



**BreezeMAX™ 3000 Modular Base  
Station**

**System Manual**

**SW Version 2.5  
June 2006  
P/N 213920**

## Document History

Topic	Description	Version/Date Issued
General	Base Station, Micro Base Station and CPE have been divided to separate manuals	SW Version 2.0, January 2006
New Radio Bands Sections <a href="#">1.1</a> , <a href="#">1.5.1</a>	New ODUs that support 3.3g, 3.6a and 3.6b frequency bands	SW Version 2.0, January 2006
Monitor/Telnet access Sections <a href="#">4.2.1</a> , <a href="#">4.5.2.1</a>	3 access levels: Administrator, Installer, Monitor	SW Version 2.0, January 2006
Per Trap Configuration Section <a href="#">4.4.3.4</a>	Per trap configuration of Admin Status, Severity and Suppression Interval	SW Version 2.0, January 2006
Multi Channels Sections <a href="#">4.4</a> , <a href="#">4.6</a> , <a href="#">4.7</a> , <a href="#">4.8</a>	Support of Multi-Channels AU. Radio Cluster, ODU, AU and Channel entities, including new and modified parameters.	SW Version 2.0, January 2006
Frequency Bands File Section <a href="#">4.7.5</a>	Separating availability of radio bands (new HW) from SW releases.	SW Version 2.0, January 2006
Cumulative Power On Time Sections <a href="#">4.5.1</a> , <a href="#">4.8.4.1</a>	Display of the cumulative power on time for NPU and AU modules.	SW Version 2.0, January 2006
Additional Back-Up Files Section <a href="#">4.5.2.5</a>	Create/download Back Up Files for Filtering parameters (including MAC Address Deny List) and for Trap Configuration.	SW Version 2.0, January 2006
Performance Monitoring Sections <a href="#">4.5.4</a> , <a href="#">4.8.5</a> , <a href="#">4.9.6.4</a> , <a href="#">4.10.4.3.2</a>	Improved counters for NPU, AU, SU and Service	SW Version 2.0, January 2006
SU Service Fault Status Section <a href="#">4.9.1</a>	Indication of reason for service denial: Loop problem or SU Duplicate Name	SW Version 2.0, January 2005
Configurable SU Name Section <a href="#">4.9.6.3.1.1</a>	To enable a solution to situations with Duplicate SU Names	SW Version 2.0, January 2006
SU Estimated Distance Section <a href="#">4.9.1</a>	Displaying for each SU its estimated distance from the Base Station	SW Version 2.0, January 2006
MAC Addresses Behind SU Section <a href="#">4.9.6.5</a>	Displaying the list of MAC Addresses (and VLAN IDs if applicable) of devices behind SU	SW Version 2.0, January 2006

Topic	Description	Version/Date Issued
Filtering Sections <a href="#">4.10.2</a> , <a href="#">4.10.4.8</a> , <a href="#">4.10.4.9</a> , <a href="#">4.10.4.10</a>	Controlling traffic by forwarding/discarding packets according to a set of rules. Support of L2 and L3/L4 filters. Filtering is per interface (from either network or wireless side)	SW Version 2.0, January 2006
MAC Address Deny List Sections <a href="#">4.10.2</a> , <a href="#">4.10.4.11</a>	Controlling traffic by discarding packets to/from specific MAC Addresses	SW Version 2.0, January 2006
Hybrid VLAN Mode Sections <a href="#">4.10.1.5</a> , <a href="#">4.10.4.3.1.6</a>	Enabling classification of both tagged and untagged frames	SW Version 2.0, January 2006
VLAN Transparency Mode Sections <a href="#">4.10.1.5</a> , <a href="#">4.10.4.4.3</a>	Defining the method of transferring packets to the operator's upstream network	SW Version 2.0, January 2006
Multicast VLAN Sections <a href="#">4.10.1.5</a> , <a href="#">4.10.4.5.6</a>	Modified functionality. The feature is needed only to support multiple VLANs behind SUs that use a SW version below 2.0. In SW version 2.0 and higher the SU handles multiple VLANs by properly duplicating messages.	SW Version 2.0, January 2006
DRAP TTL Retries Section <a href="#">4.5.3.5</a>	Parameter added in formal release of SW version 1.5, defining the maximum time before "dropping" the gateway.	SW Version 2.0, January 2006
Bridge Aging Time (Micro Base Station) Section <a href="#">4.5.3.4</a>	Option of No Aging Time (null entry) added	SW Version 2.0, January 2006
AU-ODU-HP	New Product	SW Version 2.5, June 2006
ODU-Power Feeder	New Product	SW Version 2.5, June 2006
Licenses Sections <a href="#">4.4.4</a> and <a href="#">4.9.6.3.9</a>	New feature	SW Version 2.5, June 2006
Debug Stream Section <a href="#">4.5.3.6</a>	New feature	SW Version 2.5, June 2006

Topic	Description	Version/Date Issued
Transparent Forwarding Rule <a href="#">Table 4-20</a>	No editing of Transparent Forwarding Rule Name.	SW Version 2.5, June 2006
BER Test	The BER Test feature was removed.	SW Version 2.5, June 2006

---

## Legal Rights

© Copyright 2006 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<sup>®</sup>, BreezeCOM<sup>®</sup>, WALKair<sup>®</sup>, WALKnet<sup>®</sup>, BreezeNET<sup>®</sup>, BreezeACCESS<sup>®</sup>, BreezeMANAGE<sup>™</sup>, BreezeLINK<sup>®</sup>, BreezeCONFIG<sup>™</sup>, BreezeMAX<sup>™</sup>, AlvariSTAR<sup>™</sup>, BreezeLITE<sup>™</sup>, MGW<sup>™</sup>, eMGW<sup>™</sup>, WAVEXpress<sup>™</sup>, MicroXpress<sup>™</sup>, WAVEXchange<sup>™</sup>, WAVEView<sup>™</sup>, GSM Network in a Box and TurboWAVE<sup>™</sup> 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' 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 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, Power Feeders and outdoor units are required to be bonded to protective grounding using the bonding stud or screw provided with each unit.

## Safety Considerations - DC Powered Equipment (BST & Power Feeder)



### CAUTION

Risk of electric shock and energy hazard. Disconnecting one Power Interface Unit (PIU) disconnects only one PIU module. To isolate the Base Station completely, disconnect both PIUs

### ATTENTION

Risque de décharge électrique et d'électrocution. La déconnexion d'un seul module d'alimentation (PIU) n'isole pas complètement la Station de Base. Pour cela, il faut impérativement débrancher les deux modules d'alimentation (PIU).

**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 Power Feeder, 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 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.

## Disposal of Electronic and Electrical Waste



### **Disposal of Electronic and Electrical Waste**

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

---

## Important Notice

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

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



# About This Manual

This manual describes the BreezeMAX 3000 ("BreezeMAX") Base Station equipment Release 2.5 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 Base Station equipment, 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 Base Station system components.
- **Chapter 3 - Commissioning:** Describes how to configure basic parameters and validate units' operation.
- **Chapter 4 - Operation and Administration:** Describes how to use the Monitor application for configuring parameters, checking system status and monitoring performance.
- **Appendix A - Software Upgrade:** Describes how to load new software files using TFTP, and how to switch to a new software version in BreezeMAX units.
- **Appendix B - Defining Service Profiles for Generic VoIP Gateways:** Describes the principles of defining Service Profiles for 3rd party generic (non DRAP based) VoIP devices.
- **Glossary:** A listing of commonly used terms.
- **Index**



# Contents

## Chapter 1 - System Description

<b>1.1 Introducing BreezeMAX</b> .....	<b>2</b>
<b>1.2 Base Station Equipment</b> .....	<b>5</b>
1.2.1 Base Station Chassis .....	5
1.2.2 Network Processing Unit (NPU) .....	5
1.2.3 Access Unit (AU-IDU) .....	6
1.2.4 AU-ODU .....	7
1.2.5 Power Feeder.....	7
1.2.6 Power Interface Unit (PIU) .....	8
1.2.7 Power Supply Unit (PSU).....	8
1.2.8 Air Ventilation Unit (AVU).....	9
<b>1.3 Networking Equipment</b> .....	<b>10</b>
<b>1.4 Management Systems</b> .....	<b>10</b>
1.4.1 AlvariSTAR™ .....	10
1.4.2 BreezeLITE™.....	11
<b>1.5 Specifications</b> .....	<b>13</b>
1.5.1 Radio.....	13
1.5.2 Base Station Antennas (Optional).....	14
1.5.3 AU-IDU to AU-ODU Communication.....	15
1.5.4 Data Communication (Ethernet Ports) .....	16
1.5.5 Configuration and Management.....	16
1.5.6 Standards Compliance, General .....	17
1.5.7 Environmental .....	17

1.5.8 Services .....	18
1.5.9 Physical and Electrical .....	19
<b>Chapter 2 - Installation Guidelines</b>	
<b>2.1 Installing the AU-ODU.....</b>	<b>24</b>
2.1.1 AU-ODU Installation Requirements .....	24
2.1.2 Guidelines for Positioning the AU-ODU .....	25
2.1.3 IF Cables.....	25
2.1.4 Pole Mounting the ODU .....	26
2.1.5 AU-ODU .....	31
2.1.6 Connecting the Cables.....	32
<b>2.2 Installing the Base Station Equipment.....</b>	<b>33</b>
2.2.1 BST Installation Requirements.....	33
2.2.2 BMAX-BST-SH Chassis Slot Assignments .....	34
2.2.3 Power Requirements.....	35
2.2.4 HOT SWAP Support .....	35
2.2.5 Power Interface Unit (PIU) .....	35
2.2.6 Power Supply Unit (PSU).....	38
2.2.7 Access Unit Indoor Module (AU-IDU) .....	39
2.2.8 Network Processing Unit (NPU).....	41
2.2.9 Using the Hot Swap Injector/Ejector Handles .....	44
2.2.10 Installing the Base Station Chassis and Modules .....	46
2.2.11 Air Ventilation Unit (AVU).....	47
<b>2.3 Installing the ODU Power Feeder .....</b>	<b>50</b>
2.3.1 Installation Requirements.....	50
2.3.2 The ODU Power Feeder .....	51
2.3.3 Installing the ODU Power Feeder .....	52

## Chapter 3 - Commissioning

<b>3.1 Configuring Basic Parameters of Base Station.....</b>	<b>56</b>
<b>3.2 Operation Verification.....</b>	<b>58</b>
3.2.1 AU-ODU LEDs .....	58
3.2.2 Base Station LEDs .....	59
3.2.3 ODU Power Feeder LEDs.....	62
3.2.4 Verifying the Ethernet Connection .....	62

## Chapter 4 - Operation and Administration

<b>4.1 BreezeMAX System Management.....</b>	<b>64</b>
<b>4.2 The Monitor Program.....</b>	<b>66</b>
4.2.1 Accessing the Monitor Program .....	66
4.2.2 Using the Monitor Program .....	67
<b>4.3 The NPU's Main Menu.....</b>	<b>70</b>
4.3.1 Base Station Menu.....	70
4.3.2 NPU Menu.....	70
4.3.3 Radio Cluster Menu .....	70
4.3.4 ODU Menu .....	70
4.3.5 AU Menu .....	71
4.3.6 SU Menu .....	71
4.3.7 Services Menu .....	71
4.3.8 Exit .....	71
<b>4.4 Base Station Menu .....</b>	<b>72</b>
4.4.1 Show .....	72
4.4.2 Configuration.....	73
4.4.3 Alarms and Traps.....	75

4.4.4 Licenses .....	78
<b>4.5 NPU Menu .....</b>	<b>81</b>
4.5.1 Show .....	81
4.5.2 Unit Control .....	83
4.5.3 Configuration .....	87
4.5.4 Performance Monitoring.....	95
<b>4.6 Radio Cluster Menu.....</b>	<b>98</b>
4.6.1 Show Summary .....	98
4.6.2 Select .....	98
4.6.3 Add.....	99
4.6.4 Radio Cluster Parameters.....	99
<b>4.7 ODU Menu .....</b>	<b>101</b>
4.7.1 Show Summary .....	101
4.7.2 Select .....	102
4.7.3 Add.....	103
4.7.4 ODU Parameters.....	103
4.7.5 Frequency Bands File and Frequency Bands Groups .....	104
<b>4.8 AU Menu.....</b>	<b>106</b>
4.8.1 Show Summary .....	106
4.8.2 SW Files in NPU .....	107
4.8.3 Select .....	107
4.8.4 AU Slot # Menu .....	107
4.8.5 Performance Monitoring.....	117
<b>4.9 SU Menu .....</b>	<b>120</b>
4.9.1 Show Summary .....	120
4.9.2 Show Summary by AU .....	122



---

4.9.3 SW Files in NPU .....	122
4.9.4 Select by Name.....	123
4.9.5 Select by MAC Address .....	123
4.9.6 SU # Menu .....	123
4.9.7 Add New SU.....	136
<b>4.10 Services Menu.....</b>	<b>137</b>
4.10.1 Introduction to Services.....	137
4.10.2 Introduction to Filtering Features .....	144
4.10.3 Common Operations in Services Menu .....	145
4.10.4 The Services Menu .....	146
4.10.5 Defining Services .....	170
4.10.6 Pre-configured Profiles.....	171
<b>4.11 NPU Parameters Summary .....</b>	<b>178</b>
<b>Appendix A - Software Upgrade</b>	
<b>A.1 Before you Start .....</b>	<b>190</b>
<b>A.2 File Loading Procedure .....</b>	<b>191</b>
<b>A.3 Completing the Software Upgrade (Switching Versions).....</b>	<b>193</b>
<b>Appendix B - Defining Service Profiles for Generic VoIP Gateways</b>	
<b>B.1 Introduction .....</b>	<b>196</b>
B.1.1 Priority Marking .....	196
B.1.2 General Assumptions.....	196
<b>B.2 1 POTS Basic VoIP G.729 Service Profile .....</b>	<b>198</b>
B.2.1 Service Characteristics .....	198
B.2.2 RTP BW Calculation .....	198
B.2.3 RTCP BW Calculation.....	198

B.2.4	QoS Profile .....	198
<b>B.3 1</b>	<b>POTS Advanced VoIP G.729 Service Profile.....</b>	<b>200</b>
B.3.1	Service Characteristics .....	200
B.3.2	Voice RTP BW Calculation .....	200
B.3.3	Voice RTCP BW Calculation .....	200
B.3.4	T.38 14,400 Kbps Fax RTP BW Calculation .....	200
B.3.5	FAX RTCP BW Calculation .....	201
B.3.6	QoS Profiles .....	201
<b>B.4 1</b>	<b>POTS Basic VoIP G.711 Service Profile .....</b>	<b>202</b>
B.4.1	Service Characteristics .....	202
B.4.2	RTP BW Calculation .....	202
B.4.3	RTCP BW Calculation .....	202
B.4.4	QoS Profile .....	202
<b>B.5 1</b>	<b>POTS Advanced VoIP G.711 Service Profile.....</b>	<b>204</b>
B.5.1	Service Characteristics .....	204
B.5.2	Voice RTP BW Calculation .....	204
B.5.3	Voice RTCP BW Calculation .....	204
B.5.4	T.38 14,400 Kbps Fax RTP BW Calculation .....	204
B.5.5	FAX RTCP BW Calculation .....	205
B.5.6	QoS Profiles .....	205
<a href="#">Glossary</a> .....		<a href="#">207</a>
<a href="#">Index</a> .....		<a href="#">221</a>



# Figures

Figure 1-1: BreezeMAX System Architecture.....	4
Figure 2-1: AU-ODU Pole Installation Using Special Clamps .....	27
Figure 2-2: AU-ODU Pole Installation Using Metal Band .....	28
Figure 2-3: AU-ODU-HP Pole Installation Using Special Clamps .....	29
Figure 2-4: AU-ODU-HP Pole Installation Using Metal Band.....	30
Figure 2-5: Bottom Panel of the AU-ODU .....	31
Figure 2-6: BMAX-BST-SH Chassis Slot Assignments.....	34
Figure 2-7: PIU Module Front Panel.....	36
Figure 2-8: PSU Module Front Panel .....	39
Figure 2-9: AU-IDU Module Front Panel .....	40
Figure 2-10: NPU Module Front Panel.....	42
Figure 2-11: AVU Drawer Front Panel .....	47
Figure 2-12: ODU Power Feeder Front Panel.....	51
Figure 2-13: ODU Power Feeder Rear Panel .....	51
Figure 4-1: Base Station Chassis Slot Assignment.....	73
Figure 4-2: Uplink and Downlink Scheduled Transmissions .....	135
Figure 4-3: Filtering Functionality .....	145





# Tables

Table 1-1: 3.3 GHz Frequency Bands.....	2
Table 1-2: 3.5 GHz Frequency Bands.....	3
Table 1-3: 3.6 GHz Frequency Bands.....	3
Table 1-4: PSU Requirements, Configurations with one NPU (excluding PSU redundancy) .....	8
Table 1-5: PSU Requirements, Configurations with two NPUs (excluding PSU redundancy) .....	8
Table 1-6: Radio Specifications.....	13
Table 1-7: Base Station Antennas, Electrical Specifications.....	14
Table 1-8: AU-IDU to AU-ODU Communication.....	15
Table 1-9: Data Communication (Ethernet Ports) .....	16
Table 1-10: Configuration and Management.....	16
Table 1-11: Standards Compliance, General.....	17
Table 1-12: Environmental Specifications.....	17
Table 1-13: Services .....	18
Table 1-14: Mechanical Specifications, Base Station Equipment .....	19
Table 1-15: Electrical Specifications, Base Station Equipment.....	19
Table 1-16: Connectors, Base Station Equipment .....	20
Table 1-17: Base Station Antennas, Mechanical Specifications .....	21
Table 2-1: AU-ODU Types .....	24
Table 2-2: IF Cables Requirements .....	26
Table 2-3: Maximum IF Cable Length (Double Shielded Cables) .....	26
Table 2-4: AU-ODU LEDs .....	31
Table 2-5: AU-ODU Connectors.....	31
Table 2-6: Power Requirements, Base Station Equipment.....	35

Table 2-7: PIU LEDs .....	37
Table 2-8: PSU Requirements, Configurations with one NPU (excluding PSU redundancy) .....	38
Table 2-9: PSU Requirements, Configurations with two NPUs (excluding PSU redundancy) .....	38
Table 2-10: PSU LEDs .....	39
Table 2-11: AU-IDU LEDs .....	40
Table 2-12: NPU Connectors .....	42
Table 2-13: NPU LEDs .....	43
Table 2-14: AVU LEDs .....	48
Table 2-15: ODU Power Feeder Connectors .....	51
Table 2-16: ODU Power Feeder LEDs .....	52
Table 3-1: Basic NPU Parameters .....	56
Table 3-2: AU-ODU LEDs .....	58
Table 3-3: AU-IDU LEDs .....	59
Table 3-4: NPU LEDs .....	60
Table 3-5: PIU LEDs .....	61
Table 3-6: PSU LEDs .....	61
Table 3-7: AVU LEDs .....	61
Table 3-8: ODU Power Feeder LEDs .....	62
Table 4-1: COM Port Configuration .....	66
Table 4-2: Default Passwords .....	84
Table 4-3: Frequency Bands .....	105
Table 4-4: Automatic Association of Channel 1 Upon First Power-Up .....	114
Table 4-5: Rates (Modulation Schemes and Coding) .....	116
Table 4-6: Hybrid VLAN Mode .....	143
Table 4-7: Hybrid VLAN Mode .....	149
Table 4-8: Priority Marking Values .....	157

---

Table 4-9: CT Values .....	164
Table 4-10: Pre-Configured Data Service Profiles .....	172
Table 4-11: Pre-Configured Forwarding Rules for Data Service.....	173
Table 4-12: Pre-Configured Priority Classifiers for Data Services .....	173
Table 4-13: Pre-Configured QoS Profiles for Data Services .....	174
Table 4-14: Pre-Configured Voice Service Profiles (for DRAP-based Gateways) .....	174
Table 4-15: Pre-Configured Service Profiles for Generic (non-DRAP) VoIP Services.....	174
Table 4-16: Pre-Configured Forwarding Rule for Voice Services .....	175
Table 4-17: Pre-Configured Priority Classifiers for Generic (non-DRAP) VoIP Services .....	175
Table 4-18: Pre-Configured BE and RT QoS Profile for Voice Services.....	176
Table 4-19: Pre-Configured CG QoS Profile for Generic (non-DRAP) VoIP Services .....	176
Table 4-20: Pre-Configured Forwarding Rule for Transparent Services .....	176
Table 4-21: Pre-Configured QoS Profile for Transparent Services .....	177
Table 4-22: NPU Monitor Parameters Summary.....	178





---

## Chapter 1 - System Description

### In This Chapter:

- “Introducing BreezeMAX” on page 2
- “Base Station Equipment” on page 5
- “Networking Equipment” on page 10
- “Management Systems” on page 10
- “Specifications” on page 13

## 1.1 Introducing BreezeMAX

BreezeMAX 3000 is Alvarion's WiMAX platform for the 3 - 4 GHz licensed frequency bands. 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 3000 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 3.3 GHz, 3.5 GHz and 3.6 GHz frequency bands, as shown in the following tables. 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: 3.3 GHz Frequency Bands**

Series (band)	Duplex Separation	Uplink Frequency	Downlink Frequency
3.3e	50 MHz	3366-3385 MHz	3316-3335 MHz
3.3f	50 MHz	3381-3400 MHz	3331-3350 MHz
3.3g	-76 MHz	3300-3324 MHz	3376-3400 MHz

\* The 3.3 GHz CPE supports the full range of the 3.3e and 3.3f bands. The 3.3 GHz g CPE supports the 3.3g band. The Base Station's radio (ODU) supports a single band: 3.3e, 3.3f or 3.3g.

**Table 1-2: 3.5 GHz Frequency Bands**

Series (band)	Duplex Separation	Uplink Frequency	Downlink Frequency
3.5a	-100 MHz	3399.5 to 3453.5 MHz	3499.5 to 3553.5 MHz
3.5b	-100 MHz	3450 to 3500 MHz	3550 to 3600 MHz

\* The 3.5 GHz CPE supports the full range. The Base Station's radio (ODU) supports either band 3.5a or band 3.5b.

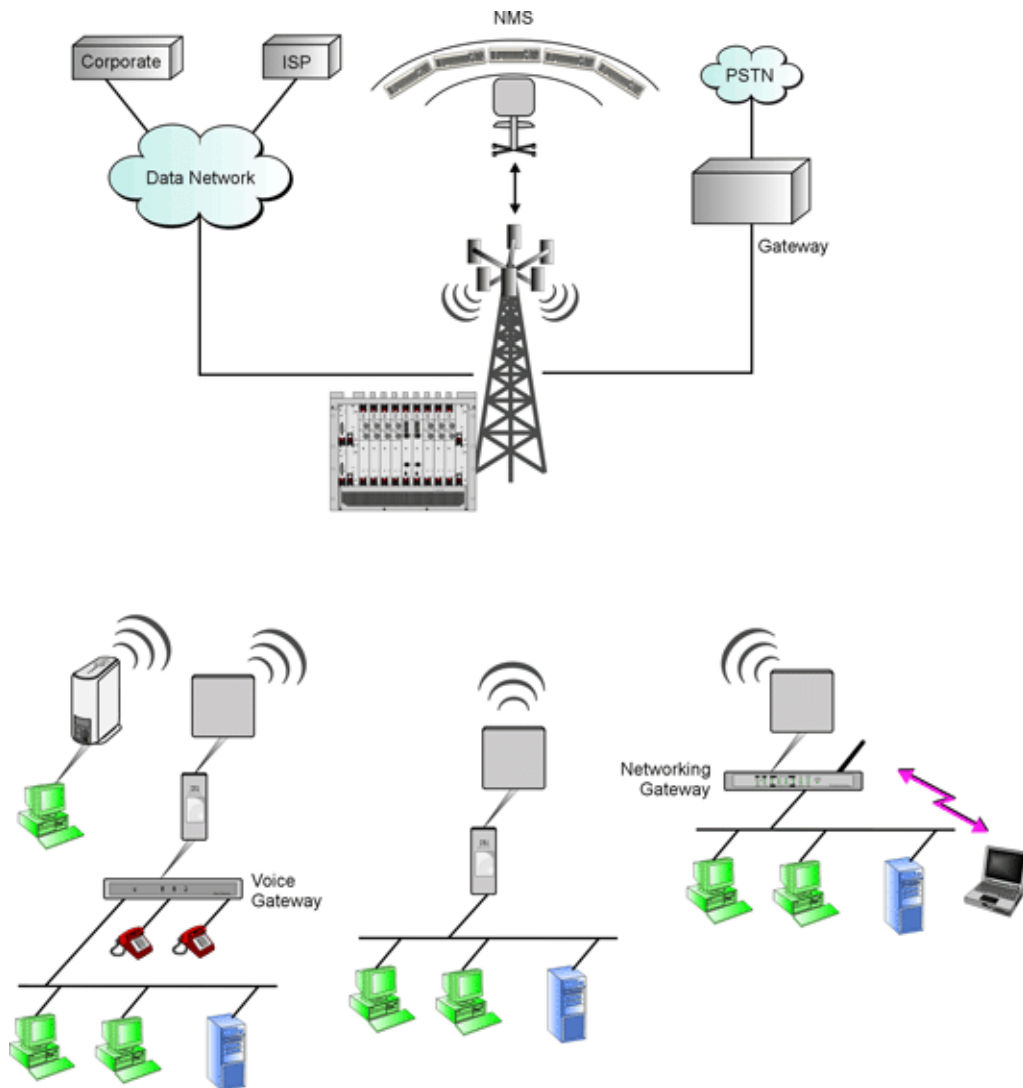
**Table 1-3: 3.6 GHz Frequency Bands**

Series (band)	Duplex Separation	Uplink Frequency	Downlink Frequency
3.6a	-100 MHz	3600 to 3653.5 MHz	3700 to 3753.5 MHz
3.6b	-100 MHz	3646.5 to 3700 MHz	3746.5 to 3800 MHz

\* The 3.6 GHz CPE supports the full range. The Base Station's radio (ODU) supports either band 3.6a or band 3.6b.

