual Private Link. A virtual connection between two points on the network, such as a base station and a service provider or corporate network. Identified by the VPL ID, with functionality that is similar to VLAN ID (VLAN on the backbone network).
VPN	Virtual Private Network. A private network of computers that's at least partially connected by public lines. A good example would be a private office LAN that allows users to log in remotely over the Internet (an open, public system). VPNs use encryption and secure protocols like PPTP to ensure that data transmissions are not intercepted by unauthorized parties.
WAN	Wide Area Network. A computer network that spans a relatively large geographical area. Wide area networks can be made up of interconnected smaller networks spread throughout a building, a state, or the entire globe.

WIMAX

The name commonly given to the IEEE 802.16 standard. Specifications for fixed broadband wireless metropolitan access networks (MANs) that use a point-to-multipoint architecture. WIMAX supports very high bit rates in both uploading to and downloading from a base station up to a distance of 30 miles.