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 Base Station Equipment

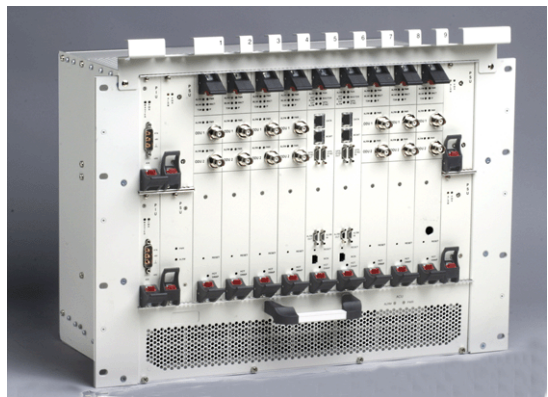
The Multi Carrier, High Power, Full Duplex Base Station provides all the functionality necessary to communicate with SUs and to connect to the backbone of the Service Provider.

The Base Station comprises the following elements:

### 1.2.1 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.

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

### 1.2.2 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.

### 1.2.3 Access Unit (AU-IDU)

The double Euro AU-IDU module contains the wireless IEEE 802.16-2004 based 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 can connect to one or two ODUs. The AU-IDU module connects to the AU ODUs via Intermediate Frequency (IF) cables carrying 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.

## 1.2.4 AU-ODU

The AU ODU is a 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 larger channels (e.g. 7/14 MHz) or using an IF multiplexer.

There are two versions of the AU-ODU:

- AU-ODU: Maximum output power of 28 dBm
- AU-ODU -HP (High Power ODU): Maximum output power of 34 dBm. The AU-ODU-HP is currently available in the 3.5 GHz bands (3.5a and 3.5b). Because of the higher power consumption, the AU-ODU-HP should be powered by an ODU Power Feeder.



### NOTE



For convenience, all references in this manual to AU-ODU are applicable also for AU-ODU-HP, unless explicitly stated otherwise.

## 1.2.5 Power Feeder

The ODU Power Feeder is used to provide power (-48 VDC) to AU-ODU-HP High Power ODUs. It transfers transparently all signals between the AU-IDU and the ODU, while injecting DC power received from an external source. Each ODU Power Feeder unit can serve up to four High Power ODUs. Up to three ODU Power Feeder units can be installed in a 1U high Power Feeder panel.



## 1.2.6 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.



## 1.2.7 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 1-4 displays the number of PSU modules (excluding redundant units) required for various Base Station configurations without NPU redundancy (one NPU):



**Table 1-4: PSU Requirements, Configurations with one NPU (excluding PSU redundancy)**

Number of AUs	Minimum Required Number of PSUs
1 - 2	1
3 - 6	2

Table 1-5 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 1-5: PSU Requirements, Configurations with two NPUs (excluding PSU redundancy)**

Number of AUs	Minimum Required Number of PSUs
1 - 5	2
6	3



## 1.2.8 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).

## 1.3 Networking Equipment

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

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

## 1.4 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 Base Station equipment as well as the Subscriber Units served by it. 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.

### 1.4.1 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
- Data Collection
- 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.

## 1.4.2 BreezeLITE™

Alvarion's BreezeLITE is an SNMP (Simple Network Management Protocol) application designed for on-line management of BreezeMAX system components. This utility simplifies the installation and maintenance of small size installations by easily enabling the change of settings or firmware upgrade for one Base Station/Micro Base Station at a time (including the managed device's components and associated SUs).

BreezeLITE allows accessing a wide array of monitoring and configuration options, including:

- Device Manager for Base Station and Micro Base Station, including NPU, AUs and SUs
- Unit status and current configuration verification
- Selected unit configuration modification

- Service Profiles verification and modification
- Service Provisioning
- Firmware upgrade for the NPU/Micro Base Station, AUs and SUs
- On-line performance data monitoring and statistics collection
- A special MS Excel Add-In for effective tabular and graphical display of collected data
- Support for http cut-through to Voice Gateways and Networking Gateways

## 1.5 Specifications

### 1.5.1 Radio

**Table 1-6: Radio Specifications**

Item	Description		
Frequency	Unit/Band	Uplink (MHz)	Downlink (MHz)
	AU-ODU-3.3e	3366-3385	3316-3335
	AU-ODU-3.3f	3381-3400	3331-3350
	AU-ODU-3.3g	3300-3324	3376-3400
	AU-ODU-3.5a	3399.5-3453.5	3499.5-3553.5
	AU-ODU-3.5b	3450-3500	3550-3600
	AU-ODU-3.6a	3600-3653.5	3700-3753.5
	AU-ODU-3.6b	3646.5-3700	3746.5-3800
Operation Mode	FDD, Full duplex		
Channel Bandwidth	<ul style="list-style-type: none"> <li>■ 3.5 MHz</li> <li>■ 1.75 MHz</li> </ul>		
Central Frequency Resolution	0.125 MHz		
Antenna Port (AU-ODU)	N-Type, 50 ohm		
Max. Input Power (at AU-ODU antenna port)	-50 dBm before saturation, -17 dBm before damage		
Output Power (at AU-ODU antenna port)	AU-ODU: 28 dBm +/-1 dB maximum. AU-ODU-HP: 34 dBm +/-1 dB maximum  Power control range: From 13 dBm to the maximum supported by the unit. In 3.6 GHz ODUs, the minimum power is 18 dBm.		
Modulation	OFDM modulation, 256 FFT points; BPSK, QPSK, QAM16, QAM64		
FEC	Convolutional Coding: 1/2, 2/3, 3/4		

**Table 1-6: Radio Specifications**

Item	Description				
		3.5 MHz bandwidth		1.75 MHz bandwidth	
Bit Rate and Typical Sensitivity (PER=1%)	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	5.65	-86
	QAM64 3/4	12.71	-82	6.35	-85

## 1.5.2 Base Station Antennas (Optional)

**Table 1-7: Base Station Antennas, Electrical Specifications**

Item	Description
BS ANT 60V/3.3-3.8	16.5 dBi minimum in the 3.3-3.8 GHz band, 60° AZ x 10° EL, vertical polarization, compliant with ESTI EN 302 085 V.1.1.2 (2001-02) CS2.
BS ANT 90V/3.3-3.8	15 dBi typical in the 3.3-3.8 GHz band, 90° AZ x 9° EL, vertical polarization, compliant with ESTI EN 302 085 V.1.1.2 (2001-02) CSI,CS2,CS3
BS ANT 120/3.5V	14 dBi typical in the 3.3-3.7 GHz band, 120° AZ x 6.7° EL, vertical polarization, compliant with ESTI EN 302 085 V.1.2.3 (2005-09) CS1.
BS ANT 60/3.5H	16 dBi typical in the 3.4-3.6 GHz band, 60° AZ x 9° EL, horizontal polarization, compliant with EN 302 085, V1.1.1 CS3
BS ANT 90/3.5H	14 dBi typical in the 3.4-3.6 GHz band, 85° AZ x 9° EL, horizontal polarization, compliant with EN 302 085, V1.1.1 CS3
Omni ANT 3.4-3.6	10 dBi typical in the 3.4-3.6 GHz band, 360° AZ x 9° EL, vertical polarization
Omni ANT 3.3-3.5	10 dBi typical in the 3.3-3.5 GHz band, 360° AZ x 9° EL, vertical polarization

## 1.5.3 AU-IDU to AU-ODU Communication

**Table 1-8: AU-IDU to AU-ODU Communication**

Item	Description
IF Frequency	<ul style="list-style-type: none"> <li>■ Tx: 240 MHz</li> <li>■ Rx: 140 MHz</li> </ul>
Ref Synchronization Frequency	64 MHz
Bi-Directional Control Frequency	14 MHz
IF cable Impedance	50 ohm
Maximum IF cable Attenuation	AU-ODU: 19 dB @ 240 MHz, 15 dB @ 140 MHz, 8 dB @ 64 MHz  AU-ODU-HP: 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	AU-ODU: 4.0 ohm  AU-ODU-HP: 1.5 ohm

## 1.5.4 Data Communication (Ethernet Ports)

**Table 1-9: Data Communication (Ethernet Ports)**

Item	Description	
Standard Compliance	IEEE 802.3 CSMA/CD	
Maximum Packet Size	1550 Bytes (including 4 CRC bytes and 4 VLAN tag bytes)	
Speed	Data Port	100/1000 Mbps, Full Duplex
	Management Port	10/100 Mbps, Half/Full Duplex with Auto Negotiation

## 1.5.5 Configuration and Management

**Table 1-10: Configuration and Management**

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



## 1.5.6 Standards Compliance, General

**Table 1-11: Standards Compliance, General**

Type	Standard
EMC	ETSI EN 301 489-1
Safety	<ul style="list-style-type: none"> <li>■ EN 60950-1(CE)</li> <li>■ UL 60 950-1</li> </ul>
Environmental	ETS 300 019: <ul style="list-style-type: none"> <li>■ Part 2-1 T 1.2 &amp; part 2-2 T 2.3 for indoor &amp; outdoor</li> <li>■ Part 2-3 T 3.2 for indoor</li> <li>■ Part 2-4 T 4.1E for outdoor</li> </ul>
Radio	<ul style="list-style-type: none"> <li>■ ETSI EN 301 753 V.1.1.1</li> <li>■ ETSI EN 301 021 V.1.6.1</li> </ul>

## 1.5.7 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

## 1.5.8 Services

**Table 1-13: Services**

Item	Description
Max number of Services per BST	4,095 (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	3999 - 3 x number of SUs (3 connections are reserved for each SU)
Max number of SUs per AU	510
Max number of AUs per BST	7
Max number of MAC addresses in Bridging Table	BST: 6,000 SU: 512 (Aging time is configurable. The default is 3 minutes for SU, 10 minutes for NPU)
Max number of VLANs per Service	16
Max number of VLANs per SU	16
Max number of VLANs (VPL IDs) per BST	1,024
Max number of concurrent voice calls per Voice/L2 Service	50
Max number of concurrent voice calls per AU	300

## 1.5.9 Physical and Electrical

### 1.5.9.1 Mechanical

**Table 1-14: Mechanical Specifications, 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
AU-ODU-HP	31.5 x 16 x 16	5.5
AVU	2U x 84HP x 16	1.7
Power Feeder panel	1U ETSI type panel	0.14
Power Feeder Module	15.7 x 14.6 x 3.17	

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

### 1.5.9.2 Electrical

**Table 1-15: Electrical Specifications, Base Station Equipment**

Unit	Details
Power Source	-40.5 to -60 VDC
Full Base station, including 1 ODU per AU	640W maximum for a fully equipped base station, including 6 ODUs (1 NPU, 6 AUs with 1 ODU per AU, 1+1 PIUs, 2+1 PSUs)
Full Base station, including 2 regular ODUs per AU	868W maximum for a fully equipped base station, including 12 regular ODUs (1 NPU, 6 AUs with 2 ODUs per AU, 1+1 PIUs, 2+1 PSUs)
Full Chassis (excluding ODUs)	412W maximum for a fully equipped chassis, excluding ODUs (1 NPU, 6 AU-IDUs, 1+1 PIUs, 2+1 PSUs)
Base station with 4 AUs, including 1 regular ODU per AU	470W maximum for a chassis with 4 AUs, including 4 regular ODUs (1 NPU, 4 AUs with 1 ODU per AU, 1+1 PIUs, 2+1 PSUs)
Base station with 4 AUs, including 2 regular ODUs per AU	621W maximum for a chassis with 4 AUs, including 8 ODUs (1 NPU, 4 AUs with 2 ODUs per AU, 1+1 PIUs, 2+1 PSUs)
Chassis with 4 AUs (excluding ODUs)	317W maximum for a chassis with 4 AUs, excluding ODUs (1 NPU, 4 AU-IDUs, 1+1 PIUs, 2+1 PSUs)

**Table 1-15: Electrical Specifications, Base Station Equipment**

Unit	Details
PIU	16W maximum (active PIU)
PSU	200W maximum output power Efficiency: 80% minimum
NPU	65W maximum, 44W typical
AU-IDU	38W maximum, 27W typical
AU-ODU	38W maximum, 33W typical
AU-ODU-HP	95W maximum, 70W typical
ODU Power Feeder	Power Source: -40.5 to -60 VDC Power Dissipation: 2W per channel
AVU	24W maximum, 23W typical

### 1.5.9.3 Connectors

**Table 1-16: Connectors, 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
	ALRM IN	9-pin micro D-Type jack
	ALRM 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, AU-ODU-HP	IF	TNC jack, lightning protected
	ANT	N-Type jack, 50 ohm, lightning protected

**Table 1-16: Connectors, Base Station Equipment**

Unit	Connector	Description
ODU Power Feeder	ODU 1 -4	4 x TNC jack, lightning protected
	IDU 1-4	4 x TNC jack, lightning protected
	Power	3 pin/20A D-Type male, Amphenol P/N

### 1.5.9.4 Base Station Antennas, Mechanical Specifications

**Table 1-17: Base Station Antennas, Mechanical Specifications**

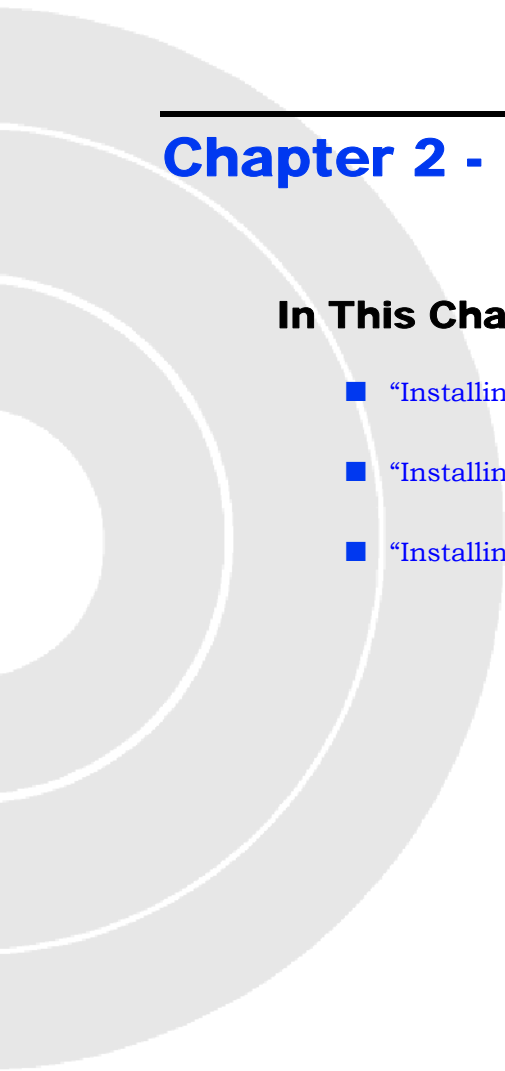
Unit	Description	Dimensions (cm)	Weight (kg)
BS ANT 60V/3.3-3.8	Mounting kit: 2" to 4" pole Connector: N-Type female	50 x 20 x 3	1.5
BS ANT 90V/3.3-3.8	Mounting kit: 2" to 4" pole Connector: N-Type female	53.6 x 36 x 3	2.3
BS ANT 120/3.5V	Mounting kit: 0.75" to 2" pole Mechanical tilt: 0° to -30°. Connector: N-Type female	76.2 x 8.3 x 7.6	2.0
BS ANT 60/3.5H	Mounting kit: 2" to 4" pole Connector: N-Type female	48 x 20 x 4	2
BS ANT 90/3.5H	Mounting kit: 2" to 4" pole Connector: N-Type female	60 x 25 x 5.5	2
Omni ANT 3.4-3.6	Mounting bracket: 30 to 53 mm pole. Connector: N-Type female	67.5 x 8 x 7.8	0.29
Omni ANT 3.3-3.5	Mounting bracket: 30 to 50 mm pole. Connector: N-Type female	67.5 x 8 x 7.8	0.29



---

## Chapter 2 - Installation Guidelines

### In This Chapter:

- [“Installing the AU-ODU” on page 24](#)
  - [“Installing the Base Station Equipment” on page 33](#)
  - [“Installing the ODU Power Feeder” on page 50](#)
- 

## 2.1 Installing the AU-ODU

The following sections describe how to install the AU-ODU, including pole mounting the ODU and connecting the cables.

### 2.1.1 AU-ODU Installation Requirements

#### 2.1.1.1 AU-ODU Packing List

- ODU: Any of the following:

**Table 2-1: AU-ODU Types**

Item	Description
BMAX-BST-AU-ODU-3.3d	AU-ODU operating in the 3.3d band
BMAX-BST-AU-ODU-3.3e	AU-ODU operating in the 3.3e band
BMAX-BST-AU-ODU-3.3f	AU-ODU operating in the 3.3f band
BMAX-BST-AU-ODU-3.3g	AU-ODU operating in the 3.3g band
BMAX-BST-AU-ODU-3.5a	AU-ODU operating in the 3.5a band
BMAX-BST-AU-ODU-3.5b	AU-ODU operating in the 3.5b band
BMAX-BST-AU-ODU-HP-3.5a	High Power AU-ODU operating in the 3.5a band
BMAX-BST-AU-ODU-HP-3.5b	High Power AU-ODU operating in the 3.5b band
BMAX-BST-AU-ODU-3.6a	AU-ODU operating in the 3.6a band
BMAX-BST-AU-ODU-3.6b	AU-ODU operating in the 3.6b band

- Pole mounting kit

#### 2.1.1.2 Additional Installation Requirements

The following items are also required to install the ODU:

- IF cable with two TNC connectors\* (see [Section 2.1.3](#) for details on IF cable types and length).
- Antenna\* and RF cable\* for connecting the antenna to the AU-ODU.
- Grounding cable with an appropriate termination.



- Installation tools and materials, including appropriate means (e.g. a 1" to 4" pole) for installing the AU-ODU (and antenna).

**NOTE**

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

## 2.1.2 Guidelines for Positioning the AU-ODU

This section provides key guidelines for selecting the optimal installation locations for the AU-ODU and its antenna.

**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 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 ODU should be installed as close as possible to the antenna.

## 2.1.3 IF Cables

The AU-ODU is connected to the AU-IDU (or to the Power Feeder) 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 2-2](#).

**Table 2-2: 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	AU-ODU: 19 dB @ 240 MHz, 15 dB @ 140 MHz, 8 dB @ 64 MHz AU-ODU-HP: 19 dB @ 240 MHz, 15 dB @ 140 MHz, 8 dB @ 64 MHz
Maximum IF cable DC Resistance	AU-ODU: 4.0 ohm AU-ODU-HP: 1.5 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 2-3](#) provides details on maximum length for some popular cables.

**Table 2-3: Maximum IF Cable Length (Double Shielded Cables)**

Cable	Maximum Length for AU-ODU	Maximum Length for AU-ODU-HP
LMR-195	80 meters	30 meters
LMR-240	150 meters	60 meters
LMR-400	250 meters	150 meters

### 2.1.4 Pole Mounting the ODU

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

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

### 2.1.4.1 Pole Mounting the Regular AU-ODU Using Clamps

Figure 2-1 illustrates the method of mounting a regular AU-ODU on a pole, using the clamps and threaded rods.

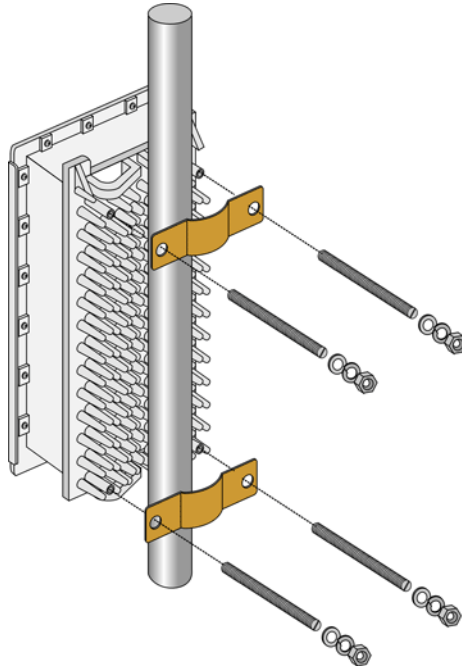


Figure 2-1: AU-ODU Pole Installation Using Special Clamps



#### NOTE

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

### 2.1.4.2 Pole Mounting the Regular AU-ODU Using Metal Bands

Figure 2-2 illustrates the method of mounting a regular AU-ODU on a pole, using metal bands.

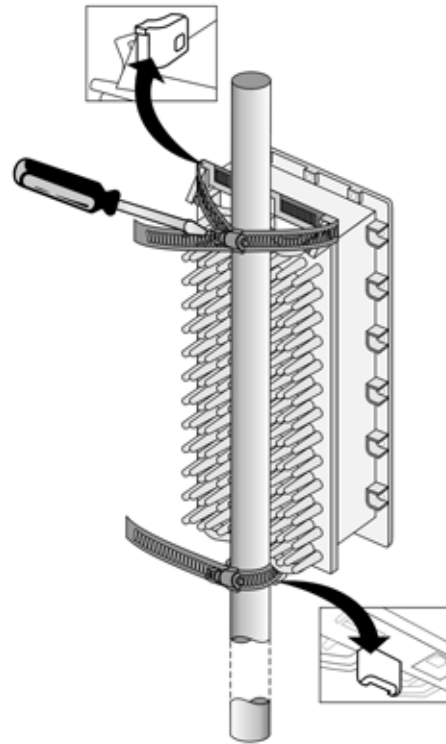


Figure 2-2: AU-ODU Pole Installation Using Metal Band

### 2.1.4.3 Pole Mounting the AU-ODU-HP Using Clamps

Figure 2-3 illustrates the method of mounting a High Power AU-ODU-HP on a pole, using the clamps and threaded rods.

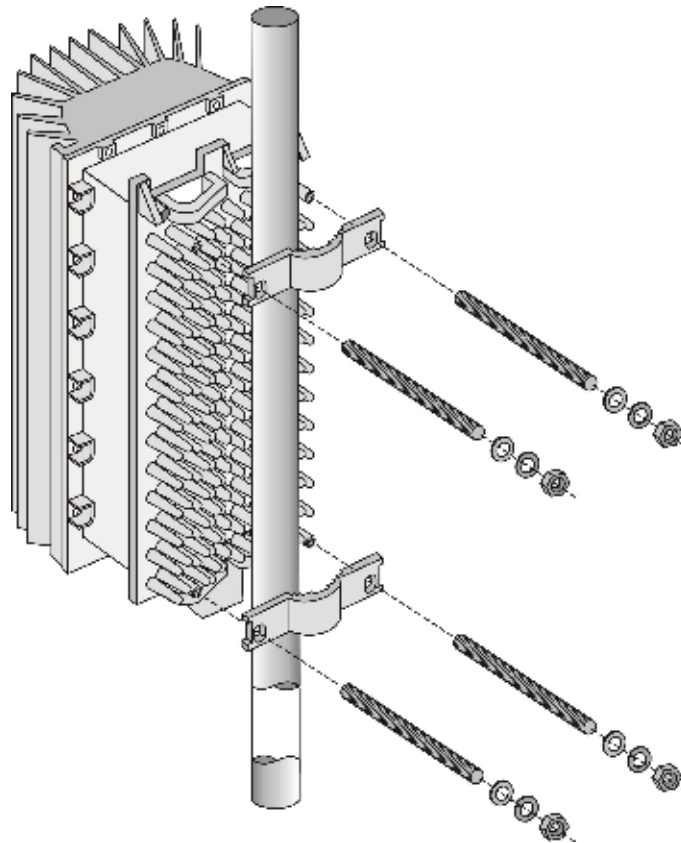


Figure 2-3: AU-ODU-HP Pole Installation Using Special Clamps



#### NOTE

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

### 2.1.4.4 Pole Mounting the AU-ODU-HP Using Metal Bands

Figure 2-4 illustrates the method of mounting a High Power AU-ODU-HP on a pole, using metal bands.

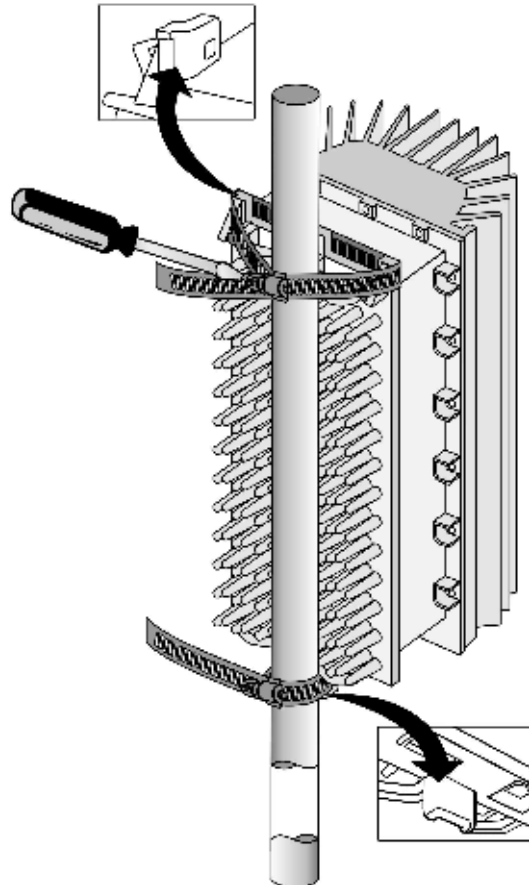


Figure 2-4: AU-ODU-HP Pole Installation Using Metal Band

## 2.1.5 AU-ODU

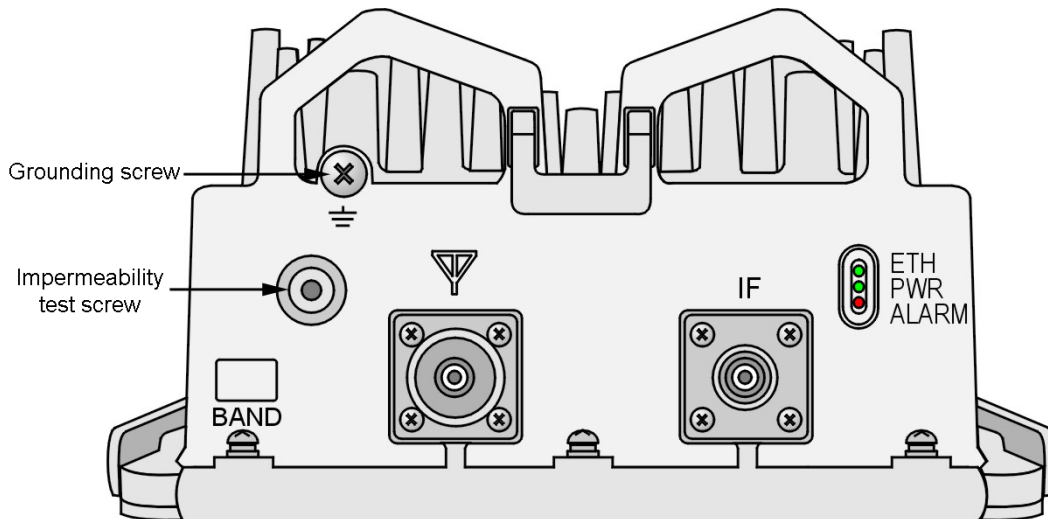


Figure 2-5: Bottom Panel of the AU-ODU

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

Table 2-5: AU-ODU Connectors

Name	Connector	Functionality
IF	TNC jack	Connection to the AU-IDU/Micro Base Station/ODU Power Feeder
ANT (ANT)	N-Type jack, 50 ohm	Connection to an external antenna
GND (GND)	Grounding Screw	Connection to ground (earth)

## 2.1.6 Connecting the Cables

### 2.1.6.1 Connecting the Grounding Cable

The Grounding screw (marked  $\text{⏏}$  ) 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.

### 2.1.6.2 Connecting the Antenna Cable



#### To connect the RF cable:

- 1 Connect one end of the coaxial RF cable to the RF connector (marked  $\text{Y}$  ) 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.

### 2.1.6.3 Connecting the 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/Power Feeder. See IF cable length limitation in [Section 2.1.3](#).
- 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.



## 2.2 Installing the 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

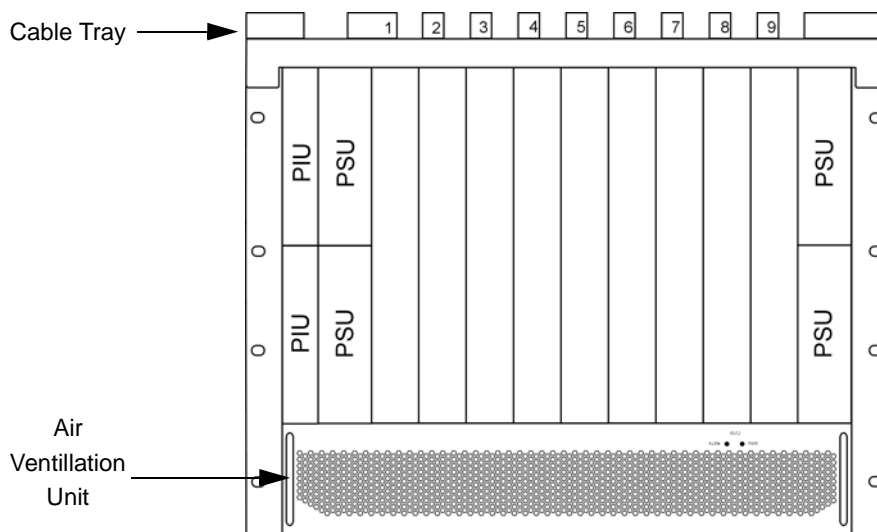
The maximum length of the Ethernet cable is 100m when operating at 100 Mbps and 70m when operating at 1 Gbps.

- 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 [Table 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 2-8](#) and [Table 2-9](#)). 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 worst-case power source requirements for the Base Station equipment (see also some examples in [Table 1-15](#)):

**Table 2-6: Power Requirements, Base Station Equipment**

Unit	Details
Power Source	-40.5 to -60 VDC
PIU	16W maximum (active PIU)
PSU	200W max output power Efficiency: 80% minimum
NPU	65W maximum
AU-IDU	38W maximum
AU-ODU	38W maximum
AU-ODU-HP	95W maximum
AVU	24W maximum



### NOTE

The PSU(s) do not supply power to the AU-ODUs. Regular AU-ODUs are powered directly from the power source via the PIU and the back plane. High Power AU-ODU HPs are powered from an ODU Power Feeder.

## 2.2.4 HOT SWAP Support

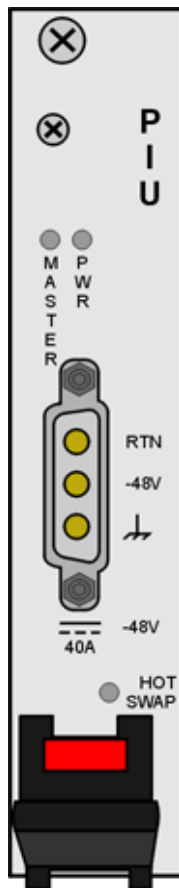
The NPU, AU-IDU and new PIU modules includes a blue HOT SWAP LED and a micro-switch in the injector/ejector handle to support hot-swap control. After releasing the ejector's button, the HOT SWAP LED should turn on, indicating that power to/from the back-panel is disconnected and the module can be removed safely. For more details refer to [Section 2.2.9](#).

## 2.2.5 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**

**NOTE**



The HOT SWAP blue LED does not exist in first generation PIUs.

**CAUTION**

In a first generation PIU (without HOT SWAP LED), 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.

In a second generation PIU (with HOT SWAP LED), disconnect power from the PIU module only after it is taken out from the chassis (or after the HOT SWAP LED is turned on). Connect power to the PIU only after it is fully inserted into the chassis.

**Table 2-7: PIU LEDs**

PWR and MASTER LEDs		PIU 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.
HOT SWAP		<p>Off: Power from the module to the chassis is not disconnected, the PIU is not ready for removal</p> <p>Blue: Power from the module to the chassis can be disconnected and the PIU can be safely removed</p> <p>For instructions on using the HOT SWAP handles refer to <a href="#">Section 2.2.9</a>.</p>

### 2.2.5.1 Preparing a Power Cable

A 2.5m DC power cable is supplied with each chassis. Additional DC cables can be ordered from Alvarion.



#### To prepare a 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.

## 2.2.6 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 2-8: PSU Requirements, Configurations with one NPU (excluding PSU redundancy)**

Number of AUs	Minimum Required Number of PSUs
1 - 2	1
3 - 6	2

**Table 2-9: 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. The regular AU-ODUs are powered directly from the power source via the PIU and the back plane. The High Power AU-ODU-HPs are powered from an ODU Power Feeder.



Figure 2-8: PSU Module Front Panel

Table 2-10: 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

### 2.2.7 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 can connect to AU-ODUs. If only a single AU ODU per AU-IDU is used, it should be connected to the ODU1 (Channel 1) connector.



Figure 2-9: AU-IDU Module Front Panel

Table 2-11: AU-IDU LEDs

Name	Description	Functionality
PWR	Power indication	<ul style="list-style-type: none"> <li>■ Off - AU-IDU is not powered</li> <li>■ Red - AU-IDU power supply failed (low power)</li> <li>■ Green - AU-IDU power is OK</li> </ul>



Table 2-11: AU-IDU LEDs

Name	Description	Functionality
ALARM	Alarm indication	<ul style="list-style-type: none"> <li>■ Off - AU-IDU is OK</li> <li>■ Red - AU-IDU failure</li> </ul>
WLINK	Wireless link status indication	<ul style="list-style-type: none"> <li>■ Off - No SU is associated</li> <li>■ Green - At least one SU is associated</li> </ul>
WACT	IDU transmission indication	<ul style="list-style-type: none"> <li>■ Off - No IDU transmission</li> <li>■ Green - IDU transmission OK</li> </ul>
SP	Spare	Not Used
IP	IP activity indication	<ul style="list-style-type: none"> <li>■ Off - No downlink (AU to SU) IP activity</li> <li>■ Green (blinking) - Downlink (AU to SU) IP activity</li> </ul>
ODU1/ODU2 PWR	IDU to ODU Power Indication	<ul style="list-style-type: none"> <li>■ Off - No IDU to ODU power output</li> <li>■ Red - IDU to ODU power output failed</li> <li>■ Green - IDU to ODU power output OK</li> </ul>
ODU1/ODU2 ALRM		<ul style="list-style-type: none"> <li>■ Off - IDU-ODU communication OK</li> <li>■ Red - IDU-ODU communication failure</li> </ul>
HOT SWAP	IDU readiness for hot swap removal	<ul style="list-style-type: none"> <li>■ Off: Power to the module is not disconnected, the AU-IDU is not ready for removal</li> <li>■ Blue: Power to the module can be disconnected and the AU-IDU can be safely removed</li> </ul> <p>For instructions on using the HOT SWAP handles refer to <a href="#">Section 2.2.9</a>.</p>

## 2.2.8 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 2-12: 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

**Table 2-12: NPU Connectors**

Name	Connector	Functionality
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 2-13: NPU LEDs**

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

Table 2-13: NPU LEDs

Name	Description	Functionality
HOT SWAP	NPU readiness for hot-swap removal	<ul style="list-style-type: none"> <li>■ Off: Power to the module is not disconnected, the NPU is not ready for removal</li> <li>■ Blue: Power to the module can be disconnected and the NPU can be safely removed</li> </ul> <p>For instructions on using the HOT SWAP handles refer to <a href="#">Section 2.2.9</a>.</p>

## 2.2.9 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. Second generation PIU modules also support hot-swap, as indicated by the HOT SWAP blue LED.

### 2.2.9.1 Inserting Modules



**To insert a module with hot-swap support (NPU, AU-IDU, PIU):**

- 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 if available)/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 (only in AU and NPU), indicating that the module is being powered up.

#### CAUTION



In a PIU with HOT SWAP LED, connect power to the PIU only after it is fully inserted into the chassis.

- 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 PSU or a PIU without HOT SWAP support:**

**CAUTION**

In a PIU without HOT SWAP LED, disconnect power from the PIU module before inserting it to the chassis.

- 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.

## 2.2.9.2 Ejecting Modules



**To eject a module with hot-swap support (NPU, AU-IDU, new PIU):**

- 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.

**CAUTION**

In a PIU with HOT SWAP LED, disconnect power from the PIU module only after it is taken out from the chassis (or after the HOT SWAP LED is turned on).

- 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 PSU or a PIU without HOT SWAP support:**



**CAUTION**

In a PIU without HOT SWAP LED, disconnect power from the PIU module before ejecting it 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.

- 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.

## 2.2.10 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.



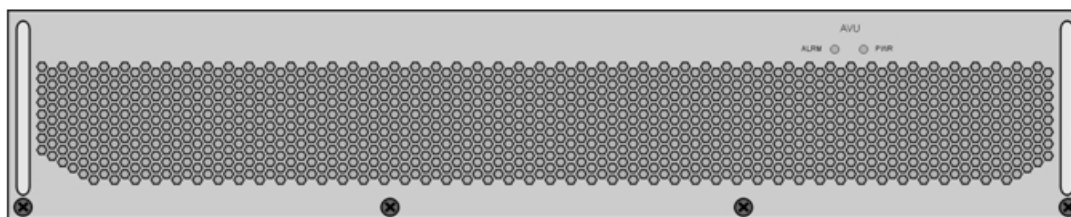
**To install the Base Station chassis and modules:**

- 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 [Section 2.2.9.1](#) 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 For regular AU-ODU(s): Connect the IF cable(s) (already connected at the other end to the AU-ODU(s)) to the ODU-1/ODU-2 connector(s) of the applicable AU-IDU module(s). If only a single AU-ODU per AU-IDU is used, connect the IF cable(s) to the appropriate ODU-1 connector(s). To avoid transmissions at undesired frequencies, verify that the frequency and bandwidth parameters are properly configured before connecting the IF cables.

For High Power AU-ODU-HP units: Refer to [Section 2.3.3](#).

## 2.2.11 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 2-14: 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:**

Release the 4 screws securing the AVU to the chassis.

Using the handle take out the faulty chassis.

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

### 2.2.11.1 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 [Section 4.5.2.6](#) 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 ODU Power Feeder

### 2.3.1 Installation Requirements

#### 2.3.1.1 Packing List

- A 19" panel (can hold up to three ODU Power Feeder modules).
- ODU Power Feeder module, including a DC power cable, four 0.5 meter IF cables and four screws.

#### 2.3.1.2 Additional Installation Requirements

- A grounding cable with appropriate terminations for connecting the unit's ground terminal to the rack or to a ground connection.
- For installation in a 21" ETSI rack: two 21" ETSI rack adapters
- Other installation tools and materials

## 2.3.2 The ODU Power Feeder

The ODU Power Feeder is used to provide power (-48 VDC) to AU-ODU-HP High Power ODUs. It transfers transparently all signals between the AU-IDU and the ODU, while injecting DC power received from an external source. Each ODU Power Feeder unit can serve up to four High Power ODUs. Up to three ODU Power Feeder units can be installed in a 1U high Power Feeder panel.

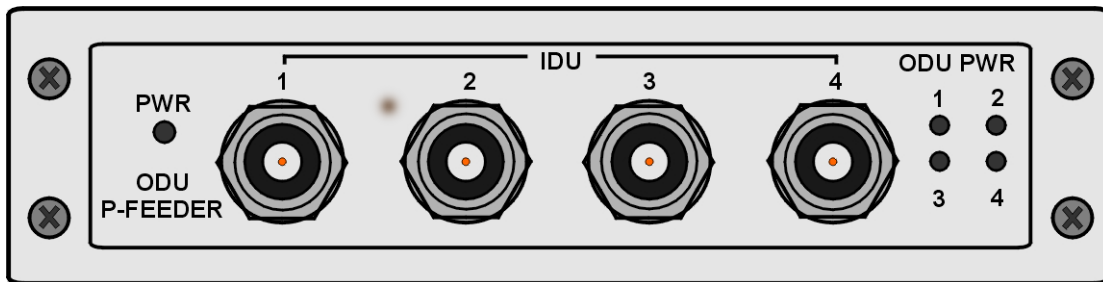


Figure 2-12: ODU Power Feeder Front Panel

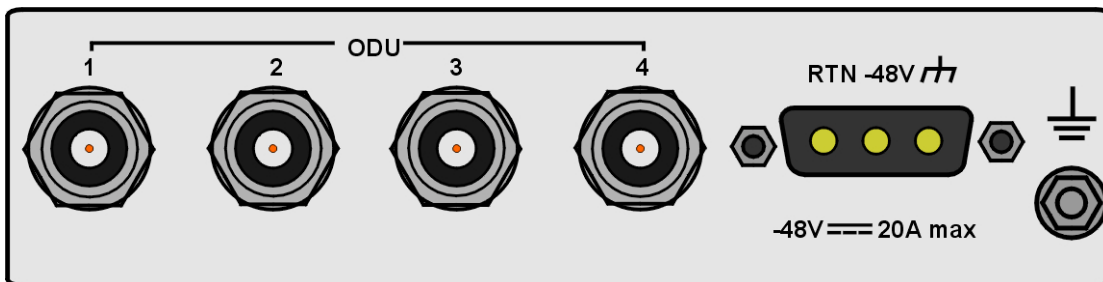


Figure 2-13: ODU Power Feeder Rear Panel

Table 2-15: ODU Power Feeder Connectors

Name	Connector	Functionality
IDU 1 - 4	4 x TNC jacks	Connection to ODU connectors of AU-IDUs/Micro Base Station
ODU 1 - 4	4 x TNC jacks	Connections to IF connectors of AU-ODU-HP units
-48V	3-pin D-Type power jack	Connection to DC power source
⏏ (GND)	Grounding Screw	Connection to ground (earth)

Table 2-16: ODU Power Feeder LEDs


Name	Description	Functionality
PWR	Input power indication	<ul style="list-style-type: none"> <li>■ Off - ODU Power Feeder is not powered</li> <li>■ Green - ODU Power Feeder power is OK</li> </ul>
ODU PWR 1 - 4	Output power indications	<ul style="list-style-type: none"> <li>■ Off - AU-ODU-HP is not connected</li> <li>■ Red - Power output problem (short or overload)</li> <li>■ Green - AU-ODU-HP is connected and powered</li> </ul>

### 2.3.2.1 Preparing a Power Cable

A 2.5m DC power cable is supplied with each ODU Power Feeder module. 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 ODU Power Feeder

The ODU Power Feeder should be installed as close as possible to the location where the IF cable(s) enters the building. The location of the ODU Power Feeder should take into account its connection to the power source and to the Base Station equipment.

**To install the ODU Power Feeder:**

- 1 The panel is supplied with blank covers. Release the nuts on the rear side of the panels to remove the blank cover(s) you want to replace with ODU Power Feeder module(s). Attach the ODU Power Feeder module(s) to the panel using the four screws supplied with each module.
- 2 Place the panel with the ODU Power Feeder module(s) on a shelf/desk or install it in a 19" cabinet, next to the Base Station equipment. For installation in a 21" cabinet, attach suitable ETSI rack adapters to the chassis.
- 3 Connect one end of a grounding cable to the grounding screw located on the rear panel of each ODU Power Feeder module and firmly tighten the grounding screw. Connect the opposite end of the grounding cable(s) to a ground (earth) connection or to the cabinet, if applicable.
- 4 Connect the IDU connector(s) to the appropriate ODU connector(s) of the AU-IDU(s) using the short (0.5 meter) IF cables supplied with the module.
- 5 Connect the power cord to the ODU Power Feeder's DC socket, located on the rear panel. Connect the other end of the power cord to the -48 VDC power source.
- 6 Connect the IF cable(s), that should already be connected at the other end to the AU ODU-HP(s), to the appropriate ODU connector(s). To avoid transmissions at undesired frequencies, verify that the frequency and bandwidth parameters are properly configured before connecting the IF cables.

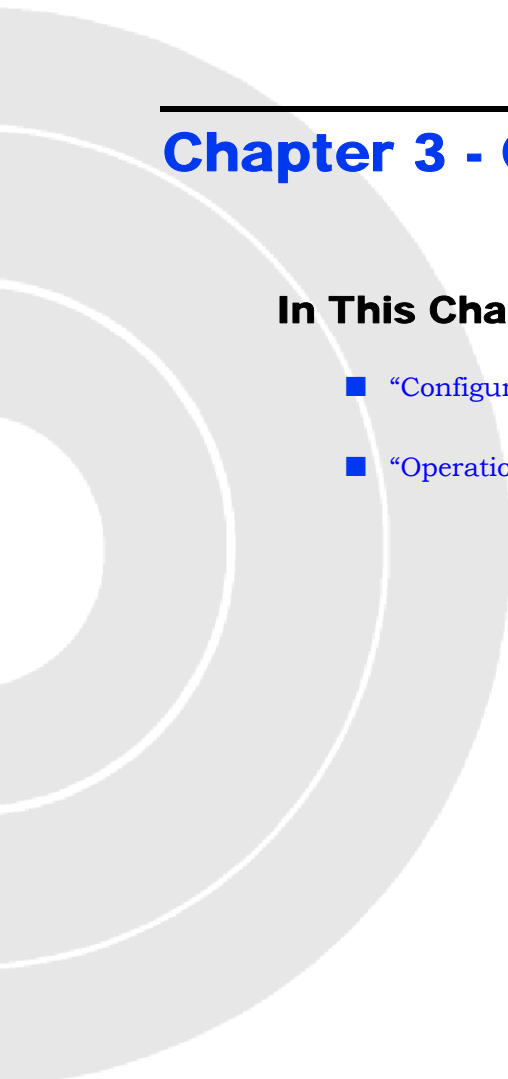




---

## Chapter 3 - Commissioning

### In This Chapter:

- “Configuring Basic Parameters of Base Station” on page 56
  - “Operation Verification” on page 58
- 

## 3.1 Configuring Basic Parameters of 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. 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](#) for detailed information on the applicable parameters.

**Table 3-1: Basic NPU Parameters**

Management Option	Parameters
MGMT port	<ul style="list-style-type: none"> <li>■ Management Port IP address</li> <li>■ Management Port Subnet Mask</li> <li>■ Management Port Gateway</li> <li>■ Management Port Destination Subnet</li> <li>■ Management Port Destination Subnet Mask</li> <li>■ Management Port Management Traffic Enable/Disable</li> </ul>
DATA port	<ul style="list-style-type: none"> <li>■ Data Port IP address</li> <li>■ Data Port Subnet Mask</li> <li>■ Data Port Gateway</li> <li>■ Data Port Management VLAN ID</li> <li>■ Data Port Management Traffic Enable/Disable</li> <li>■ Data Port Speed</li> </ul>
Authorized Managers (per manager)	<ul style="list-style-type: none"> <li>■ IP Address</li> <li>■ Send Traps</li> <li>■ Read Community</li> <li>■ Write Community</li> </ul>

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 OOB management via a router connected to the Management 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 Management port.

**NOTE**

It is highly recommended to use the Management port for local management only. Typically the port should be down (disconnected).

**CAUTION**

Do not configure the IP Address of the Management port to 0.0.0.0, as this will cause loss of management connectivity via the DATA port.

- Authorized Manager(s) must be configured properly to enable remote management using AlvariSTAR (or another SNMP based application).

**NOTE**

If no Authorized Manager is defined in the device, it can be managed using SNMP by any station. If at least one Authorized Manager is defined, the device can be managed only by a station whose parameters match a defined Authorized Manager.

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 serial 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 Installer password is "installer".

## 3.2 Operation Verification

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

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

## 3.2.2 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"> <li>■ Off - AU-IDU is not powered</li> <li>■ Red - AU-IDU power supply failed (low power)</li> <li>■ Green - AU-IDU power is OK</li> </ul>
ALARM	Alarm indication	<ul style="list-style-type: none"> <li>■ Off - AU-IDU is OK</li> <li>■ Red - AU-IDU failure</li> </ul>
WLINK	Wireless link status indication	<ul style="list-style-type: none"> <li>■ Off - No SU is associated</li> <li>■ Green - At least one SU is associated</li> </ul>
WACT	IDU transmission indication	<ul style="list-style-type: none"> <li>■ Off - No IDU transmission</li> <li>■ Green - IDU transmission OK</li> </ul>
SP	Spare	Not Used
IP	IP activity indication	<ul style="list-style-type: none"> <li>■ Off - No downlink (AU to SU) IP activity</li> <li>■ Green (blinking) - Downlink (AU to SU) IP activity</li> </ul>
ODU1/ODU2 PWR	IDU to ODU Power Indication	<ul style="list-style-type: none"> <li>■ Off - No IDU to ODU power output</li> <li>■ Red - IDU to ODU power output failed</li> <li>■ Green - IDU to ODU power output OK</li> </ul>
ODU1/ODU2 ALRM	IDU-ODU communication status	<ul style="list-style-type: none"> <li>■ Off - IDU-ODU communication OK</li> <li>■ Red - IDU-ODU communication failure</li> </ul>
HOT SWAP	IDU readiness for hot swap removal	<ul style="list-style-type: none"> <li>■ Off: Power to the module is not disconnected, the AU-IDU is not ready for removal</li> <li>■ Blue: Power to the module can be disconnected and the AU-IDU can be safely removed</li> </ul> <p>For instructions on using the HOT SWAP handles refer to <a href="#">Section 2.2.9</a>.</p>

Table 3-4: NPU LEDs

Name	Description	Functionality
PWR	Power indication	<ul style="list-style-type: none"> <li>■ Off - NPU is not powered</li> <li>■ Red - NPU power failure</li> <li>■ Green - NPU power is ok</li> </ul>
ALRM	NPU Alarm indication	<ul style="list-style-type: none"> <li>■ Off - NPU is OK</li> <li>■ Red - NPU failure</li> </ul>
BST ALRM	Base Station chassis alarm indication	<ul style="list-style-type: none"> <li>■ Off - All Base Station modules are OK</li> <li>■ Red - Failure in one (or more) Base Station modules</li> </ul>
EXT ALRM	External alarm indication	<ul style="list-style-type: none"> <li>■ Off - No alarm received via the AL IN connector</li> <li>■ Red - Alarm received via the AL IN connector</li> </ul>
MASTER	Master/Slave (primary/secondary) operation indication	<ul style="list-style-type: none"> <li>■ Off - Secondary NPU (backup)</li> <li>■ Green - Primary NPU</li> </ul>
GPS/SYNC	GPS/IF clock synchronization functionality indication	<ul style="list-style-type: none"> <li>■ Off - GPS/IF clock synchronization is disabled</li> <li>■ Green - GPS/IF clock synchronization is enabled</li> </ul>
HOT SWAP	NPU readiness for hot-swap removal	<ul style="list-style-type: none"> <li>■ Off: Power to the module is not disconnected, the NPU is not ready for removal</li> <li>■ Blue: Power to the module can be disconnected and the NPU can be safely removed</li> </ul> <p>For instructions on using the HOT SWAP handles refer to <a href="#">Section 2.2.9</a>.</p>

**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
HOT SWAP		<p>Off: Power from the module to the chassis is not disconnected, the PIU is not ready for removal</p> <p>Blue: Power from the module to the chassis can be disconnected and the PIU can be safely removed</p> <p>For instructions on using the HOT SWAP handles refer to <a href="#">Section 2.2.9</a>.</p>

**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

### 3.2.3 ODU Power Feeder LEDs

To verify the correct operation of the ODU Power Feeder, examine the LED indicators located on the front panel of the unit. The following table lists the LEDs of the ODU Power Feeder and their associated indications.

**Table 3-8: ODU Power Feeder LEDs**

Name	Description	Functionality
PWR	Input power indication	<ul style="list-style-type: none"> <li>■ Off - ODU Power Feeder is not powered</li> <li>■ Green - ODU Power Feeder power is OK</li> </ul>
ODU PWR 1 - 4	Output power indications	<ul style="list-style-type: none"> <li>■ Off - AU-ODU-HP is not connected</li> <li>■ Red - Power output problem (short or overload)</li> <li>■ Green - AU-ODU-HP is connected and powered</li> </ul>

### 3.2.4 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.

---

## Chapter 4 - Operation and Administration

### In This Chapter:

- “BreezeMAX System Management” on page 64
- “The Monitor Program” on page 66
- “The NPU's Main Menu” on page 70
- “Base Station Menu” on page 72
- “NPU Menu” on page 81
- “Radio Cluster Menu” on page 98
- “ODU Menu” on page 101
- “AU Menu” on page 106
- “SU Menu” on page 120
- “Services Menu” on page 137
- “NPU Parameters Summary” on page 178

## 4.1 BreezeMAX System Management

All BreezeMAX system components associated with a 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.

### NOTE



The SU can also be managed directly from its Ethernet port using the Installer Monitor program or the built-in Web Server. These options are 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.

### NOTE



It is not possible to manage the Base Station via the wireless link (from the SU's side).

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.

### NOTE



To enable remote management of devices behind the SU, including Voice and Networking Gateways, IP connectivity with the managed device is needed. This is possible only 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 [Section 4.5.3](#).

## 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 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



There are 3 access levels, as described in [Section 4.2.2](#). The default password for each of the access levels is:

Access Level	Default Password
Administrator	admin
Installer	installer
Monitor	monitor



### 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



Following three unsuccessful login attempts (using incorrect passwords), the monitor program is blocked for 10 minutes.

If you forgot the Installer or Monitor password, the Administrator can login (with the Administrator password) and define a new password for Installer and/or Monitor access level.

If you forgot the Administrator 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.

- There are three access levels to the Monitor program. The available actions depend on the access level (password) used for accessing the program:
  - ◇ **Administrator:** Read/Write permissions for all parameters. The default password is admin.
  - ◇ **Installer:** Read-only permission for the Services menu, Read/Write permissions for all other options excluding the Change Password option. The default password is installer.
  - ◇ **Monitor:** Read-only permissions for all parameters. The default password is monitor.

- Each menu or submenu specifies the unit type (BreezeMAX/NPU), the IP address of the port used for accessing the Monitor program (when using the MON port, there is no IP address), the running SW version and a description of the menu.
- 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 NPU's Main Menu

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

- 1 - Base Station
- 2 - NPU
- 3 - Radio Cluster
- 4 - ODU
- 5 - AU
- 6 - SU
- 7 - Services
- X - Exit

### 4.3.1 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 [Section 4.4](#).

### 4.3.2 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 [Section 4.5](#).

### 4.3.3 Radio Cluster Menu

The Radio Cluster menu enables viewing the details of existing Radio Clusters, defining new Radio Clusters, updating the parameters of an existing Radio Cluster and deleting a Radio Cluster from the database. For details refer to [Section 4.6](#).

### 4.3.4 ODU Menu

The ODU menu enables viewing the status and configuration details of existing ODUs, configuring the parameters of new ODUs including pre-configuration of ODUs that are not yet installed, updating the parameters of existing ODUs and deleting ODUs from the database. For details refer to [Section 4.7](#).

### 4.3.5 AU Menu

The AU menu enables configuring the 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 [Section 4.8](#).

### 4.3.6 SU Menu

The SU menu enables viewing summary information of all relevant SUs, configuring the parameters of a selected SU and defining new SUs. It also enables managing a selected SU's SW versions and viewing its current status, configuration and performance information. For details refer to [Section 4.9](#).

### 4.3.7 Services Menu

The Service menu enables viewing, updating and adding service profiles and subscribers, and allocating services to subscribers. It also enables viewing and updating filtering rules and the MAC Address Deny List. For details refer to [Section 4.10](#).

### 4.3.8 Exit

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

## 4.4 Base Station Menu

The Base Station menu includes the following options:

- Show
- Configuration
- Alarms and Traps
- Licenses

### 4.4.1 Show

Select this option to view the current value/selected option of configurable parameters. Refer to [Section 4.4.2](#) for more details on these parameters. In addition, some general status information is displayed, as follows:

- Configurable Parameters:
  - ◇ Device Name
  - ◇ Device Location
  - ◇ ATPC Status
  - ◇ Optimal Uplink RSSI (dBm)
  - ◇ Operator ID
  - ◇ Cell ID
- Status Information:
  - ◇ Slots status, displaying for each slot (1-9) the following:
    - Installed module type (or "Not Installed" for an empty slot)
    - Operational status (OK/Fault) of an installed module
  - ◇ Operational status (OK/Fault) of the AVU module
  - ◇ PIU slots status, displaying for each PIU slot:
    - Mode: Master, Redundant or Not Installed



- Operational status (OK/Fault) of an installed module
- ◇ PSU slots table, displaying the status of each slot: Not installed, OK or Fault.

#### ■ Licenses Status

- ◇ CPEs License Bank status
- ◇ Base Station License Status

For details refer to [Section 4.4.4](#).

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 4-1: Base Station Chassis Slot Assignment**

## 4.4.2 Configuration

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

### 4.4.2.1 Device Name

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

The device name consists of up to 255 printable characters.

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

### 4.4.2.2 Device Location

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

The location name consists of up to 255 printable characters.

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

### 4.4.2.3 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-ODU at an optimal level. The algorithm is managed by the AU and optimal values are calculated separately for each SU based on the actual level at which it is received by the AU-ODU. MAP messages transmitted to the SUs include information on the estimated up/down power level change required to achieve optimal transmit power level.

The ATPC menu enables viewing/updating the following parameters for all AUs:

#### 4.4.2.3.1 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 Base Station.

The default is Enable.



#### NOTE

The ATPC algorithm should always be enabled. The option to disable it is available to support certain tests. After each reset, the Base Station boots with the ATPC enabled, disregarding its status before the device was reset.

#### 4.4.2.3.2 Optimal Uplink RSSI

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

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

The default is -69 dBm.

### 4.4.2.4 Cell Parameters

The Cell parameters provide a unique identifier for the Base Station, and they are common to all AUs in the Base Station. Updated Cell parameters are applied for each AU after resetting the AU (or after resetting the NPU, which causes reset of all AUs). The Cell menu enables viewing/updating the following parameters:

#### 4.4.2.4.1 Operator ID

A unique identifier of the network. The same Operator ID must be defined for all Base Stations/Micro Base Stations in the network, and it should not be used by any Base Station/Micro Base Station belonging to another network in the same area.

The Operator ID consists of 3 groups of up to three digits each, where the range for each group is 0 to 255.

The default Operator ID is 186.190.0.

Changes in the value configured for the Operator ID are applied only after reset.

#### **4.4.2.4.2 Cell ID**

A unique identifier of Base Station. The same Cell ID should not be used by any other Base Station/Micro Base Station belonging to the network.

The Cell ID consists of 2 groups of up to three digits each, where the range for each group is 0 to 255.

The default Operator ID is 0.250.

Changes in the value configured for the Cell ID are applied only after reset.

### **4.4.3 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

#### **4.4.3.1 Show Active Alarms**

Select to view the currently active alarms. For more details on active alarms refer to the Traps and Alarms document.

#### **4.4.3.2 Traps Display Filter**

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

##### **4.4.3.2.1 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.

#### 4.4.3.2 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.

#### 4.4.3.3 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 the Traps and Alarms document.

#### 4.4.3.4 Trap Configuration

The Trap Configuration menu enables viewing current parameters of all traps and updating the parameters of a selected trap. It also enables viewing traps with modified parameters (different from the default) and restoring the configuration of all modified traps to their default values.

The available options are:

- Show Trap Status
- Admin Status
- Severity
- Suppression Interval

##### 4.4.3.4.1 Show Traps Status

Select this option to view a list of all traps and their parameters. For each trap, the following details are displayed:

- Trap ID
- Name
- Admin Status (the default Admin Status for all traps is Enabled)

- Default Severity
- Current Severity
- Suppression Interval (in seconds. The default Suppression Interval is 0, which means no suppression)

#### 4.4.3.4.2 Admin Status

The Admin Status menu enables viewing a list of all traps with Admin Status Disabled, updating the Admin Status of a selected trap and restoring the Admin Status of all traps to the default Enabled status. The Admin Status menu includes the following options:

- **Show Disabled Traps List:** Displays all traps with Admin Status Disabled (the default Admin Status for all traps is Enabled).
- **Update:** Enables modifying the Admin Status of a selected trap.
- **Restore Defaults:** Enables restoring the Admin Status of all traps to Enable.

#### 4.4.3.4.3 Severity

The Severity menu enables viewing a list of all traps with Severity that differs from the default severity, updating the Severity of a selected trap and restoring the Severities of all traps to the default severities. The Severity menu includes the following options:

- **Show Traps with Modified Severity:** Displays all traps with Severity that differs from the default severity.
- **Update:** Enables modifying the Severity of a selected trap.
- **Restore Defaults:** Enables restoring the Severities of all traps to the default severities.

#### 4.4.3.4.4 Suppression Interval

The Suppression Interval is the minimum time between consecutive transmissions of the same trap. This parameter can be used to prevent excessive retransmissions of the same trap. The Suppression Interval menu enables viewing a list of all traps with Suppression Interval that differs from the default suppression interval, updating the Suppression Interval of a selected trap and

restoring the Suppression Intervals of all traps to the default value of 0 (no suppression).

The Severity menu includes the following options:

- **Show Traps with Modified Suppression Interval:** Displays all traps with Suppression Interval that differs from the default suppression interval, which is 0 (no suppression).
- **Update:** Enables modifying the Suppression Interval of a selected trap. The available range is from 0 to 86,400 (seconds). 0 means no suppression.
- **Restore Defaults:** Enables restoring the Suppression Intervals of all traps to the default value (0).

#### 4.4.4 Licenses

The License feature enables managing the license(s) granted to CPEs with limited capabilities (“L model” CPEs) as well as the general Base Station licenses. In an “L model” CPE, the overall throughput (the aggregate downlink and uplink MIR in all services allocated to subscribers behind the CPE) is limited to 2 Mbps. The Network Service Provider may purchase from Alvarion a bank of CPE unlimited bandwidth licenses, and allocate licenses to selected L model CPEs on a need basis (refer to [Section 4.9.6.3.9](#) for details on assigning a license to a selected CPE). Rather than granting licenses only to specific L model CPEs, The Network Service Provider may also purchase a Base Station unlimited bandwidth license to override the bandwidth limitations of all L model CPEs served by the Base Station. The various licenses (CPEs Unlimited Bandwidth Licenses Bank, Base Station Unlimited Bandwidth License for all CPEs) are supplied as files to be loaded to the Base Station using TFTP. A license file can be loaded only to the Base Station specified in the applicable order.

The Licenses menu enables viewing the current status of CPEs and Base Station Licenses. The available options are:

- Show CPEs License Bank Status
- Show Base Station Licenses
- Show Temporary Grace Licenses
- Show Grace Licenses

#### 4.4.4.1 Show CPEs License Bank Status

Select this option to view the current status of the CPEs Licenses Bank (if available). The displayed information includes:

- **License ID:** The relevant license type. In the current version only a BW (Band-Width) license type is available.
- **License Value:** The specific details of the relevant licenses. In the current version all BW licenses are Unlimited.
- **License Count:** The number of currently available licenses (balance). Each time a license is granted to a specific CPE, the License Count is decremented by one.

#### 4.4.4.2 Show Base Station Licenses

Select this option to view the current Base Station Licenses (if applicable). The displayed information includes the License ID and License Value for each applicable license. Currently, the applicable license that may be available is Unlimited Bandwidth for all CPEs (License ID = BW, License Value = Unlimited).

#### 4.4.4.3 Show Temporary Grace Licenses and Show Grace Licenses

The aggregate uplink and downlink MIR in all the services allocated to an L model CPE should not exceed 2 Mbps. If the aggregate MIR in the services assigned to such a CPE exceeds this limit, the Network Service Provider has a 30 days grace period. During the grace period the assigned services are provided to the CPE. At any time during the 30 days grace period the Network Service Operator can load to the CPE the required permanent license for unlimited bandwidth. If a license was not loaded during this grace period, the following will happen:

- During the first 3 days, defined as a temporary grace period, the Network Service Provider may change the services assigned to the CPE so that the aggregate MIR is no longer above 2 Mbps. The CPE will be removed from the list of Temporary Grace Licenses and will return to its previous status.
- After expiry of the 3 days temporary grace period, the CPE is moved to the Grace Licenses list. After expiry of the full 30 days grace period, the CPE is moved to a list of "Grace Period Expired" CPEs (even if during the grace period the services assigned to them were changed so that the aggregate MIR is no longer above 2 Mbps). A CPE that was moved to the Grace Period Expired list will remain in this list for 3 months. A CPE that is included in this list cannot be granted another grace period. Any attempt to assign to it a

service that will bring the aggregate MIR to a value above 2 Mbps will be rejected.

The Show Temporary Grace Licenses option displays a table that includes the MAC addresses of CPEs that are currently included in the Temporary Grace License list. For each CPE the displayed list includes also the License ID (only BW license is applicable in the current version) and the expiry date of the temporary grace period.

The Show Grace Licenses option displays a table that includes the MAC addresses of CPEs that are currently included in the Grace License list. For each CPE the displayed list includes also the License ID (only BW license is applicable in the current version) and the expiry date of the temporary grace period.



## 4.5 NPU Menu

The NPU menu includes the following options:

- Show
- Unit Control
- Configuration
- Performance Monitoring

Following is a detailed description of these options.

### 4.5.1 Show

Select this option to view the current value/selected option of configurable parameters. Refer to [Section 4.5.3](#) for more details on these parameters. In addition, some general status information is shown, as follows:

- General Status Information:
  - ◇ Serial Number
  - ◇ HW Version
  - ◇ HW Configuration
  - ◇ Temperature (Celsius)
  - ◇ Cumulative Power On Time (hours): The cumulative power-on time of the NPU since first power-up.
- Management Port Parameters and Status:
  - ◇ 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 (Up/Down)
- ◇ Management Port Management Traffic (Enabled/Disabled)
- Data Port Parameters and Status:
  - ◇ 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 (Up/Down)
  - ◇ Data Port Management Traffic (Enabled/Disabled)
- Authorized Managers (per manager) details:
  - ◇ 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

## 4.5.2 Unit Control

The Unit Control menu of the NPU enables changing the access Passwords and the Monitor Inactivity Timeout, resetting the NPU, reverting the Base Station and the NPU to the factory default configuration, 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

### 4.5.2.1 Change Password

For security and control reasons, the Change Password option is available only for users with Administration access rights, using the Administrator Password to access the program. The Change Password option enables defining the passwords for each of the three different access levels: Administrator, Installer and Monitor. After changing the password for a selected access level, you will be prompted to re-enter the new password for confirmation.



#### NOTE

For security reasons, the passwords do not change after performing the Set Factory Defaults operation. For the same reason, the passwords are not included in backup configuration files.

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

The default passwords are:

Table 4-2: Default Passwords

Access Level	Default Password
Administrator	admin
Installer	installer
Monitor	monitor

### 4.5.2.2 Reset Unit

Select this option to reset the NPU. 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 [Section 4.11](#) for information on which parameters are changeable in run time and which changes are applied only after reset.

### 4.5.2.3 Set Factory Defaults

Select this option to set the Base Station and NPU parameters (excluding the access Passwords) to their factory default values. Refer to [Section 4.11](#) 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 to their default values will disable remote management of the Base Station since this affects the IP and Ethernet parameters and will delete all Authorized Managers.

### 4.5.2.4 SW Version Control

The NPU can contain two SW versions:

- Main: Each time the NPU 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, 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. 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

#### 4.5.2.4.1 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

#### 4.5.2.4.2 Run from Shadow

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

#### 4.5.2.4.3 Set as Main

When the NPU 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.

### 4.5.2.5 Create Backup

The Create Backup option enables creating backup files of the 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 configuration (excluding Passwords and 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).
- Filtering: All the configurations of Filtering Rules, Interface Filtering and MAC Address Deny List.
- Traps Configuration: The configuration parameters for all traps.

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, 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
- Filtering: filtering.res
- Traps Configuration: traps\_config.res

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

The target NPU will decrypt the backup file, extract all the configuration files and databases and will store them, replacing existing files/databases. The NPU 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. The values of these parameters configured in the target NPU before the loading process, are maintained.

### 4.5.2.6 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 0 to 60 minutes. 0 means no inactivity timeout.

The default value is 10 minutes.

## 4.5.3 Configuration

The NPU 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. It also enables configuring per Telnet session the types of messages that will be displayed upon occurrence of various events.

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.



#### NOTE

It is highly recommended to use the Management port for local management only. Typically the port should be down (disconnected).

- 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
- Voice
- Debug Stream

### 4.5.3.1 Management Port Parameters

These parameters define the IP parameters for the Management (MGMT) port connecting the base station to the backbone.

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

#### 4.5.3.1.1 Management Port IP Address

The IP address of the Management port.



The default is 10.0.0.1.



#### CAUTION

Do not configure the IP Address of the Management port to 0.0.0.0, as this will cause loss of management connectivity via the DATA port.

#### 4.5.3.1.2 Management Port Subnet Mask

The Subnet mask of the Management port.

The default is 255.255.255.0.



#### NOTE

The local subnet of the Management port (defined by the Management Port IP Address and Management Port Subnet Mask parameters), must differ from the local subnet of the Data port (defined by the Data Port IP Address and Data Port Subnet Mask parameters) and from the subnet that is used as the Static Route for remote management via the Management port (defined by the Management Port Dest Subnet and Management Port Dest Subnet Mask parameters).

#### 4.5.3.1.3 Management Port Gateway

The Gateway IP address of the Management port.

The default is 0.0.0.0.

#### 4.5.3.1.4 Management Port Dest Subnet and Management Port Dest Subnet Mask

The Destination Subnet parameters define a Static Route, which is an IP subnet of stations that can manage the device when connected via a router to the Management port. The Static Route is applicable only when remote management is enabled for both the Management and Data ports (i.e., when both Management Port Management Traffic Enable/Disable and Data Port Management Traffic Enable/Disable parameters are set to Enable).

The default is 0.0.0.0. for both parameters (meaning no Static Route).



#### NOTE

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

The subnet that is used as the Static Route for remote management via the Management port (defined by the Management Port Dest Subnet and Management Port Dest Subnet Mask parameters) must differ from the local subnet of the Management port (defined by the Management Port IP Address and Management Port Subnet Mask parameters) and from the local subnet of the Data port (defined by the Data Port IP Address and Data Port Subnet Mask parameters).

#### 4.5.3.1.5 Management Port Management Traffic Enable/Disable

The Management Port Management Traffic Enable/Disable parameter allows enabling/disabling remote management traffic via a router connected to the Management port. This parameter does not affect management traffic via the local subnet defined by the Management Port IP Address and Management Port Subnet Mask.

If remote management for the Management port is disabled, then the unit can be managed by any PC on any of the following subnets (provided the PC is defined as an Authorized Manager):

- A** The local subnet of the Management port (defined by the Management Port IP Address and Management Port Subnet Mask parameters).
- B** The local subnet of the Data port (defined by the Data Port IP Address and Data Port Subnet Mask parameters).
- C** Any subnet reachable via the default Gateway of the Data port (if Data Port Gateway is defined).

If remote management is enabled for both the Data Port and the Management port, then the unit can be managed by any PC on any of the following subnets (provided the PC is defined as an Authorized Manager):

- A** The local subnet of the Management port (defined by the Management Port IP Address and Management Port Subnet Mask parameters).
- B** The local subnet of the Data port (defined by the Data Port IP Address and Data Port Subnet Mask parameters).
- C** Any subnet reachable via the default Gateway of the Data port (if Data Port Gateway is defined).
- D** The Static Route subnet (defined by the Management Port Dest Subnet and Management Port Dest Subnet Mask parameters) reachable via the Gateway of the Management port.

#### NOTE



To prevent the undesired situation where remote management traffic is unintentionally disabled in both the Management 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.

#### 4.5.3.2 Data Port Parameters

These parameters define the IP and Ethernet parameters for the Data (DATA) port connecting the base station to the backbone.

#### 4.5.3.2.1 Data Port IP Address

The IP address of the Data port.

The default is 1.1.1.3.

#### 4.5.3.2.2 Data Port Subnet Mask

The subnet mask of the Data port.

The default is 255.255.255.0.



#### NOTE

The local subnet of the Data port (defined by the Data Port IP Address and Data Port Subnet Mask parameters), must differ from the local subnet of the Management port (defined by the Management Port IP Address and Management Port Subnet Mask parameters) and from the subnet that is used as the Static Route for remote management via the Management port (defined by the Management Port Dest Subnet and Management Port Dest Subnet Mask parameters).

#### 4.5.3.2.3 Data Port Gateway

The IP address of the default Gateway for the Data port.

The default is 0.0.0.0.

#### 4.5.3.2.4 Data Port Management VLAN

This parameter defines the VLAN ID for management frames via the Data port. If a value from 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).

#### 4.5.3.2.5 Data Port Speed

The speed of the Data port's Ethernet interface that operates always in full duplex mode. Auto negotiation is not supported.

The available options are 100 Mbps and 1 Gbps.

The default speed is 100 Mbps.

#### 4.5.3.2.6 Data Port Management Traffic Enable/Disable

The Data Port Management Traffic Enable/Disable parameter allows enabling/disabling remote management traffic via a router connected to the DATA port. This parameter does not affect management traffic via the local subnet defined by the Data Port IP Address and Data Port Subnet Mask.

If remote management for the Data port is disabled, then the unit can be managed by any PC on any of the following subnets (provided the PC is defined as an Authorized Manager):

- A** The local subnet of the Management port (defined by the Management Port IP Address and Management Port Subnet Mask parameters).
- B** The local subnet of the Data port (defined by the Data Port IP Address and Data Port Subnet Mask parameters).
- C** Any subnet reachable via the Gateway of the Management port (if defined). Note that in this case the Static Route (if defined) is ignored, and the defined Gateway becomes the default Gateway, enabling remote management by any PC reachable via the Gateway.

If remote management is enabled for both the Data Port and the Management port, then the unit can be managed by any PC on any of the following subnets (provided the PC is defined as an Authorized Manager):

- A** The local subnet of the Management port (defined by the Management Port IP Address and Management Port Subnet Mask parameters).
- B** The local subnet of the Data port (defined by the Data Port IP Address and Data Port Subnet Mask parameters).
- C** Any subnet reachable via the default Gateway of the Data port (if Data Port Gateway is defined).
- D** The remote Static Route subnet (defined by the Management Port Dest Subnet and Management Port Dest Subnet Mask parameters) reachable via the Gateway of the Management port.

#### NOTE



To prevent the undesired situation where remote management traffic is unintentionally disabled in both the Management 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.

### 4.5.3.3 Authorized Managers

The Authorized Managers submenu enables defining the properties of management stations that are allowed to manage the Base Station using SNMP, including all its components and the SUs associated with it.



#### NOTE

If no Authorized Manager is defined in the device, it can be managed using SNMP by any station. If at least one Authorized Manager is defined, the device can be managed only by a station whose parameters match a defined Authorized Manager.

The Authorized Manager submenu includes the following options:

#### 4.5.3.3.1 Show All

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

#### 4.5.3.3.2 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.

#### 4.5.3.3.3 Add

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

##### 4.5.3.3.3.1 IP Address

The IP address of the Authorized Manager.

##### 4.5.3.3.3.2 Send Traps

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

##### 4.5.3.3.3.3 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.

##### 4.5.3.3.3.4 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.

### 4.5.3.4 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, or 0 for no aging.

The default is 10 minutes.

### 4.5.3.5 Voice

The Voice submenu enables configuring the DRAP TTL Retries parameter. This parameter sets the limit of TTL retries for gateways that support the DRAP protocol before concluding that the gateway is no longer active and removing it from the database. The TTL retry time (the maximum time between two consecutive Allocation Requests) is 255 seconds.

The range is from 1 to 100.

The default is 4.



#### NOTE

During SW download to a gateway, which may take up to almost 15 minutes under worst conditions, the DRAP protocol is not active. If the gateway is removed from the database before SW download is completed, the download process will fail. During SW download, the DRAP TTL Retries parameter should be set to its default value of 4 (equivalent to 17 minutes).

### 4.5.3.6 Debug Stream

The Debug stream submenu enables configuring the types of messages that will be displayed during the Telnet session upon the occurrence of various events. These messages are typically used for investigating various problem situations, and many of them are meaningful only to Alvarion's technicians. The DS Class Enable and DS Class Disable options can be used to enable or disable various classes of messages. The classes of messages that can be controlled include:

- ERR: Error messages that should not occur under regular conditions.
- SYS: Indication of important events and alarms.
- TRAP: Text messages displaying the information supplied by relevant traps.

The default for all classes is Disable.

**NOTE**

Enabling the display of selected classes is applicable only for the current Telnet session. These parameters affect only the session and are not stored in the device. Upon starting a new session, or after resetting the unit, all classes are disabled.

## 4.5.4 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

### 4.5.4.1 Data Port Counters

The Data Port option enables viewing or resetting the Data (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
  - ◇ Total Packets Received: The total number of packets received on the interface. Packets with errors are not counted.
  - ◇ Management Packets Forwarded: The total number of management packets (packets whose destination is the NPU, and broadcasts) received on the Data port and forwarded to the NPU's internal management.
  - ◇ Packets Forwarded to Slot 1: The total number of packets received from the Data port and forwarded by the NPU to AU Slot 1.
  - ◇ Packets Forwarded to Slot 2: The total number of packets received from the Data port and forwarded by the NPU to AU Slot 2.
  - ◇ Packets Forwarded to Slot 3: The total number of packets received from the Data port and forwarded by the NPU to AU Slot 3.

- ◇ Packets Forwarded to Slot 4: The total number of packets received from the Data port and forwarded by the NPU to AU Slot 4.
- ◇ Packets Forwarded to Slot 7: The total number of packets received from the Data port and forwarded by the NPU to AU Slot 7.
- ◇ Packets Forwarded to Slot 8: The total number of packets received from the Data port and forwarded by the NPU to AU Slot 8.
- ◇ Packets Forwarded to Slot 9: The total number of packets received from the Data port and forwarded by the NPU to AU Slot 9.
- ◇ Packets Discarded on Rx: Packets received from the Data port that were discarded due to switching and classification failures.

■ Data Port Tx Counters

- ◇ Total Packet Transmitted: The total number of packets transmitted to the interface. Packets with errors are not counted.
- ◇ Management Packets Submitted: The total number of management packets submitted by the NPU.
- ◇ Packets Submitted from Slot 1: The total number of packets received by the NPU from the AU in Slot 1 and submitted to the Data port.
- ◇ Packets Submitted from Slot 2: The total number of packets received by the NPU from the AU in Slot 2 and submitted to the Data port.
- ◇ Packets Submitted from Slot 3: The total number of packets received by the NPU from the AU in Slot 3 and submitted to the Data port.
- ◇ Packets Submitted from Slot 4: The total number of packets received by the NPU from the AU in Slot 4 and submitted to the Data port.
- ◇ Packets Submitted from Slot 7: The total number of packets received by the NPU from the AU in Slot 7 and submitted to the Data port.
- ◇ Packets Submitted from Slot 8: The total number of packets received by the NPU from the AU in Slot 8 and submitted to the Data port.
- ◇ Packets Submitted from Slot 9: The total number of packets received by the NPU from the AU in Slot 9 and submitted to the Data port.
- ◇ Packets Discarded on Tx: Always 0. Currently packets are not discarded on Tx.



#### 4.5.4.2 Management Port Counters

The Management Port option enables viewing or resetting the Management (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:

- Packets Received
- Packets Discarded on Rx
- Packets Transmitted
- Packets Discarded on Tx

#### 4.5.4.3 All Counters

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

## 4.6 Radio Cluster Menu

Radio Cluster is a logical entity used to describe and support management of the Base Station's elements associated with specific geographical sectors. A Radio Cluster represents one or several ODUs that serve (through their directional antennas) the same geographical sector. Up to a maximum of six Radio Clusters can be defined per Base Station, representing a cell coverage using 6 x 60 antennas.

The Radio Cluster(s) must be defined prior to defining the relevant ODU(s), AU(s) and AU Channel(s).

The Radio Cluster menu includes the following options:

- Show Summary
- Select
- Add

### 4.6.1 Show Summary

Select this option to view the current status of all defined Radio Clusters.

For each defined Radio Cluster, the display includes the following information:

- ID: Radio Cluster ID (1-6)
- Name: The string that is used as the descriptive name of the Radio Cluster.
- Location: The string that is used as the descriptive location of the Radio Cluster.
- Sector Heading: The direction (angle from the north) of the geographical sector.
- Sector Beam Width: The beam width of the antenna(s) used in the geographical sector.

### 4.6.2 Select

Use this option and select an already defined Radio Cluster to open the Radio Cluster # menu that will enable managing and configuring the selected Radio Cluster.

The selected Radio Cluster # menu includes the following options:

- **Show:** Select this option to view the current values defined for the selected Radio Cluster's parameters.
- **Update:** Select this option to update one or more of the selected Radio Cluster's parameters. For details on the configurable parameters Refer to [Section 4.6.4](#).
- **Delete:** Select this option to delete the selected Radio Cluster from the database.

### 4.6.3 Add

Select this option to define a new Radio Cluster. For details on the configurable parameters refer to [Section 4.6.4](#).

## 4.6.4 Radio Cluster Parameters

### 4.6.4.1 Radio Cluster ID

A number used to identify the Radio Cluster. The Radio Cluster ID is configurable only when adding a new Radio Cluster.

The available values range from 1 to 6.

### 4.6.4.2 Name

A string of up to 32 printable characters used as the descriptive name of the Radio Cluster. This is an optional descriptive parameter.

The default is an empty string.

### 4.6.4.3 Location

A string of up to 255 printable characters used to describe the location of the Radio Cluster. This is an optional descriptive parameter.

The default is the string defined as the Location parameter of the Base Station.

### 4.6.4.4 Sector Heading

The direction of the geographical sector, defined in degrees from the north. This is an optional descriptive parameter.

The values range is from 0 to 359 (degrees from north).

The default value is 0 (degrees from north).

#### **4.6.4.5 Sector Beam Width**

The beam width, in degrees, of the antenna(s) used in the geographical sector. This is an optional descriptive parameter.

The values range is from 0 to 359 (degrees).

The default value is 90 (degrees).

## 4.7 ODU Menu

The ODU(s) must be defined prior to defining the relevant AU(s) and AU Channel(s).

The ODU menu includes the following options:

- Show Summary
- Select
- Add

### 4.7.1 Show Summary

Select this option to view the current status of all defined Radio Clusters.

For each defined Radio Cluster, the display includes the following information:

- ID: ODU ID (1-24)
- Associated Radio Cluster: The ID (1-6) defined for the associated Radio Cluster.
- Tx Power: The defined Tx Power in dBm units.
- ODU Configured Band: The radio band configured for the ODU.
- Admin Status: Enabled or Disabled.

For details on the parameters refer to [Section 4.7.4](#).

Upon first power-up of the Base Station, 7 ODUs are defined automatically, with ODU IDs from 1 to 7. The parameters of these automatically created ODUs are:

- Associated Radio Cluster: NA
- Tx Power: 28 dBm
- ODU Configured Band: Not Defined
- Admin Status: Enabled

## 4.7.2 Select

Use this option and select an already defined ODU to open the ODU # menu that will enable managing and configuring the selected ODU.

The selected ODU # menu includes the following options:

### 4.7.2.1 Show

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

- ID
- Associated Radio Cluster
- Tx Power
- ODU Configured Band
- Admin Status
- Oper Status
- HC08 Version
- CPLD Version
- Serial Number
- Temperature (Celsius)
- HW Revision
- HW Configuration Description
- Max Tx Power: The maximum Tx Power supported by the ODU. This read-only parameter sets the upper limit for the Tx Power parameter.

### 4.7.2.2 Update

Select this option to update one or more of the selected ODU's parameters. For details on the configurable parameters refer to [Section 4.7.4](#).

### 4.7.2.3 Delete

Select this option to delete the selected ODU from the database.

### 4.7.3 Add

Select this option to define a new ODU. For details on the configurable parameters refer to [Section 4.7.4](#).

## 4.7.4 ODU Parameters

### 4.7.4.1 ODU ID

A number used to identify the ODU. The ODU ID is configurable only when adding a new ODU.

The available values range from 1 to 24.

### 4.7.4.2 Associated Radio Cluster

The ID of the associated Radio Cluster.

The available values range from 1 to 6. The value must be that of an already defined Radio Cluster.

### 4.7.4.3 Configured ODU Frequency Band

The Configured ODU Frequency Band will be modified through the use of Frequency Bands Configuration file (see [Section 4.7.5](#)).

The available values are the list numbers from the displayed list of available Frequency Bands.

The Configured ODU Frequency Band can be updated only if the ODU is not associated with any AU Channel, or if the Admin Status of the associated AU Channel is Disabled.

Compatibility between the Configured ODU Frequency Band and its actual band is verified by the AU upon trying to associate the ODU with a Channel. If the Configured ODU Frequency Band differs from the actual band supported by the ODU, a mismatch trap will be sent by the AU upon trying to associate it with a Channel and the association will be rejected.

### 4.7.4.4 Tx Power

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

The range is from 13 to 50 dBm using a 0.25 dBm resolution. In case the entered value is not compatible with the installed ODU, a trap will be issued. If the entered value is below the minimum supported by the ODU (currently applicable only for 3.6 GHz units where the minimum power is 18 dBm) the actual power will be set to the minimum supported by the unit. If the entered value is above the maximum supported by the ODU, the power will be changed to the maximum value supported by the ODU (28 dBm for a regular ODU, 34 dBm for a High Power ODU).

The default is 28 dBm.

#### 4.7.4.5 Admin Status

The transmit on/off status of the ODU.

The default option is Disabled.

### 4.7.5 Frequency Bands File and Frequency Bands Groups

The Frequency Bands Configuration file defines the characteristics of each of the frequency bands supported by the system. These characteristics include:

- Lowest Downlink Frequency
- Highest Downlink Frequency
- Step (resolution)
- Duplex Separation: the difference between downlink (Tx) and uplink (Rx) frequencies.
- Group ID: For certain bands, the relevant SU may use a frequency band that includes more than one of the discrete bands available for the ODU. The Group ID defines the Frequency Bands Group, which includes frequency bands that can be used by SUs served by the ODU using the selected band. The Frequency Bands Group defines also the range of frequencies that can be used by the relevant AU.

In the current release, the following Frequency Bands are supported:



**Table 4-3: Frequency Bands**

Frequency Band	Group (ID)	Downlink Frequency Range	Duplex Separation
3.3e	3.3GHz (2)	3316-3335 MHz	50 MHz
3.3f	3.3GHz (2)	3331-3350 MHz	50 MHz
3.3g	3.3GHz g (3)	3376-3400 MHz	-76 MHz
3.5a	3.5GHz (1)	3499.5-3553.5 MHz	-100 MHz
3.5b	3.5GHz (1)	3550-3600 MHz	-100 MHz
3.6a	3.6GHz (4)	3700-3753.5 MHz	-100 MHz
3.6b	3.6GHz (4)	3746.5-3800 MHz	-100 MHz

This mechanism allows adding new frequency bands without modifying the software by simply loading a new Frequency Bands File when the supporting hardware becomes available. The file will be either a part of the NPU's software or loaded later to the NPU, using an updated file obtained from Alvarion. The version of the current file and information on the supported bands is available in the NPU's Show menu.

## 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
- Configured SW File Name: The SW File configured in the NPU (together with the Configured Operation).
- Configured SW Version: The SW Version of the SW File configured in the NPU.
- Configured Operation: The operation to be performed with the Configured SW 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.
- Active Voice Calls: The number of currently active voice calls handled by the AU.

For more details on SW File/Version and Operation refer to [Section 4.8.4.2.3](#).

## 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 Status Parameters:

- ◇ IDU Serial Number
- ◇ IDU IF Card HW Revision
- ◇ IDU IF Card HW Configuration
- ◇ IDU Boot Version
- ◇ IDU Main Card HW Revision
- ◇ IDU Main Card HW Configuration
- ◇ IDU Temperature (Celsius)
- ◇ Cumulative Power On Time (hours)

■ SW Files and Versions:

- ◇ For an installed AU - details on the current SW files and versions:
  - Main SW File Name
  - Main SW Version
  - Shadow SW File Name
  - Shadow SW Version
  - Running From (Main or Shadow)
  - Configured SW File Name
  - Configured SW Version
  - Configured Operation

■ MAC Parameters:

- ◇ Base Station ID (Operator ID, Call ID, Sector ID)
- ◇ Operator ID (as defined in the Base Station-Cell menu)
- ◇ Cell ID (as defined in the Base Station-Cell menu)
- ◇ Sector ID
- ◇ ARQ Enable/Disable
- ◇ Maximum Cell Radius (km)

■ Multirate Parameters:

- ◇ Multirate Enable/Disable
- ◇ Uplink Basic Rate
- ◇ Downlink Basic Rate
- ATPC Parameters (as defined in the Base Station-Cell menu):
  - ◇ ATPC Enable/Disable
  - ◇ Optimal Uplink RSSI (dBm)
- Voice Parameters:
  - ◇ Maximum Number of Voice Calls
  - ◇ Active 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 [Section 4.11](#) 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 [Section 4.11](#) 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
- Multi Channel
- Multirate
- Voice Parameters

#### 4.8.4.3.1 MAC Parameters

The MAC menu enables viewing/updating the following parameters:

#### 4.8.4.3.1.1 ID Parameters

The Operator ID, Cell ID and Sector ID constitute together the Base Station ID, which is the unique identifier of the AU. An SU can be authenticated by the AU only if its defined parameters match the Base Station ID configured for the AU.

The Operator ID and Cell ID are defined for the Base Station (see [Section 4.4.2.4](#)) and are used by all AUs in the Base Station. In the AU's MAC Parameters menu they are available only in the Show option.

The Sector ID parameter consists of three digits in the range of 0 to 255.

The default Sector ID is 206.

Changes in Sector ID are applied only after reset.

#### 4.8.4.3.1.2 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.

#### 4.8.4.3.1.3 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 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  $N \cdot 10$  km and smaller than or equal to  $(N+1) \cdot 10$ .

#### 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 110 km. Use 10 km increments (10, 20, ..., 110).



The default is 20 km.

#### 4.8.4.3.2 **Phy Parameters**

The Phy menu enables viewing/updating the Bandwidth parameter:

##### 4.8.4.3.2.1 **Bandwidth**

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

The Admin Status of all Channels belonging to the same AU must be disabled to enable a configuration change in the Bandwidth parameter.

The available options are:

1 - 1.75 MHz

2 - 3.5 MHz

The default is 3.5 MHz.

#### 4.8.4.3.3 **Multi Channel Parameters**

Each AU can include up to 4 Channels with Channel IDs from 1 to 4, corresponding to up to 4 ODU connectors. In the current release only AUs with 2 Channels are available, corresponding to ODU 1 and ODU 2 connectors. Each channel can be connected to an ODU. The Multi Channel menu includes the following options:

- Show Summary
- Select

Following is a description of these options:

##### 4.8.4.3.3.1 **Show Summary**

Select this option to view the following information for each Channel:

- Channel (1-4)
- Associated ODU
- Downlink (Tx) Frequency (MHz)
- Uplink (Rx) Frequency (MHz): Applicable only to Channels associated with a defined ODU. Computed using the rules defined in the Frequency Bands Configuration File.

- Admin Status (Enabled/Disabled)
- Tx Power: Applicable only to Channels associated with a defined ODU. The Tx Power in dBm configured in the ODU.
- Associated Radio Cluster: The Associated Radio Cluster defined in the ODU.

Upon first power-up of the Base Station, the channels are defined automatically, as follows:

- Associated ODU: Channel 1 of all AUs is automatically associated with an ODU:

**Table 4-4: Automatic Association of Channel 1 Upon First Power-Up**

AU Slot ID	ODU ID
AU Slot 1	1
AU Slot 2	2
AU Slot 3	3
AU Slot 4	4
AU Slot 7	5
AU Slot 8	6
AU Slot 9	7

For all other Channels (2-4) the Associated ODU is NA.

- Downlink (Tx) Frequency (MHz): 3551.750
- Admin Status: Enabled for Channel 1, Disabled for all other Channels (2-4)

#### 4.8.4.3.3.2 Select

Use this option to select a Channel ID (1-4) to open the Channel # menu for viewing or updating the Channel's parameters. The configurable Channel parameters are:

- Associated ODU: An ODU ID (1-24) of an already defined ODU.
- Downlink (Tx) Frequency (MHz): The Tx frequency in MHz, which must be in accordance with the selected Bandwidth (see [Section 4.8.4.3.2.1](#)) and the rules defined in the Frequency Bands File for the frequency band selected as the

Configured ODU Frequency Band of the associated ODU (see [Section 4.7.4.3](#)). The help text (displayed upon clicking the Tab key) reflects the limitations imposed by these rules.

In addition, the following rules must be followed:

- 1 After configuring the Downlink Frequencies  $f_1$  for one of the AU's Channels, the Downlink Frequencies for other Channels of the same AU should be configured using increments of  $\pm 0.875$  MHz from the defined frequency:  $f_1 \pm (N \times 0.875)$ .
  - 2 The Downlink Frequencies of all Channels of the same AU should belong to the same Frequency Bands Group (see [Section 4.7.5](#)).
- Admin Status: The Admin Status must be disabled to enable changes in the Configured ODU Frequency Band of an associated ODU. If the Configured ODU Frequency Band differs from the actual band supported by the ODU, a mismatch trap will be sent by the AU upon trying to associate it with a Channel and the association will be rejected.

The Admin Status of all Channels belonging to the same AU must be disabled to enable a configuration change in the Bandwidth parameter.

The Show menu includes also the following read-only parameters:

- Tx Power: As configured in the Associated ODU.
- Associated Radio Cluster: As configured in the Associated ODU.
- Uplink (Rx) Frequency: Computed from the configured Downlink (Tx) Frequency according to the Duplex Separation of the applicable Frequency Band.
- Frequency Band: The Configured ODU Frequency Band. If there is a mismatch between the Configured ODU Frequency Band and its actual band, both values will be displayed.
- Operational Status

#### 4.8.4.3.4 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 taking into account also information received

from the served SUs. 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. This is also the rate to be used for downlink 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, 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 [Section 4.9.6.3.4.2](#)), which becomes available only when the Multirate algorithm is disabled in the AU, enables setting the Uplink Current Rate and the Downlink Current Rate to any of the values listed in [Figure 4-5](#).

The multirate algorithm chooses dynamically between 8 rates. These are also the rates that can be configured for the Basic 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

The Multirate menu enables viewing/updating the following parameters:

#### 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 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 [Figure 4-5](#).

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 [Figure 4-5](#).

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

#### 4.8.4.3.5 Voice Parameters

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

##### 4.8.4.3.5.1 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:

- Ports Counters
- Burst Error Rate Counters

### 4.8.5.1 Ports Counters

The Ports Counters option enables viewing or resetting the Back-Panel 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 Back-Panel port of the AU is the internal Ethernet port between the AU and the NPU.

The counters describe the traffic at the Back-Panel and Wireless ports, as follows:

**■ Back-Panel Port Counters**

- ◇ Data Bytes Received: The total number of data bytes received from the Back-panel (NPU). Management frames and frames with errors are not included.
- ◇ Data Bytes Discarded on Rx: The number of bytes in packets discarded due to communication errors between the AU and the NPU.
- ◇ Data Bytes Transmitted: The total number of data bytes transmitted to the Back-Panel (NPU). Management frames and frames with errors are not included.
- ◇ Data Bytes Discarded on Tx: This count is always 0 (No discards).

**■ Wireless Port Counters**

- ◇ Data Bytes Received: The total number of data bytes received from the Wireless link. MAC management frames and frames with errors are not included.
- ◇ Data Bytes Discarded on Rx: The number of bytes in packets received from the Wireless link and discarded due to MAC protocol receive errors, such as duplicate sequence number, wrong sequence number etc. (not CRC errors).
- ◇ Data Bytes Transmitted: The total number of data bytes transmitted to the Wireless link. MAC Management frames and frames with errors are not included.
- ◇ Data Bytes Discarded on Tx: The number of bytes in packets discarded due to congestion in the wireless medium.

- ◇ ARQ Enabled Bytes Transmitted: The number of bytes transmitted over BE and NRT connections. Applicable only if the ARQ mechanism is enabled.
- ◇ Bytes Retransmitted: The number of unacknowledged bytes that were retransmitted. Retransmissions are applicable only to BE and NRT connections provided the ARQ mechanism is enabled.
- ◇ Retransmission Rate (%): Retransmission Rate in percents is defined as:  
 $100 * (\text{Bytes Retransmitted}) / (\text{ARQ Enabled Bytes Transmitted})$ .

### 4.8.5.2 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 the uplink is the accumulated number since the last time the counters were reset. The downlink counters can be viewed in the applicable SU menu. For each rate the displayed information (for the uplink) 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 Type: BMAX CPE, PRO CPE, PRO-L CPE, Si CPE.
  - ◇ SU Status (Permanent or Temporary)
  - ◇ Connected AU Slot ID
  - ◇ Registration Status (In Service, Out Of Service)
  - ◇ Configured SW File Name: The SW File configured in the NPU (together with the Configured Operation).
  - ◇ Configured SW Version: The SW Version of the SW File configured in the NPU.



- ◇ Configured Operation: The operation to be performed with the Configured SW 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: Basic or IDU-NG-4D1W
- ◇ Number of Gateways: The number of Alvarion Gateways connected to the SU (including IDU-NG-4D1W, if exists).
- ◇ Service Fault Status: OK or reason for denying services to the SU. The reason can be:
  - 1 Loop problem. A loop was detected on the Ethernet side of the SU. rbNetworkingError Trap will be sent, and services to this SU will be denied until resetting the SU from the network (NPU) side (provided the problem no longer exists). The problem is detectable through periodical (every 5 seconds) transmissions to the Ethernet link of SNAP packets with "AA AA 03" in the header, and the destination MAC address is 00:10:E7:00:00:01. If the SU receives this packet from the Ethernet, it means that there is a loop and the SU will send an appropriate message to the NPU.



#### NOTE

Another loop avoidance mechanism that is transparent to the operator is performed by the NPU: The NPU scans packets received from the network (DATA port) and verifies that the SRC MAC in the received packet does not match any of the addresses in the NPU's bridging table. If there is a match it means that the source MAC address of the message received from the network side is identical to a MAC address of a device behind one of the SUs served by the Base Station. In case of a match, the NPU discards all packets designated to the device with this MAC address, until its aging time expires.

- 2 Duplicate SU Name: The SU Name is already in use by another SU. rbSuDuplicateName Trap will be sent and services to the SU will be denied until another unique name is configured for the SU (see also [Section 4.9.6.3.1.1](#)).

#### ■ 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 [Section 4.9.1](#). You will be prompted to select the required AU Slot ID.

## 4.9.3 SW Files in NPU

Up to three SU SW files can be stored in the NPU. Any of the available files can be loaded by the NPU to a selected SU. When three SU 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 SU SW files stored in the NPU and deleting selected file(s). It also enables defining a Default SU SW 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 [Section 4.10.1](#) 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. For each available SW file, the file name and the version number are displayed.

In addition, the Default SU 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 SW 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 SW 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 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
- Show MAC Addresses Behind SU
- 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

- ◇ SU Type: BMAX CPE, PRO CPE, PRO-L CPE, Si CPE.
- ◇ Organization Name
- ◇ Address
- ◇ Country
- ◇ SU Status (Permanent or Temporary)
- ◇ Connected AU Slot ID
- ◇ SU IDU Type
- ◇ Number of Gateways
- ◇ Service Fault Status

■ General HW Parameters

- ◇ Serial Number
- ◇ Cumulative Power On Time (hours)
- ◇ RF Card HW Revision
- ◇ 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)
- ◇ Configured SW File Name
- ◇ Configured SW Version
- ◇ Configured Operation

- MAC Parameters

- ◇ Base Station ID
- ◇ Base Station Mask

- Phy Parameters

- ◇ Bandwidth (MHz)
- ◇ Uplink (Tx) Frequency (MHz)
- ◇ Selected Antenna (Si CPE only)

- ATPC Parameters and Current Link Quality Indicators

- ◇ ATPC Support
- ◇ Uplink RSSI (dBm)
- ◇ Uplink SNR (dB)
- ◇ Uplink Current Rate
- ◇ Downlink RSSI (dBm)
- ◇ Downlink SNR (dB)
- ◇ Downlink Current Rate
- ◇ TX Power (dBm)
- ◇ Estimated Distance from BS (m). The accuracy is from several hundreds of meters for line-of-sight links to 1500 meters for non-line-of-sight links.

- 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 [Section 4.11](#) 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 [Section 4.11](#) 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, and is performed using one of the SU SW files installed in the NPU. 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: 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 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 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 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

- License

#### 4.9.6.3.1 Registration Parameters

The SU Registration Parameters option in the NPU Monitor enables viewing the SU's Registration parameters and updating the SU Name parameter. Other Registration parameters can be configured only locally at the SU (via the Ethernet port).

##### 4.9.6.3.1.1 SU Name

The SU Name is typically configured locally in the SU (Common Name).

The default SU Name given to a new SU during the definition process (see [Section 4.9.7](#)) is SU@<SU's MAC Address>. When an SU is registered, it receives services based on its MAC address, and the default SU Name is replaced by the name configured in the SU (Common Name).

Under normal conditions, the SU Name should be changed only upon identifying an SU with an SU Name that is identical to that of a previously registered SU. In this case, the new SU will be registered (to enable management), but will not receive any services. Its name in the NPU database will be changed to SU@<SU's MAC Address>. The system administrator will be informed of the problem through the Fault Status parameter in any of the relevant Show menus (Fault Status 2) and through a trap message (rbSuDuplicateName trap). If the administrator decides that the SU is legitimate and should receive services, a new SU Name must be configured. The SU will receive services only after configuring it with a unique SU Name.

A new SU Name can be configured also for a temporary SU.

The SU Name comprises a string of up to 32 printable characters.

A change in the SU Name parameter takes effect only after reset.

##### 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

The Country name configured in the SU.

#### 4.9.6.3.2 MAC Parameters

The SU MAC menu enables viewing/updating the following parameters:

#### 4.9.6.3.2.1 Base Station ID

The Base Station ID is the identifier of the AU/ BST to which the SU can connect. An SU can be authenticated by an AU/ 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/ 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.

#### 4.9.6.3.2.2 Base Station ID Mask

The Base Station ID Mask, together with the Base station ID define the AU(s)/ 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.

#### 4.9.6.3.3 Phy Parameters

The SU Phy menu enables viewing/updating the following parameters:

##### 4.9.6.3.3.1 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

##### 4.9.6.3.3.2 Uplink (Tx) Frequency (MHz)

The frequency used in the uplink (from SU to AU). A change in the Uplink Frequency parameter will take effect only after resetting the SU.

The available values depend on the Bandwidth and on the available Frequency Bands in the Frequency Bands Group supported by the AU (see [Section 4.7.5](#)).

#### 4.9.6.3.4 Multirate and ATPC Parameters

The Multirate and ATPC mechanism are controlled by the AU (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 (see [Section 4.8.4.3.4](#)), allowing to set the Uplink Current Rate and the Downlink Current Rate to any of the values listed in [Table 4-5](#).

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.
- VG-1D1V: A stand-alone (external) Voice Gateway, supporting 1 data port and 1 POTS port.
- VG-1D2V: A stand-alone (external) Voice Gateway, supporting 1 data port and 2 POTS ports.

#### 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.

#### 4.9.6.3.9 License

The License menu is applicable only to L model CPE. It enables viewing the details of installed licenses and loading a new license (if a required license is available in the CPE Licenses Bank).

#### 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 displayed counters include:

■ **Ethernet Port Counters**

- ◇ **Data Bytes Received:** The total number of data bytes received from the Ethernet link. Management frames and frames with errors are not included.
- ◇ **Data Bytes Discarded on Rx:** The number of bytes discarded when a packet received from the Ethernet port is not forwarded to the Wireless port due to bridging or classification considerations.
- ◇ **Data Bytes Transmitted:** The total number of data bytes transmitted to the Ethernet link. Management frames and frames with errors are not included.
- ◇ **Data Bytes Discarded on Tx:** The number of bytes discarded when a packet received from the Wireless port is not forwarded to the Ethernet port due to bridging or VLAN considerations.

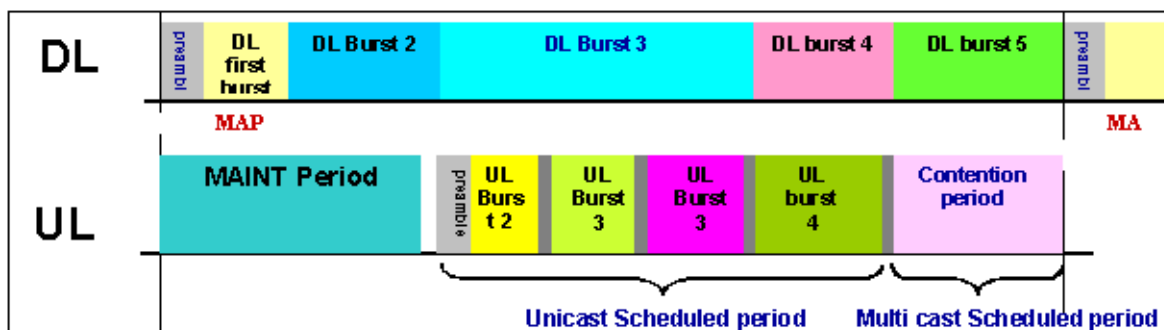
■ **Wireless Port Counters**

- ◇ **Data Bytes Received:** The total number of data bytes received from the Wireless link. Management frames and frames with errors are not included.
- ◇ **Data Bytes Discarded on Rx:** The number of bytes in packets received from the Wireless link and discarded due to MAC protocol receive errors, such as duplicate sequence number, wrong sequence number etc. (not CRC errors).
- ◇ **Data Bytes Transmitted:** The total number of data bytes transmitted to the Wireless link. MAC Management frames and frames with errors are not included.
- ◇ **Data Bytes Discarded on Tx:** The number of bytes in packets discarded due to congestion in the wireless medium.

- ◇ **ARQ Enabled Bytes Transmitted:** The number of bytes transmitted over BE and NRT connections. Applicable only if the ARQ mechanism in the AU is enabled.
- ◇ **Bytes Retransmitted:** The number of unacknowledged bytes that were retransmitted. Retransmissions are applicable only to BE and NRT connections, provided the ARQ mechanism in the AU is enabled.
- ◇ **Retransmission Rate (%):** Retransmission Rate in percents is defined as:  $100 * (\text{Bytes Retransmitted}) / (\text{ARQ Enabled Bytes Transmitted})$ .

#### 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 4-2: 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 Burst Error Rate counters. The information displayed for each rate in uplink and downlink is the accumulated number since the last time the counters were reset. For each direction (uplink/downlink) the displayed information includes the following statistics for each rate:

- 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 Show MAC Addresses Behind SU**

Select this option to view a list of the MAC Addresses of the devices behind the SU. If VLAN behind the SU is used, the VLAN ID used by each device is displayed next to its MAC Address.

#### **4.9.6.6 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 NPU.
  
- Operation: The action to be performed with the specified SW File after the SU connects to the AU (None, Download, Run from Shadow or Set as Main).

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 to Services

#### 4.10.1.1 Services, Subscribers and Service Profiles

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.
- **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 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 [Section 4.10.4.7](#)) 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 [Section 4.10.6](#). For details on defining Service Profiles for generic VoIP devices, refer to [Appendix B](#).

### 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). It is possible to define up to two Default Service Profiles: one for PPPoE services and one for L2 or Voice services (note that L2 service can support also Voice services). When the SU is defined as Permanent and services are assigned to it, it will be able to use the defined default 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 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) and VLAN Transparency Mode is Off, frames arriving from the infrastructure side with a VLAN ID tag 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 (applicable only if VLAN Transparency Mode is Off), all untagged 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 VPL ID 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.

The VLAN Transparency Mode defines the method of transferring packets to the operator's upstream network. When set to On, data packets sent from the Base Station to the backbone will be transferred transparently. The VPL ID parameter is not applicable to Service Profiles with VLAN Transparency Mode On.

- For tagged packets, the VPL ID will be their VLAN tag.
- For untagged packets, the VPL ID will be None.

For packets received from the network, the forwarding decision will be according to the packet's VPL ID. If the VPL ID is unknown (either None or not included in the list of VPL IDs defined for any of the existing, non-transparent Service Profiles), the system will assume this is a transparent VLAN packet (if at least one transparent Service is defined) and transfer it with the original VLAN tag (or untagged if there is no VLAN tag).

For transparent services, VLAN Classification Mode can be set to On to enable downlink classification based on both the MAC Address and VLAN ID, to support applications with multiple VLAN IDs per a single MAC address. All Services assigned to the same SU must be configured with the same VLAN Classification Mode (Either On or Off). If VLAN Classification Mode is On, only a single VLAN ID can be defined for the Service. This means that the allowed combinations are:

- Hybrid VLAN Mode is Off and the VLAN List includes a single VLAN ID.
- Hybrid VLAN Mode is On and the VLAN List is empty.

For transparent services it is also possible to configure an Access VLAN to be used with untagged packets received on the Ethernet port of the SU. This parameter is applicable only for a transparent service with Hybrid Mode set to On, or a transparent service with Hybrid Mode set to Off and an empty VLAN list.

A maximum of one Access VLAN can be defined per SU.

Hybrid VLAN Mode of operation enables classification of both tagged and untagged packets or untagged packets only, according to the following rules:

**Table 4-6: Hybrid VLAN Mode**

Hybrid VLAN Mode	VLAN List	Forwarded Packets
Off	Exists	Only packets tagged with a VLAN ID that exists in the VLAN List. VLAN List can include up to 16 entries.
	Empty	All (both untagged and tagged with any VLAN ID)
On	Exists	Untagged packets, and packets tagged with a VLAN ID that exists in the VLAN List. VLAN List can include up to 15 entries.
	Empty	Only untagged frames.

The guidelines that should be followed when defining VLAN IDs and related parameters are:

- 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.
- For each Service Type, a maximum of one Service that enables forwarding of untagged packets can be assigned to an SU. Forwarding of untagged packets is supported when either Hybrid VLAN Mode is On, or Hybrid VLAN Mode is Off and the VLAN List is empty. It is not possible to define for the same SU two Services of the same Service Type that enable forwarding of untagged packets. However, the same SU and untagged packets can be associated with two Services of different Service Types, excluding the combination of L2 Service and Voice Service.
- The maximum total number of VLAN IDs behind the same SU is 16 (15 when there is a Service with Hybrid VLAN Mode On is assigned to the SU).
- The combination of VLAN Transparency Service On, Hybrid VLAN Mode Off and an empty VLAN List means that all packets are forwarded. This combination should be used only if the Service Provider can ensure that there will not be conflicts between VLAN IDs used by devices behind the SU and existing VPL IDs.

- To avoid conflicts, a transparent Service Profile cannot be assigned to a Service if the Service's VLAN ID list includes a VLAN ID that is equal to any of the already assigned VPL IDs.
- The combination VLAN Transparency Mode On, Hybrid VLAN Mode On and an empty VLAN List means that only untagged frames should be forwarded. Such a Service cannot be assigned if there is an assigned non-transparent Service with VPL ID = None.

## 4.10.2 Introduction to Filtering Features

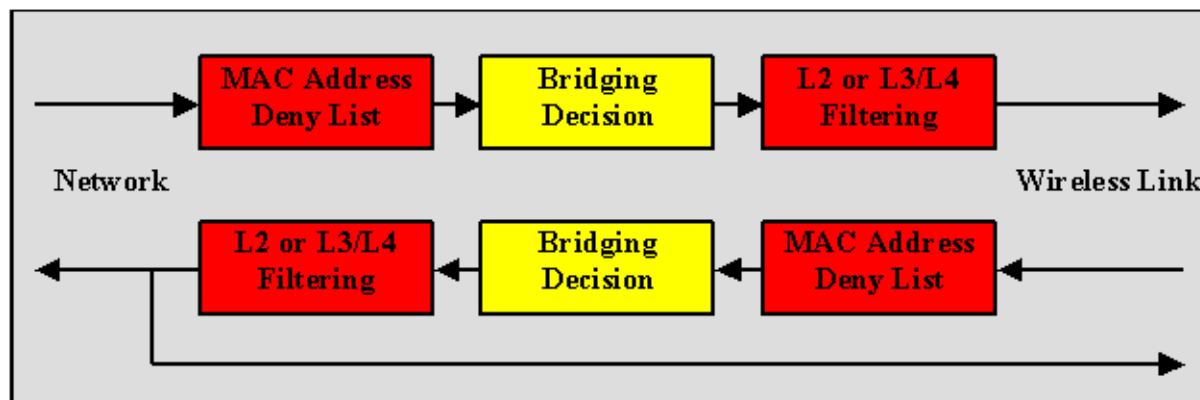
The Filtering features allow a network operator to control the traffic in the system by forwarding or discarding packets according to a set of rules based on multiple allow/deny criteria. This provides both improved network security and better utilization of the wireless medium.

The filtering is done at the base station, controlling the traffic between the network and the wireless link. The filtering features enable:

- Filtering packets arriving from the network interface (From Network Filtering), using a set of either Layer 2 or Layer 3/Layer 4 Filtering Rules.
- Filtering packets arriving from the wireless link (From Wireless Filtering), using a set of either Layer 2 or Layer 3/Layer 4 Filtering Rules.
- Discarding packets to/from specific MAC addresses (MAC Address Deny List). This is applicable to MAC Addresses behind SUs.

The filtering functionality is described in [Figure 4-3](#).





**Figure 4-3: Filtering Functionality**

The filtering definition process includes the following steps:

- 1 Defining list(s) of Filtering Rules. Each Filtering Rule defines a combination of values for certain packet fields. Filtering Rules can be of 2 types: Layer 2 Filtering Rules (using fields of the Ethernet frame) and Layer 3/Layer 4 Filtering Rules (using fields of the IP and/or UDP/TCP headers).
- 2 Associating each Interface (From Network, From Wireless Link) with a set of either Layer 2 or Layer 3/Layer 4 filters from the relevant Filtering Rules lists, and defining the action to be taken upon receiving a packet that matches any of the selected Filtering Rules: Allow (forward) or Deny (discard).

### 4.10.3 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:

#### 4.10.3.1 Show All

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

#### 4.10.3.2 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.

### 4.10.3.3 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.

### 4.10.3.4 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.

### 4.10.3.5 Add

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

## 4.10.4 The Services Menu

The Services menu includes the following options:

- General
- Subscribers
- Services
- Service Profile
- Forwarding Rules
- Priority Classifiers
- QoS Profiles
- Filtering Rules
- Interface Filtering

- MAC Addresses Deny List

#### 4.10.4.1 General

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

##### 4.10.4.1.1 Show

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

##### 4.10.4.1.2 Update

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

###### 4.10.4.1.2.1 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 [Section 4.10.1.4](#).

The default Service Mode is Quick (2).

###### 4.10.4.1.2.2 Default L2/Voice Service Profile

The default L2 or Voice Service Profile to be used by temporary SUs in Quick Mode.

Available profiles - any of the L2 or Voice Service Profiles existing in the database.

###### 4.10.4.1.2.3 Default PPPoE Service Profile

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

Available profiles - any of the PPPoE Service Profiles existing in the database.

#### 4.10.4.2 Subscribers

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

The Subscribers database in the NPU can hold up to 1024 Subscribers.

The configurable Subscriber's parameters are:

#### 4.10.4.2.1 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.

#### 4.10.4.2.2 First Name

An optional parameter for information purposes.

A First Name consists of up to 50 printable characters.

#### 4.10.4.2.3 Last Name

An optional parameter for information purposes.

A Last Name consists of up to 50 printable characters.

#### 4.10.4.2.4 Description

An optional parameter for information purposes.

A Description consists of up to 50 printable characters

#### 4.10.4.2.5 Admin Status

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

### 4.10.4.3 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.

#### NOTE



The proper process of removing a Service is:

1. Disable the Service (set the Admin Status to Disable)
2. Delete the Service.

If the Service is not disabled prior to being the deleted, VLAN ID included in the VLAN List of the deleted Service may still be used by other Services to the same SU that use the same Forwarding Rule as the deleted Service.

The Services database in the NPU (Base Station) can hold up to 4095 Services.

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

#### 4.10.4.3.1 Service Parameters

The Service's parameters are:

##### 4.10.4.3.1.1 Name

A Service Name consists of up to 32 printable characters.

#### 4.10.4.3.1.2 Subscriber Name

The Subscriber to which the Service is allocated.

The Subscriber Name must be that of a Subscriber that exists in the database.

#### 4.10.4.3.1.3 Service Profile Name

The Service Profile to be used in the Service.

The Service Profile Name must be that of a Service that exists in the database.

#### 4.10.4.3.1.4 SU MAC Address

The MAC Address of the SU associated with the Service.

The SU MAC Address must be that of a Permanent SU that exists in the database.

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

#### 4.10.4.3.1.5 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.

When Hybrid VLAN Mode is Off, the VLAN List can include up to 16 VLAN IDs. When Hybrid VLAN Mode is On, the VLAN List can include up to 15 VLAN IDs (the 16th entry is reserved for No VLAN).

The maximum total number of VLAN IDs behind a single SU is 16. (15 when there is a Service with Hybrid VLAN Mode On is assigned to the SU).

Refer to [Section 4.10.1.5](#) for guidelines regarding VLAN ID configuration.

#### 4.10.4.3.1.6 Hybrid VLAN Mode

Hybrid VLAN Mode of operation enables classification of both tagged and untagged packets or untagged packets only, according to the following rules:

**Table 4-7: Hybrid VLAN Mode**

Hybrid VLAN Mode	VLAN List	Forwarded Packets
Off	Exists	Only packets tagged with a VLAN ID that exists in the VLAN List. VLAN List can include up to 16 entries.
	Empty	All (both untagged and tagged with any VLAN ID)

**Table 4-7: Hybrid VLAN Mode**

Hybrid VLAN Mode	VLAN List	Forwarded Packets
On	Exists	Untagged packets, and packets tagged with a VLAN ID that exists in the VLAN List. VLAN List can include up to 15 entries.
	Empty	Only untagged frames.

Note that for each Service Type, a maximum of one Service that enables forwarding of untagged packets can be assigned to an SU. Forwarding of untagged packets is supported when either Hybrid VLAN Mode is On, or Hybrid VLAN Mode is Off and the VLAN List is empty. It is not possible to define for the same SU two Services of the same Service Type that enable forwarding of untagged packets. However, the same SU and untagged packets can be associated with two Services of different Service Types, excluding the combination of L2 Service and Voice Service.

#### 4.10.4.3.1.7 VLAN Classification Mode

The VLAN Classification feature enables using VLAN ID (in addition to destination MAC address) for classification of transparent service downlink traffic before transmission to the destination MAC address. The VLAN Classification feature supports applications where multiple VLANs are associated with a single MAC address, allowing to assign different services to different VLANs.

VLAN Classification Mode can be set to On only if the following conditions are met:

- The VLAN Transparency Mode of the applicable Service Profile is set to On.
- A single VLAN ID is defined for the Service. This means that the allowed combinations are:
  - ◇ Hybrid VLAN Mode is Off and the VLAN List includes a single VLAN ID.
  - ◇ Hybrid VLAN Mode is On and the VLAN List is empty.
- All Services assigned to the same SU must be configured with the same VLAN Classification Mode (Either On or Off).

#### 4.10.4.3.1.8 Access VLAN

The Access VLAN parameter enables defining a VLAN ID to be used with untagged packets received on the Ethernet port of the SU. This parameter is applicable only for a transparent service (VLAN Transparency Mode is On) with Hybrid Mode set to On, or a transparent service with Hybrid Mode set to Off and an empty VLAN list.

A tag with the defined Access VLAN will be added by the NPU to untagged packets in the uplink. The tag will be removed by the NPU from packets in the downlink. For a multicast connection, the NPU will send in addition to the VLAN list the single Access VLAN. The SU will be responsible to remove the Access VLAN if it is received on a multicast connection.

A maximum of one Access VLAN can be defined per SU.

The range is from 1 to 4094 or null for no Access VLAN.

#### 4.10.4.3.1.9 Admin Status

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

#### 4.10.4.3.1.10 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.

#### 4.10.4.3.2 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
- Connection Type: BE, NRT, RT or CG.
- QoS Profile Parameters: The values of the relevant QoS Profile's parameters.
- Bytes Submitted: The number of bytes submitted by upper layers to this connection.
- Bytes Transmitted: The number of bytes transmitted to the wireless port through this connection, including retransmissions.
- Bytes Retransmitted: The number of bytes retransmitted to the wireless port through this connection.
- Bytes Dropped: The number of bytes dropped from this connection due to congestion in the wireless link. (identical to Bytes Discarded).
- Bytes Discarded: The number of bytes discarded from this connection due to congestion in the wireless link. (identical to Bytes Dropped).

- **Packets Submitted:** The number of packets submitted by upper layers to this connection.
- **Packets Transmitted:** The number of packets transmitted to the wireless port through this connection, excluding retransmissions.
- **Packets Dropped:** The number of packets dropped from this connection due to congestion in the wireless link. (identical to Packets Discarded).
- **Packets Discarded:** The number of packets discarded from this connection due to congestion in the wireless link. (identical to Packets Dropped).
- **Average Delay:** The average packet delay in milliseconds, measured for this connection over the last 15 seconds. The value is updated every 15 seconds.
- **Delay Variance:** The variance (the standard deviation squared) of the packet delay, in milliseconds squared, measured for this connection over the last 15 seconds. The value is updated every 15 seconds.
- **Maximum Delay:** The maximum packet delay in milliseconds, measured for this connection over the last 15 seconds. The value is updated every 15 seconds.
- **Data Loss Indicator (%):** The percentage of dropped packets, out of the total demand, measured for this connection over the last 15 seconds. The value is updated every 15 seconds.

$$\text{DLI (\%)} = 100 * (\text{Packets Dropped}) / (\text{Packets Submitted})$$

- **CIR Utilization (%):** The CIR utilization measured for an RT or NRT connection over the last 15 seconds. Not applicable for BE and CG connections.

$k = 100 \times (\text{the minimum between bytes transferred and CIR}) / \text{CIR}$  is calculated for each 1 second interval. CIR Utilization equals the average of  $k$  over the last 15 seconds, and may vary from 0 to 100. The value is updated every 15 seconds.

- **EIR Utilization (%):** Excess Information Rate utilization measured for a BE or NRT connection over the last 15 seconds. Not applicable for RT and CG connections.



$k = 100 \times (\text{bytes transferred} - \text{CIR}) / (\text{MIR} - \text{CIR})$  is calculated for each 1 second interval. In BE CIR = 0. The EIR Utilization equals the average of k over the last 15 seconds, and may range from 0 to 100. The value is updated every 15 seconds.

- Average Throughput (bits/s): The average throughput, in bits/second, measured for this connection over the last 15 seconds. The value is updated every 15 seconds.

#### 4.10.4.4 Service Profiles

Each Service Profile defines the properties of the defined service. Each Service Profile is associated with specific Forwarding Rule and Priority Classifier (Priority Classifiers are not applicable to Voice Service Profiles).

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 Service Profiles database can hold up to 1024 Service Profiles.

The configurable Service Profile's parameters are:

##### 4.10.4.4.1 Service Profile Name

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

##### 4.10.4.4.2 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 [Section 4.10.1.2](#).

##### 4.10.4.4.3 VLAN Transparency Mode

The VLAN Transparency Mode defines the method of transferring packets to the operator's upstream network.

When set to On, data packets sent from the Base Station to the backbone will be transferred transparently. The VPL ID parameter is not applicable to Service Profiles with VLAN Transparency Mode On.

Also the Forwarding Rule selection parameter is not applicable to transparent Service Profiles. All transparent Service Profiles share a single pre-configured Forwarding Rule, and a pre-configured QoS Profile for multicasts. For details on these profiles refer to [Table 4-20](#) and [Table 4-21](#). The pre-configured Transparent Forwarding Rule can be modified but not deleted.

- For tagged packets, the VPL ID will be their VLAN tag.
- For untagged packets, the VPL ID will be None.

For packets received from the network, the forwarding decision will be according to the packet's VPL ID. If the VPL ID is unknown (either None or not included in the list of VPL IDs defined for any of the existing, non-transparent Service Profiles), the system will assume this is a transparent VLAN packet (if at least one transparent Service is defined) and transfer it with the original VLAN tag (or untagged if there is no VLAN tag).

#### NOTE



The combination of VLAN Transparency Service On, Hybrid VLAN Mode Off and an empty VLAN List means that all packets are forwarded. This combination should be used only if the Service Provider can ensure that there will not be conflicts between VLAN IDs used by devices behind the SU and existing VPL IDs.

When set to Off, data packets sent from the Base Station to the backbone will be transferred with a VLAN tag according to the VPL ID. The VLAN ID in tagged frames arriving from the wireless network will be replaced by the VPL ID. For packets received from the network, the forwarding decision will be according to the Forwarding Rule defined in the Service Profile with a matching VPL ID.

To avoid conflicts, a transparent Service Profile cannot be assigned to a Service if the Service's VLAN ID list includes a VLAN ID that is equal to any of the already assigned VPL IDs.

#### NOTE



The combination VLAN Transparency Mode On, Hybrid VLAN Mode On and an empty VLAN List means that only untagged frames should be forwarded. Such a Service cannot be assigned if there is an assigned non-transparent Service with VPL ID = None.

#### 4.10.4.4.4 VPL ID

A Virtual Private Link ID to be used in the backbone behind the Base Station. The VPL ID parameter is applicable only to Service Profiles with VLAN Transparency Mode Off.

To avoid conflicts, it is not allowed to define a VPL ID that is identical to any of the VLAN IDs in the already assigned transparent Services (Services using a Service Profile with VLAN Transparency Mode On).

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.

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.

#### 4.10.4.4.5 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 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 according to the following rules:

- ◇ If VLAN Transparency Mode is Off, the frames will be forwarded 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.
- ◇ If VLAN Transparency Mode is On, the frames will be forwarded without any change (with the original 802.1p value and VLAN ID, if exists).

For DSCP classification at the SU:

- ◇ If the VPL ID is configured (VLAN Transparency Mode Off), the NPU adds an 802.1Q header with the configured VPL ID and 802.1p=0.
- ◇ If VLAN Transparency Mode is On, The NPU adds a 802.1Q header with the original VLAN ID (if exists).

Note that there may be a disparity between the DSCP values and the default 802.1p = 0 value.

## 2 802.1p Marking Mode:

- ◇ If VLAN Transparency Mode is Off, all frames are marked with the configured VPL ID and the 802.1p Marking Value. If no VPL ID is configured (VPL ID = None), the 802.1Q header will include a VLAN ID = 0.
- ◇ If VLAN Transparency Mode is On, all frames are marked with the original VLAN ID and the 802.1p Marking Value.

### NOTE



If the Priority Marking Value is set to 0, untagged packets (without VLAN ID) will be forwarded without any change. This is applicable to transparent services and to non-transparent services with no VPL ID.

- ◇ 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 (if VLAN Transparency Mode is Off) or the original VLAN ID (if VLAN Transparency Mode is On), and the 802.1p Marking Value. 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 according to the following rules:

- ◇ If VLAN Transparency Mode is Off, the frames will be forwarded 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.
- ◇ If VLAN Transparency Mode is On, the frames will be forwarded without any change (with the original 802.1p value and VLAN ID, if exists).

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.

#### 4.10.4.4.6 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 4-8: Priority Marking Values**

Priority Marking Mode	Priority Marking Values Range
Transparent	Not Applicable
802.1p	0 - 7
DSCP	0 - 63

#### 4.10.4.4.7 Forwarding Rule

The Forwarding Rule to be used by the Service Profile. The Forwarding Rule parameter is not applicable to transparent Service Profiles (VLAN Transparency Mode On), as all transparent Service Profiles share the same pre-defined Forwarding Rule.

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.

#### 4.10.4.4.8 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.

#### 4.10.4.4.9 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 and calls made by devices that support DRAP.

The available range is from 0 to 50 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.

### 4.10.4.5 Forwarding Rules

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 Forwarding Rules database can hold up to 255 Forwarding Rules.

The configurable Forwarding Rule's parameters are:

#### 4.10.4.5.1 Forwarding Rule Name

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

#### 4.10.4.5.2 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 [Section 4.10.1.2](#).

#### **4.10.4.5.3 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.

#### **4.10.4.5.4 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.

#### **4.10.4.5.5 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 unicast 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 unicast packets sent to addresses that the AU recognizes as being on its wired backbone side.

#### **4.10.4.5.6 Multicast VLAN ID**

The Multicast VLAN ID parameter is applicable only to Services assigned to SUs with SW version below 2.0. The Multicast VLAN ID is the VLAN ID to be attached to multicast messages in order to enable full support of the VLAN feature by SUs with SW version below 2.0.

In SUs with SW version below 2.0, it was necessary to use behind the SU a VLAN switch with binding capability to support multiple VLAN IDs. The VLAN switch was responsible for duplicating all the packets to the correct ports according to the multicast connection, this required switch pre-configuration. If a VLAN switch with binding capability was not used, only a single VLAN ID behind the SU could be supported, and this VLAN ID has to be identical to the multicast VLAN ID.

In the current version, all packets received from the wireless port over a multicast connection are transmitted by the SU several times to the Ethernet port, each time with a different VLAN ID, taken from the VLAN ID list supplied by the NPU.

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

Refer to [Section 4.10.1.5](#) for guidelines regarding configuration of Multicast VLAN ID.

#### 4.10.4.5.7 Multicast QoS Profile

The Multicast QoS Profile is the QoS Profile to be used for mulicast 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.

#### 4.10.4.6 Priority Classifiers (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 Priority Classifiers database can hold up to 255 Priority Classifiers.

The configurable Priority Classifier's parameters are:

##### 4.10.4.6.1 Priority Classifier Name

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

##### 4.10.4.6.2 Priority Type

The prioritization mechanism used by the Priority Classifier.

The available options are:



1 - DSCP

2 - 802.1p

#### 4.10.4.6.3 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.

#### 4.10.4.6.4 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.

#### 4.10.4.6.5 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.

#### 4.10.4.6.6 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.

#### 4.10.4.7 QoS Profiles

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)** 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)** 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 priorities of allocating bandwidth to connections are in accordance with the QoS Type of the connections, in the following order:

- 1 CG
- 2 RT
- 3 NRT
- 4 BE

For each of the RT, NRT and BE connection, there is a second level of priorities according to the Committed Time (CT), where connections with CT=Short gets the highest priority and connections with CT=Long gets the lowest priority.

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 QoS Profiles database can hold up to 255 QoS Profiles.

The available QoS Profile parameters depend on the QoS Type. The configurable QoS Profile's parameters are:

#### **4.10.4.7.1 QoS Profile Name**

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

#### **4.10.4.7.2 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)

#### **4.10.4.7.3 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. It is used also to prioritize bandwidth allocation to connections, where for each QoS Type, connections with a shorter CT get higher priority.

The available options are Short (1), Medium (2), and Long (3).

The actual value in milliseconds for each of the three options varies according to the QoS type:

Table 4-9: CT Values

CT	BE	NRT	RT
Short	50 mS	50 mS	50 mS
Medium	100 mS	100 mS	100 mS
Long	200 mS	200 mS	200 mS

#### 4.10.4.7.4 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.

#### 4.10.4.7.5 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).

#### 4.10.4.7.6 Packet Size (CG QoS Type)

The Packet Size parameter defines the amount of data in bytes that is expected for each grant.

The range is from 64 to 1550 (bytes).

#### 4.10.4.7.7 Sample Interval (CG QoS Type)

The Sample Interval parameter defines the time in milliseconds between two successive grants (inter arrival time).

The range is from 5 to 100 (milliseconds).

### 4.10.4.8 Filtering Rules

The Filtering Rules menu enables defining L2 Filtering Rules and L3/L4 Filtering Rules.

#### 4.10.4.8.1 L2 Filtering Rules

An L2 (Layer 2) Filtering Rule includes the MAC Address and Ethertype. A range of MAC Addresses can be defined for either the Source or Destination MAC Address field. It is possible to define "Any" for either the MAC Address or Ethertype field (but not for both fields).

The L2 Filtering Rules menu enables defining new L2 Filtering Rule, viewing details of previously defined L2 Filtering Rules and removing L2 Filtering Rules from the database. It is not possible to edit the parameters of an existing L2 Filtering Rule. The database can hold up to 255 L2 Filtering Rules.

The configurable L2 Filtering Rule parameters are:

#### 4.10.4.8.1.1 Rule Name

The name of the L2 Rule. The L2 Rule Name is a string of 1 to 32 printable characters.

#### 4.10.4.8.1.2 MAC Address

The base MAC Address that is used together with the MAC Address Mask to define a range of MAC addresses. A string of 6 octets (where each octet is represented by two hexadecimal numbers) separated by dashes ("-"). An empty entry means "Any". An "Any" MAC Address means that the filter is defined only by the Ethertype field.

#### 4.10.4.8.1.3 MAC Address Mask

The mask that is used together with the MAC Address to define a range of MAC addresses. A string of 6 octets (where each octet is represented by two hexadecimal numbers) separated by dashes ("-"). In a binary representation the string must comprise a series of contiguous binary '1's starting from the MSB, followed by a series of contiguous binary '0's (if the range includes more than a single address). The MAC Address Mask parameter is not applicable for an "Any" MAC Address.

#### 4.10.4.8.1.4 MAC Address Direction

The direction (Source or Destination) of the MAC Address. Indicates whether the range defined by the MAC Address and MAC Address Mask is for the Source MAC Address field or the Destination MAC Address field in the Ethernet frame. The MAC Address Direction parameter is not applicable to "Any" MAC Address.

#### 4.10.4.8.1.5 Ethertype

The Ethertype of the Ethernet frame. The Ethertype is defined by 4 hexadecimal digits. An empty entry means "Any" and is applicable only if a MAC Address range is defined (the combination of "Any" for both the MAC Address and Ethertype is not allowed).

### 4.10.4.8.2 L3/L4 Filtering Rules

An L3/L4 (Layer 3/Layer 4) Filtering Rule includes the IP Address and Protocol. A range of IP Addresses can be defined for either the Source or Destination IP Address field. It is possible to define "Any" for either the IP Address or Protocol field (but not for both fields). If the specified Protocol is either TCP (6) or UDP (17),

either the Source or Destination Port can be defined. It is also possible to define "Any" Port.

The L3/L4 Filtering Rules menu enables defining new L3/L4 Filtering Rule, viewing details of previously defined L3/L4 Filtering Rules and removing L3/L4 Filtering Rules from the database. It is not possible to edit the parameters of an existing L3/L4 Filtering Rule. The database can hold up to 255 L3/L4 Filtering Rules.

The configurable L3/L4 Filtering Rule parameters are:

#### 4.10.4.8.2.1 Rule Name

The name of the L3/L4 Rule. The L3/L4 Rule Name is a string of 1 to 32 printable characters.

#### 4.10.4.8.2.2 IP Address

The base IP Address that is used together with the IP Address Mask to define a range of IP addresses. A string of 4 decimal numbers (where each number is in the range from 1 to 255) separated by dashes ("-"). An empty entry means "Any". An "Any" IP Address means that the filter is defined only by the Protocol field (and optionally by the Port and Port Direction for UDP or TCP protocols).

#### 4.10.4.8.2.3 IP Address Mask

The mask that is used together with the IP Address to define a range of IP addresses. A string of 4 decimal numbers (where each number is in the range from 1 to 255) separated by dashes ("-"). In a binary representation, the string must comprise a series of contiguous binary '1's starting from the MSB, followed by a series of contiguous binary '0's (if the range includes more than a single address). The IP Address Mask parameter is not applicable to an "Any" IP Address.

#### 4.10.4.8.2.4 IP Address Direction

The direction (Source or Destination) of the IP Address. Indicates whether the range defined by the IP Address and IP Address Mask is for the Source IP Address field or the Destination IP Address field in the IP frame. The IP Address Direction parameter is not applicable to "Any" IP Address.

#### 4.10.4.8.2.5 Protocol

The protocol of the IP packet. The Protocol is defined by a decimal number from 0 to 254. An empty entry means "Any" and is applicable only if an IP Address range is defined (the combination of "Any" for both the IP Address and Protocol is not allowed).

#### 4.10.4.8.2.6 Port

The TDP/UCP port number, which is applicable only if the Protocol parameter is configured to a value of either 6 (TCP) or 17 (UDP). The Port is defined by a number in the range from 0 to 65534. An empty entry means "Any" port.

#### 4.10.4.8.2.7 Port Direction

The direction (Source or Destination) of the Port. Indicates whether the Port number is for the Source Port field or the Destination Port field in the IP frame. The Port Direction parameter is not applicable to "Any" Port.

### 4.10.4.9 Interface Filtering

The Interface Filtering menu enables viewing and editing the filtering mechanisms to be used on frames received from the network (From Network Filtering) and from the wireless link (From Wireless Filtering).

The Interface Filtering menu also enables viewing and resetting the Filtering Rules Counters, which display for each of the applicable rules the number of frames matching the rule, accumulated since the last reset. In addition, there is a Non Matching counter, displaying the number of frames that did not match any of the relevant rules. The counters will be reset also after changing the Active Rule Type or disabling the Admin Status.

For each of the interfaces, the configurable parameters are:

#### 4.10.4.9.1 L2 Filtering Rules List

The L2 Filtering Rules List submenu enables viewing details on the L2 Filtering Rules assigned to the interface, adding Rules (from the L2 Filtering Rules lists) to the list of Rules assigned to the interface, and deleting one or all Rules from the list. It also enables viewing/resetting the counter for a selected Rule. The counter displays the number of frames matching the Rule, accumulated since the last reset. The counter will be reset also after changing the Active Rule Type or disabling the Admin Status.

#### 4.10.4.9.2 L3/L4 Filtering Rules List

The L3/L4 Filtering Rules List submenu enables viewing details on the L3/L4 Filtering Rules assigned to the interface, adding Rules (from the L3/L4 Filtering Rules lists) to the list of Rules assigned to the interface, and deleting one or all Rules from the list. It also enables viewing/resetting the counter for a selected Rule. The counter displays the number of frames matching the Rule, accumulated since the last reset. The counter will be reset also after changing the Active Rule Type or disabling the Admin Status.

#### 4.10.4.9.3 Active Rule Type

The Active Rule Type parameter defines which of the Filtering Rules List is used.

The available options are Layer 2 and Layer 3/4.

The default option is Layer 2.

#### 4.10.4.9.4 Admin Status

The Admin Status parameter defines whether the filtering mechanism is enabled or disabled.

The default option is Disabled.

#### 4.10.4.9.5 Default Action

The Default Action parameter defines the action to be taken for a frame matching any of the applicable Filtering Rules: Deny (discard) or Allow (forward).

If the Default Action is Allow, all frames matching any of the applicable Filtering Rules will be forwarded, and all other frames will be discarded.

If the Default Action is Deny, all frames matching any of the applicable Filtering Rules will be discarded, and all other frames will be forwarded.

#### NOTE



L3/L4 Filtering Rules are applicable only to IP packets. If the Default Action is Allow, non-IP packets will be forwarded although they do not match any of the applicable Forwarding Rules.

The default option is Deny.

The menu also enables viewing and resetting the Non Matching Counter, which displays the total number of frames that did not match any of the applicable Filtering Rules, accumulated since the last reset. The counter will be reset also after changing the Active Rule Type or disabling the Admin Status.

#### NOTE



- Broadcasts and Management frames received from the network, whose destination is the NPU, are never filtered.

- ARP messages will be forwarded automatically if the following conditions are met:

1. Active Rule Type is L3/L4.
2. The L3/L4 Filtering Rules List includes at least one L4 Filtering Rule (a defined protocol).
3. The Default Action is Allow.

This is applicable for both interfaces.



#### 4.10.4.10 Filtering Examples

##### **Example 1: Block All Broadcasts Except ARP and PPPoE**

To block all broadcasts except ARP and PPPoE, define an L2 Filtering Rule that includes all other broadcasts. Typically this includes broadcasts with IP Ethertype. The parameters of this rule will be:

- MAC Address: FF-FF-FF-FF-FF-FF
- MAC Address Mask: FF-FF-FF-FF-FF-FF
- MAC Address Direction: Destination
- Ethertype: 800

Assuming the intention is to block this broadcast in both directions, this Filtering Rule should be included in the L2 Filtering Rules List of both the From Network Filtering and the From Wireless Filtering. In addition, for both Interfaces the following configuration should be defined:

- Active Rule Type: Layer 2
- Admin Status: Enabled
- Default Action: Deny

If broadcasts using other Ethertypes except IP, ARP and PPPoE are excepted, similar Layer 2 Filtering Rules should be defined for these Ethertypes (with the broadcast MAC Address), and these rules should be added to the applicable Layer 2 Filtering Rules Lists.

##### **Example 2: Block DHCP Server behind SU**

To prevent the use of a DHCP server behind an SU, define the following L3/L4 Filtering Rule:

- IP Address: Any (empty)
- Protocol: 17 (UDP)
- Port: 67 (the source port of the DHCP server)
- Port Direction: Source

This Filtering Rule should be included in the L3/L4 Filtering Rules List of the From Wireless Filtering. In addition, the following configuration should be defined for the From Wireless Filtering Interface:

- Active Rule Type: Layer 3/4
- Admin Status: Enabled
- Default Action: Deny

#### 4.10.4.11 MAC Addresses Deny List

The MAC Addresses Deny List menu enables viewing and editing the MAC Addresses Deny List. This list is used to deny services to MAC Addresses behind SUs. Uplink frames whose source MAC address matches any of the entries in the list and downlink frames whose destination MAC address matches any of the entries in the list will be discarded.

The MAC Addresses Deny List menu also enables viewing and resetting the MAC Addresses Deny List Counters, which display for each of the entries in the list the number of frames that were discarded because they match the entry, accumulated since the last reset.

### 4.10.5 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.

### 4.10.6 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 to its default configuration (Set Factory Defaults), pre-configured Profiles that were modified are not affected.

The pre-configured Service Profiles are:

- **Internet Access L2** - for basic Internet Access service with Best Effort QoS, utilizing L2 Service Type. This is the recommended Default Service Profile for Quick Mode.
- **Internet Access PPPoE** - 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 B](#).

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 protocols.

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 4-10: 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 [Section 4.10.1.5](#).

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 4-11: 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 [Section 4.10.1.5](#).

**Table 4-12: 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

**Table 4-12: Pre-Configured Priority Classifiers for Data Services**

Name	Type	Uplink Priority Ranges	Uplink QoS Profiles	Downlink Priority Ranges	Downlink QoS Profiles
Bronze Symmetric	802.1p	7	NRT 750/850	7	NRT 750/850

**Table 4-13: 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 4-14: 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 [Section 4.10.1.5](#).

\*\* 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 4-15: 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

**Table 4-15: Pre-Configured Service Profiles for Generic (non-DRAP) VoIP Services**

Name	Service Type	VPL ID*	Forwarding Rule	Priority Classifier
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 [Section 4.10.1.5](#).

**Table 4-16: 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 [Section 4.10.1.5](#).

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 4-17: 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	BE64	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

**Table 4-17: 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 Advanced VoIP G.711	DSCP	0	BE 64	0	BE 64
		26	RT 11	26	RT 11
		63	CG 88	63	CG 88

**Table 4-18: 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 4-19: 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

The following tables provide details on the pre-configured Profiles used for Transparent Services (VLAN Transparency Mode is ON):

**Table 4-20: Pre-Configured Forwarding Rule for Transparent Services**

Name	Service Type	Unicast Relaying	Broadcast Relaying	Unknown Forwarding Policy	Multicast QoS	Multicast VLAN
@@Transparent@@	L2	Enable	Enable	Forward	@@Transparent@@	Null

**NOTE**

The name of the Transparent Forwarding Rule cannot be edited.



**Table 4-21: Pre-Configured QoS Profile for Transparent Services**

Name	Type	CIR (Kbps)	MIR (Kbps)	CT
@ @Transparent@ @	Best Effort	NA	128	Long

## 4.11 NPU Parameters Summary

**Table 4-22: NPU Monitor Parameters Summary**

Parameter	Range	Default	Run-Time Updated
<b>Base Station Configuration Parameters</b>			
Device Name	Up to 255 printable characters	Null	Yes
Device Location	Up to 255 printable characters	Null	Yes
ATPC Enable/Disable	1 - Disable 2 - Enable Disable is temporary until next reset of the AUs	Enable	Yes
Optimal Uplink RSSI (dBm)	-103 to -50	-69	Yes
Operator ID	X.X.X X: 0-255	186.190.0	No
Cell ID	X.X X: 0-255	0.250	No
<b>Base Station Alarms and Traps</b>			
Traps Display Filter-Minimum Severity	1 - Critical 2 - Major 3 - Minor 4 - Warning 5 - Info	Info	Yes
Traps Display Filter-Days	1 - 31 days	31 days	Yes
Traps Configuration-Admin Status	1 - Disable 2 - Enable	Enable	Yes
Trap Configuration-Severity	1 - Critical 2 - Major 3 - Minor 4 - Warning 5 - Info	Depends on trap	Yes

Table 4-22: NPU Monitor Parameters Summary

Parameter	Range	Default	Run-Time Updated
Trap Configuration-Suppression Interval	0 - 86,400 (seconds). 0 means no suppression	0 (no suppression )	Yes
<b>NPU Parameters</b>			
Administrator Password	Up to 16 printable characters, case sensitive	admin	Yes
Installer Password	Up to 16 printable characters, case sensitive	installer	Yes
Monitor Password	Up to 16 printable characters, case sensitive	monitor	Yes
Monitor Inactivity Timeout	0 - 60 minutes (0 means no timeout)	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
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 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	1 - 100 Mbps 2 - 1 Gbps	100 Mbps	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

**Table 4-22: NPU Monitor Parameters Summary**

Parameter	Range	Default	Run-Time Updated
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 or 0 for no aging	10 minutes	Yes
DRAP TTL Retries	1 - 100	4	Yes
<b>Radio Cluster Parameters</b>			
Radio Cluster ID	1 - 6		Yes
Name	Up to 32 printable characters	Null	Yes
Location	1 to 255 printable characters	The string defined for the Location parameter in Base Station menu	Yes
Sector Heading	0 - 359 (degrees)	0	Yes
Sector Beam Width	0 - 359 (degrees)	90	Yes
<b>ODU Parameters</b>			
ODU ID	1 - 24		Yes
Associated Radio Cluster	1 - 6 (must be a defined Radio cluster ID)		Yes
Configured ODU Frequency Band	According to loaded Frequency Bands file	0 (Not Defined)	Yes
Tx Power (dBm)	13 - 50 (dBm, in increments of 0.25) Actual value depend on ODU Type	28	Yes
Admin Status	1 - Disable 2 - Enable	Disable	Yes
<b>AU MAC Parameters</b>			
Sector ID	0-255	206	No
ARQ Enable/Disable	1 - Disable 2 - Enable	Disable	No
Maximum Cell Radius (km)	10 -110 km using 10 km steps	20 km	No
<b>AU Phy Parameters</b>			

Table 4-22: NPU Monitor Parameters Summary

Parameter	Range	Default	Run-Time Updated
Bandwidth (MHz)	1 - 1.75 2 - 3.5	3.5	No
<b>AU Multi Channel Parameters</b>			
Channel ID	1 - 4 (1 - 2 in version 2.0)		
Associated ODU	1 - 24 (must be a defined ODU ID)		No
Downlink (Tx) Frequency (MHz)	According to the Configured ODU Frequency Band and AU Bandwidth		No
Admin Status	1 - Disable 2 - Enable	Disable	No
<b>AU Multirate Parameters</b>			
Multirate Enable/Disable	1 - Disable 2 - Enable Disable is temporary until next reset	Enable	Yes
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

**Table 4-22: NPU Monitor Parameters Summary**

Parameter	Range	Default	Run-Time Updated
<b>AU Voice Parameters</b>			
Maximum Number of Voice Calls	0 - 300	50	Yes
<b>SU Control Parameters</b>			
SU Status	1 - Permanent 2 - Temporary	Permanent	Yes
<b>SU Registration Parameters</b>			
Name	Up to 32 printable characters		Yes
Organization Name	Read-only		NA
Address	Read-only		NA
Country	Read-only		NA
<b>SU MAC Parameters</b>			
Base Station ID	X.X.X.X.X X: 0 - 255		No
Base Station ID Mask	X.X.X.X.X X: 0 - 255		No
<b>SU Phy Parameters</b>			
Bandwidth (MHz)	1 - 1.75 2 - 3.5		No
Uplink (Tx) Frequency (MHz)	Depends on Frequency Bands Group available for the AU, and the Bandwidth.		No
<b>SU Multirate and ATPC Parameters</b>			

Table 4-22: NPU Monitor Parameters Summary

Parameter	Range	Default	Run-Time Updated
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
<b>SU Ethernet Port Parameters</b>			
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
<b>SU Password</b>			
Password	Up to 20 printable characters, case sensitive	installer	Yes
<b>SU Bridging Parameters</b>			
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
<b>Services - General Parameters</b>			
Service Mode	1 - Advanced 2 - Quick	Quick	Yes
Default L2/Voice Service Profile	Name of an existing L2 or Voice Service Profile, or None.	Internet Access L2	Yes

**Table 4-22: NPU Monitor Parameters Summary**

Parameter	Range	Default	Run-Time Updated
Default PPPoE Service Profile	Name of an existing PPPoE Service Profile, or None.	None	Yes
<b>Services - Subscribers Parameters</b>			
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
<b>Services - Services Parameters</b>			
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.  Up to 16 entries when Hybrid VLAN Mode is Off. Up to 15 entries when Hybrid VLAN Mode is On.		Yes
Hybrid VLAN Mode	1 - Off 2 - On		Yes
VLAN Classification Mode	1 - Off 2 - On		Yes
Access VLAN	1-4094		Yes
Admin Status	1 - Disabled 2 - Enabled		Yes
<b>Services - Service Profiles Parameters</b>			
Service Profile Name	Up to 32 printable characters.		Yes



**Table 4-22: NPU Monitor Parameters Summary**

Parameter	Range	Default	Run-Time Updated
Service Type	Applicable only for new Service Profiles (Add): 1 - L2 2 - PPPoE 3 - Voice		Yes
VLAN Transparency Mode	1 - Off 2 - On		Yes
VPL ID	0 - 4094 or null for No VPL ID.		Yes
Priority Marking Mode	1 - Transparent 2 - 802.1p 3 - DSCP		Yes
Priority Marking Value	802.1p: 0 - 7 DSCP: 0 - 63		Yes
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 - 50		Yes
<b>Services - Forwarding Rule Parameters</b>			
Forwarding Rule Name	Up to 32 printable characters		Yes
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

**Table 4-22: NPU Monitor Parameters Summary**

Parameter	Range	Default	Run-Time Updated
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. Applicable only for Services assigned to SUs with SW version below 2.0.		Yes
Multicast QoS Profile	A QoS Profile Name (up to 32 printable characters) that exists in the database		Yes
<b>Services - Priority Classifiers Parameters</b>			
Priority Classifier Name	Up to 32 printable characters		Yes
Priority Type	1 - DSCP 2 - 802.1p		Yes
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

Table 4-22: NPU Monitor Parameters Summary

Parameter	Range	Default	Run-Time Updated
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
<b>Services - QoS Profiles Parameters</b>			
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 64 - 1550 (Bytes)		Yes
Sample Interval (msec)	Applicable to CG 5 - 100 (milliseconds)		Yes
<b>L2 Filtering Rules Parameters</b>			
L2 Filtering Rule Name	Up to 32 printable characters		Yes
MAC Address	MAC address or null for Any		Yes
MAC Address Mask	MAC address		Yes
MAC Address Direction	1 - Source 2 - Destination		Yes
Ethertype	4 hexadecimal digits or null for Any		Yes
<b>L3/L4 Filtering Rules Parameters</b>			

**Table 4-22: NPU Monitor Parameters Summary**

<b>Parameter</b>	<b>Range</b>	<b>Default</b>	<b>Run-Time Updated</b>
L3/L4 Filtering Rule Name	Up to 32 printable characters		Yes
IP Address	IP address or null for Any		Yes
IP Address Mask	IP address		Yes
IP Address Direction	1 - Source 2 - Destination		Yes
Protocol	0-254 or null for Any		Yes
Port	0-65534 or null for Any		Yes
Port Direction	1 - Source 2 - Destination		Yes
<b>From Wireless Filtering/From Network Filtering Parameters</b>			
L2 Filtering Rules List - Add	L2 Filtering Rule ID		Yes
L3/L4 Filtering Rules List - Add	L3/L4 Filtering Rule ID		Yes
Active Filtering Rule Type	1 - Layer 2 2 - Layer 3/4	Layer 2	Yes
Admin Status	1 - Disabled 2 - Enabled	Disabled	Yes
Default Action	1 - Deny 2 - Allow	Deny	Yes
<b>MAC Address Deny List</b>			
Add	MAC address (of a device behind SU)		Yes



# A

---

## Appendix A - Software Upgrade

### In This Appendix:

- [“Before you Start” on page 190](#)
- [“File Loading Procedure” on page 191](#)
- [“Completing the Software Upgrade \(Switching Versions\)” on page 193](#)

## A.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/ 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/ BST:**

Select SU/AU > SW Files in NPU/ BST > Show Files.



#### **To delete an SU/AU SW file from NPU/ BST:**

Select SU/AU > SW Files in NPU/ BST > Delete a File and enter the name of the file to be deleted.

## A.2 File Loading Procedure



### To load software files:

- 1 Verify that you have IP connectivity from your computer to the NPU (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 host address is the IP address of the unit to be upgraded (NPU/ 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 *npu\_2\_0\_1\_15* to the NPU whose IP address is 172.17.31.215, use the following command:

```
tftp -i 172.17.31.215 put npu_2_0_1_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/ BST SW Versions in the unit:

Select *Unit Control>SW Versions Control>Show Versions*.



**To view the current SU/AU SW files in NPU/ BST:**

Select *SU/AU>SW Files in NPU/ BST>Show Files.*



## A.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/ BST: Select *Unit Control > SW Versions Control > Run from Shadow*. The system will reset automatically. After power-up, the NPU/ BST 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*.





# B

---

## Appendix B - Defining Service Profiles for Generic VoIP Gateways

### In This Appendix:

- [“Introduction” on page B-196](#)
- [“1 POTS Basic VoIP G.729 Service Profile” on page B-198](#)
- [“1 POTS Advanced VoIP G.729 Service Profile” on page B-200](#)
- [“1 POTS Basic VoIP G.711 Service Profile” on page B-202](#)
- [“1 POTS Advanced VoIP G.711 Service Profile” on page B-204](#)

## B.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.

### B.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).

### B.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.

## B.2 1 POTS Basic VoIP G.729 Service Profile

### B.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.

### B.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

### B.2.3 RTCP BW Calculation

RTCP BW is 10% of RTP: 10 % of 31.2 Kbps approximately 3.1 Kbps.

### B.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 x 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

## B.3 1 POTS Advanced VoIP G.729 Service Profile

### B.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

### B.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

### B.3.3 Voice RTCP BW Calculation

RTCP BW is 10% of RTP: 10 % of 31.2 Kbps is 3.12 Kbps.

### B.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

PPS = (14.4 Kbps bit rate) / (288 bits) = 50 pps

Note: 288 bits = 36 bytes (voice payload) \* 8 bits per byte

Bandwidth per call = total packet size (752bits) \* 50 pps = 37.6 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.

## B.3.5 FAX RTCP BW Calculation

RTCP BW is 10% of RTP: 10 % of 37.6 Kbps is 3.76 Kbps.

## B.3.6 QoS Profiles

### B.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

### B.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

### B.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

## B.4 1 POTS Basic VoIP G.711 Service Profile

### B.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.

### B.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

### B.4.3 RTCP BW Calculation

RTCP BW is 10% of RTP: 10 % of 87.2 Kbps approximately 8.7 Kbps.

### B.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

## B.5 1 POTS Advanced VoIP G.711 Service Profile

### B.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

### B.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

### B.5.3 Voice RTCP BW Calculation

RTCP BW is 10% of RTP: 10 % of 87.2 Kbps is 8.72 Kbps.

### B.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

PPS = (14.4 Kbps bit rate) / (288 bits) = 50 pps

Note: 288 bits = 36 bytes (voice payload) \* 8 bits per byte

Bandwidth per call = total packet size (752 bits) \* 50 pps = 37.6 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.

## B.5.5 FAX RTCP BW Calculation

RTCP BW is 10% of RTP: 10 % of 37.6 Kbps is 3.76 Kbps.

## B.5.6 QoS Profiles

### B.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

### B.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

### **B.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).

<b>BER</b>	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.
<b>BPSK</b>	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.
<b>BST</b>	Base Station
<b>BW</b>	Bandwidth
<b>BWA</b>	Broadband Wireless Access
<b>CBR</b>	Constant Bit-Rate
<b>CG</b>	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).
<b>CIR</b>	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.
<b>cPCI</b>	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.
<b>CPE</b>	Customer Premise Equipment. Communications equipment that resides on the customer's premises.
<b>CPLD</b>	Complex Programmable Logic Device
<b>CRC</b>	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.



---

<b>CSMA/CD</b>	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.
<b>CT</b>	Committed Time. The time interval used for measuring average information transfer rates.
<b>DHCP</b>	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.
<b>DL</b>	Down Link
<b>DOS</b>	Disk Operating System
<b>DRAP</b>	Dynamic Resources Allocation Protocol
<b>DSCP</b>	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.
<b>DiffServ</b>	See DSCP
<b>DLI</b>	Data Loss Indicator
<b>EIR</b>	Excess Information Rate. Specifies the excess rate (above the committed rate) of information that can be available to a user. The EIR is used by the traffic policing mechanism to prevent users from sending excess traffic to the network. (EIR = MIR-CIR).
<b>EMC</b>	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.
<b>ETSI</b>	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.

<b>FCC</b>	Federal Communications Commission. A U.S. government agency that supervises, licenses, and controls electronic and electromagnetic transmission standards.
<b>FDD</b>	Frequency Division Duplex. Full duplex operation by using a pair of frequencies, one for transmission and one for reception.
<b>FEC</b>	Forward Error Correction. A method of communicating data that can corrects 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.
<b>FFT</b>	Fast Fourier Transform. An algorithm for converting data from the time domain to the frequency domain; often used in signal processing.
<b>FTP</b>	File Transfer Protocol. A protocol for exchanging files over the Internet. FTP uses the Internet's TCP/IP protocols to enable data transfer.
<b>G.711</b>	A 64 Kbps PCM voice-coding technique. Described in the ITU-T standard in its G-series recommendations.
<b>G.723.1</b>	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.
<b>G.729</b>	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.
<b>GPS</b>	Global Positioning System. A system that uses satellites, receivers and software to allow users to determine their precise geographic position.
<b>H.323</b>	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.

---

<b>IB</b>	In-Band
<b>IDU</b>	Indoor Unit
<b>IEEE</b>	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.
<b>IEEE 802.1p</b>	A QoS method - A three-bit value that can be placed inside an 802.1Q frame tag.
<b>IEEE 802.16</b>	Also known as WIMAX. A group of broadband wireless communications standards for metropolitan area networks (MANs) developed by a working group of the IEEE.
<b>IEEE 802.16a</b>	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.
<b>IEEE 802.1Q</b>	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.
<b>IEEE 802.3</b>	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.
<b>IEEE 802.11b</b>	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.
<b>IEEE 802.11g</b>	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.

<b>IETF</b>	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.
<b>IF</b>	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.
<b>IP</b>	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.
<b>IPsec</b>	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.
<b>ISP</b>	Internet Service Provider
<b>ITU-T</b>	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.
<b>LAN</b>	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.
<b>LED</b>	Light Emitting Diode.

---

<b>MAC</b>	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.
<b>MAC Address</b>	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.
<b>MAN</b>	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).
<b>MIB</b>	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.
<b>MIR</b>	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.
<b>NA</b>	Not Available or Not Applicable
<b>NAT</b>	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.
<b>NIC</b>	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.
<b>NIU</b>	Network Interface Unit
<b>NLOS</b>	Non Line Of Sight. A term referring to wireless services which don't require a clear open path between sites.

<b>NMS</b>	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.
<b>NOC</b>	Network Operations Center. The physical space from which a typically large telecommunications network is managed, monitored and supervised.
<b>NPU</b>	Network Processing Unit
<b>NRT</b>	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.
<b>OA&amp;M</b>	Operation, Administration & Maintenance. Provides the facilities and the personnel required to manage a network.
<b>ODU</b>	Outdoor Unit
<b>OFDM</b>	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.
<b>OOB</b>	Out-Of-Band
<b>PER</b>	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.
<b>PHY</b>	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.

---

<b>PIU</b>	Power Interface Unit
<b>POTS</b>	Plain Old Telephone System. A basic analog telephone equipment.
<b>PSU</b>	Power Supply Unit
<b>PPPoE</b>	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.
<b>QAM</b>	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.
<b>QoS</b>	Quality of Service. Measure of performance for a transmission system that reflects its transmission quality and service availability.
<b>QPSK</b>	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.
<b>RF</b>	Radio frequency. An AC signal of high enough frequency to be used for wireless communications.
<b>RFC</b>	Request For Comments. The name of the result and the process for creating a standard on the Internet. New standards are proposed and published on the Internet, as a Request For Comments. The proposal is reviewed by the Internet Engineering Task Force.
<b>RSSI</b>	Received Signal Strength Indicator. A signal or circuit that indicates the strength of the incoming (received) signal in a receiver.

<b>R&amp;TTE</b>	Radio & Telecommunications Terminal Equipment. The R&TTE Directive 1999/5/EC governs the marketing and use of R&TTE equipment. With the exception of a few categories of equipment, the Directive covers all equipment, which uses the radio frequency spectrum. It also covers all terminal equipment attached to public telecommunication networks.
<b>RT</b>	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.
<b>RTCP</b>	RTP Control Protocol. A protocol that monitors the QoS of an RTP connection and conveys information about the on-going session.
<b>RTP</b>	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.
<b>Rx</b>	Receive
<b>SIP</b>	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.



---

<b>SLA</b>	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.
<b>SME</b>	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.
<b>SNAP</b>	Sub Network Access Protocol
<b>SNMP</b>	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.
<b>SNR</b>	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.
<b>SOHO</b>	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.
<b>SRC</b>	Source
<b>SU</b>	Subscriber Unit
<b>TCP</b>	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.

<b>TCP/IP</b>	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.
<b>TDM</b>	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.
<b>TFTP</b>	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.
<b>TTL</b>	Time To Live
<b>Tx</b>	Transmit
<b>BST</b>	Micro Base Station
<b>U</b>	A unit for measuring the height in rack cabinets. 1U = 1.75 inches.
<b>UDP</b>	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.
<b>UL</b>	Up Link
<b>VLAN</b>	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.
<b>VLSI</b>	Very Large Scale Integration. The process of placing thousands (or hundreds of thousands) of electronic components on a single chip.
<b>VoIP</b>	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.

<b>VPL</b>	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).
<b>VPN</b>	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.
<b>WAN</b>	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.
<b>WEEE</b>	Waste Electronic and Electrical Equipment. The WEEE EU Directive
<b>WIMAX</b>	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.



## Numerics

- 1 POTS Advanced VoIP G.711 Pre-configured Profile, 172
- 1 POTS Advanced VoIP G.729 Pre-configured Profile, 172
- 1 POTS Basic VoIP G.711 Pre-configured Profile, 172
- 1 POTS Basic VoIP G.729 Pre-configured Profile, 172
- 802.1p Marking Mode, 156

## A

- Access Unit Indoor Module, 39
- Access VLAN, 150
- Active Alarms
  - Show, 75
- Active Rule Type, 167
- Add
  - Authorized Manager, 93
  - New SU, 136
  - ODU, 103
  - Radio Cluster, 99
- Add New SU, 136
- Address, 129
- Admin Status
  - Channel, 115
  - Interface Filtering, 168
  - ODU, 104
  - Service, 151
  - Subscriber, 148
  - Trap Configuration, 77
- Administrator Password, 83
- Advanced Service Mode, 140
- Air Ventilation Unit, 47
- Alarms and Traps, 75
- ARQ Enable/Disable, 112
- Associated ODU, 114
- Associated Radio Cluster, 103
- ATPC Enable/Disable, 74
- ATPC Parameters, 74
- AU
  - Bandwidth, 113
  - Base Station ID Parameters, 112
  - Configuration Menu, 111
  - MAC Parameters, 111
  - Maximum Number of Voice Calls, 117
  - Menu, 106
  - Multirate Parameters, 115
  - Performance Monitoring, 117
  - Phy Parameters, 113
  - Reset Unit, 109
  - Select, 107
  - Set Factory Defaults, 109
  - Show Summary, 106
  - SW Files in NPU, 107
  - SW Versions Control, 109
  - Unit Control, 109
  - Voice Parameters, 117
- AU Slot #
  - Menu, 107
  - Show, 107
- AU Wireless Port Counters, 118
- AU-IDU, 39
  - Ejecting, 45
  - Inserting, 44
  - LEDs, 40
- AU-ODU
  - Connectors, 31
  - Installation, 24
  - LEDs, 31
- Authorized Managers
  - Add, 93
  - IP Address, 93

- Parameters, 93
  - Read Community, 93
  - Select, 93
  - Send Traps, 93
  - Show All, 93
  - Write Community, 93
- AVU, 47
- LEDs, 48
  - Replacing, 48
- ## B
- Back Panel Port Counters, 118
- Backup File
- Creating, 86
  - Filtering, 86
  - Full, 86
  - Profiles, 86
  - Profiles and Services, 86
  - Traps Configuration, 86
  - Upload/Download, 86
- Bandwidth
- AU, 113
  - SU, 130
- Base Station
- Chassis, 34
  - Chassis Slot Assignment, 73
  - Configuration Menu, 73
  - Installation, 33
  - Power Cable, 37
  - Power Requirements, 35
  - Show, 72
- Base Station ID
- AU, 112
  - SU, 130
- Base Station ID Mask, 130
- Base Station Licenses, 79
- Basic Parameters, 56
- BE, 162
- Best Effort (BE) Qos Profile, 162
- Bridge Aging Time
- NPU, 94
  - SU, 133
- Bridging Parameters (SU), 133
- Broadcast Relaying, 159
- Bronze Lan-to-Lan Pre-configured Profile, 171
- Bronze Teleworking Pre-configured Profile, 171
- Burst Error Rate Counters
- AU, 119
  - SU, 135
- ## C
- Cell ID, 75
- Cell Parameters, 74
- CG, 162
- Change Password, 83
- Channel
- Admin Status, 115
  - Associated ODU, 114
  - Associated Radio Cluster, 115
  - Downlink (Tx) Frequency, 114
  - Frequency Band, 115
  - Select, 114
  - Tx Power, 115
  - Uplink (Rx) Frequency, 115
- Chassis, 34
- Slot Assignment, 73
- CIR, 164
- Committed Information Rate, 164
- Committed Time, 163
- Configuration
- AU, 111
  - Base Station Parameters, 73
  - NPU, 87
  - SU, 128
- Configured Operation
- AU, 106
  - SU, 121
- Configured SW File Name
- AU, 106
  - SU, 120
- Configured SW Version
- AU, 106
  - SU, 120
- Connectors

- AU-ODU, 31
  - NPU, 42
  - ODU Power Feeder, 51
  - Continuous Grant (CG) QoS Profile, 162
  - Counters
    - AU Ports, 118
    - Back Panel Port, 118
    - Burst Error Rate (AU), 119
    - Burst Error Rate (SU), 135
    - Data Port, 95
    - Management Port, 97
    - Service, 151
    - SU Ethernet Port, 134
    - SU Port, 134
    - Wireless Port (AU), 118
    - Wireless Port (SU), 134
  - Country, 129
  - CPEs License Bank, 79
  - Create Backup, 86
  - CT, 163
- D**
- Data Port
    - Auto Negotiation Option, 91
    - Gateway, 91
    - IP Address, 91
    - Management Traffic Enable/Disable, 91
    - Management VLAN, 91
    - Parameters, 90
    - Speed, 91
    - Subnet Mask, 91
  - Data Port Counters, 95
  - Days, 76
  - DC Power Cable
    - ODU Power Feeder, 52
  - Default Action, 122
    - Interface Filtering, 168
  - Default File Name, 122
  - Default L2/Voice Service Profile, 147
  - Default PPPoE Service Profile, 147
  - Defining Services, 170
  - Delete
    - AU SW File (in NPU), 107
    - ODU, 103
    - SU, 136
    - SU SW File, 123
  - Dest Subnet, 89
  - Dest Subnet Mask, 89
  - Device Location, 73
  - Device Name, 73
  - Downlink (Tx) Frequency (Channel), 114
  - Downlink Basic Rate (AU), 117
  - Downlink QoS Profiles, 161
  - Downlink Upper Priority Limits, 161
  - DRAP
    - Description, 139
  - DRAP TTL Retries, 94
  - DSCP Marking Mode, 157
  - Duplicate SU Name, 121
- E**
- Eject
    - AU-IDU, 45
    - NPU, 45
    - PIU (with HOT SWAP), 45
    - PIU (without HOT SWAP), 46
    - PSU, 46
  - Enable/Disable Limit on Number of Supported Devices (SU), 133
  - Ethernet Port (SU), 132
  - Ethertype (L2 Filtering Rule), 165
- F**
- File Loading Procedure, 191
  - Filtering Rules
    - Menu, 164
  - First Name, 148
  - Forwarding Rule
    - Broadcast Relaying, 159
    - Definition, 137
    - Menu, 158
    - Multicast QoS Profile, 160
    - Multicast VLAN ID, 159
    - Name, 158

- Service Type, 158
- Unicast Relaying, 159
- Unkown Forwarding Policy, 159
- Forwarding Rule Name, 158
- Frequency Bands File, 104
- Frequency Bands Groups, 104
- From Network Filtering, 167
- From Wireless Filtering, 167

**G**

- Gateway
  - Data Port, 91
  - Management Port, 89
- General Service Parameters
  - Default L2/Voice Service Profile, 147
  - Default PPPoE Service Profile, 147
  - Menu, 147
  - Service Mode, 147
  - Show, 147
  - Update, 147
- Gold Lan-to-Lan Pre-configured Profile, 171
- Gold Teleworking Pre-configured Profile, 171
- Grace Licenses, 79

**H**

- HOT SWAP, 35
- Hybrid VLAN Mode, 149

**I**

- IDU Type, 121
- IF Cables, 25
- Insert
  - AU-IDU, 44
  - PIU (with HOT SWAP), 44
  - PIU (without HOT SWAP), 45
  - PSU, 45
- Inserting
  - NPU, 44
- Installation, 23
  - AU-ODU, 24
  - Base Station, 33

- ODU Power Feeder, 50
- Installer Password
  - NPU, 83
  - SU, 133
- Interface Filtering
  - Active Rule Type, 167
  - Admin Status, 168
  - Default Action, 168
  - From Network Filtering, 167
  - From Wireless Filtering, 167
  - L2 Filtering Rules List, 167
  - L3/L4 Filtering Rules List, 167
  - Menu, 167
- Internet Access L2 Pre-configured Profile, 171
- Internet Access PPPoE Pre-configured Profile, 171
- IP Address
  - Authorized Managers, 93
  - Data Port, 91
  - L3/L4 Filtering Rule, 166
  - Management Port, 88
- IP Address Direction (L3/L4 Filtering Rule), 166
- IP Address Mask (L3/L4 Filtering Rule), 166

**L**

- L2 Filtering Rules
  - Ethertype, 165
  - MAC Address, 165
  - MAC Address Direction, 165
  - MAC Address Mask, 165
  - Menu, 164
  - Rule Name, 165
- L2 Filtering Rules List, 167
- L2 Service, 138
- L3/L4 Filtering Rules
  - IP Address, 166
  - IP Address Direction, 166
  - IP Address Mask, 166
  - Menu, 165
  - Port, 167
  - Port Direction, 167
  - Protocol, 166
  - Rule Name, 166



- 
- L3/L4 Filtering Rules List, 167
  - Last Name, 148
  - LEDs
    - AU-IDU, 40
    - AU-ODU, 31
    - AVU, 48
    - NPU, 43
    - ODU Power Feeder, 52, 62
    - PIU, 37
    - PSU, 39
  - Loop, 121
  
  - M**
  - MAC Address (L2 Filtering Rule), 165
  - MAC Address Direction (L2 Filtering Rule), 165
  - MAC Address Mask (L2 Filtering Rule), 165
  - MAC Addresses Deny List, 170
  - MAC Parameters
    - AU, 111
    - SU, 129
  - Management Port
    - Dest Subnet, 89
    - Dest Subnet Mask, 89
    - Gateway, 89
    - IP Address, 88
    - Management Traffic Enable/Disable, 90
    - Parameters, 88
    - Subnet Mask, 89
  - Management Port Counters, 97
  - Management Traffic Enable/Disable
    - Data Port, 91
    - Management Port, 90
  - Management VLAN (Data Port), 91
  - Marking Mode
    - 802.1p, 156
    - DSCP, 157
    - Transparent, 156
  - Maximum Cell Radius, 112
  - Maximum Information Rate, 164
  - Maximum Number of Supported Devices
    - SU, 133
  - Maximum Number of Voice Calls
    - AU, 117
    - Service Profile, 158
  - Minimum Severity, 75
  - MIR, 164
  - Monitor
    - Via Telnet, 67
    - Via the MON Port, 66
  - Monitor Inactivity Timeout, 87
  - Monitor Password, 83
  - Multi Channel
    - Show Summary, 113
  - Multi Channel Parameters, 113
  - Multicast QoS Profile, 160
  - Multicast VLAN ID, 159
  - Multirate Algorithm, 115
  - Multirate and ATPC Parameters (SU), 131
  - Multirate Enable/Disable (AU), 117
  - Multirate Parameters
    - AU, 115
  
  - N**
  - Network Processing Unit, 41
  - Non Real Time (NRT) QoS Profile, 162
  - NPU, 41
    - Bridge Aging Time, 94
    - Configuration Menu, 87
    - Connectors, 42
    - Ejecting, 45
    - Inserting, 44
    - LEDs, 43
    - Menu, 81
    - Performance Monitoring, 95
    - Replacing, 48
    - Reset Unit, 84
    - Run from Shadow, 85
    - Set as Main, 85
    - Set Factory Defaults, 84
    - Show, 81
    - SW Versions Control, 84
    - Unit Control, 83
  - NRT, 162
  - Number of Gateways, 121

**O**

## ODU

- Add, 103
- Admin Status, 104
- Associated Radio Cluster, 103
- Configured ODU Frequency Band, 103
- Delete, 103
- ID, 103
- Menu, 101
- Parameters, 103
- Select, 102
- Show, 102
- Show Summary, 101
- Tx Power, 103
- Update, 102

## ODU Power Feeder

- Connectors, 51
- Installation, 50
- LEDs, 52, 62

## Operation Status

- Service, 151

## Operator ID, 74

## Optimal Uplink RSSI, 74

## Organization Name, 129

**P**

## Packet Size, 164

## Password

- Defaults (NPU), 84
- NPU, 83

## Performance

- Service, 151

## Performance Monitoring

- AU, 117
- NPU, 95
- SU, 133

## Permanent SU

- Definition, 140

## Phy Parameters

- AU, 113
- SU, 130

## PIU, 35

- LEDs, 37

## PIU (with HOT SWAP)

- Ejecting, 45
- Inserting, 44

## PIU (without HOT SWAP)

- Ejecting, 46
- Inserting, 45

## Port (L3/L4 Filtering Rule), 167

## Port Direction (L3/L4 Filtering Rule), 167

## Ports Counters

- AU, 118

## Power Cable, 37

## Power Interface Unit, 35

## Power Requirements, 35

## Power Supply Unit, 38

## PPPoE Service, 138

## Pre-configured Profiles, 171

## Priority Classifier

- Definition, 137
- Downlink QoS Profiles, 161
- Downlink Upper Priority Limits, 161
- Menu, 160
- Name, 160
- Priority Type, 160
- Uplink QoS Profiles, 161
- Uplink Upper Priority Limits, 161

## Priority Classifier Name, 160

## Priority Marking Mode, 155

## Priority Marking Value, 157

## Priority Type, 160

## Profiles

- Pre-configured, 171

## Protocol (L3/L4 Filtering Rule), 166

## PSU, 38

- Ejecting, 46
- Inserting, 45
- LEDs, 39

**Q**

## QoS Profile

- Best Effort (BE) Service Type, 162

- CIR, 164
  - Continuous Grant (CG) Service Type, 162
  - CT, 163
  - Menu, 162
  - MIR, 164
  - Name, 163
  - Non Real Time (NRT) Service Type, 162
  - Packet Size, 164
  - QoS Type, 163
  - Real Time (RT) Service Type, 162
  - Sample Interval, 164
  - QoS Profile Name, 163
  - QoS Type, 163
  - Quick Service Mode, 140
- R**
- Radio Cluster
    - Add, 99
    - ID, 99
    - Location, 99
    - Menu, 98
    - Name, 99
    - Parameters, 99
    - Sector Beam Width, 100
    - Sector Heading, 99
    - Select, 98
    - Show Summary, 98
  - Read Community (Authorized Manager), 93
  - Real Time (RT) QoS Profile, 162
  - Registration Parameters
    - SU, 129
  - Replace
    - AVU, 48
    - NPU, 48
  - Reset Unit
    - AU, 109
    - NPU, 84
    - SU, 126
  - RT, 162
  - Run from Shadow
    - AU, 110
    - NPU, 85
  - SU, 128
- S**
- Sample Interval, 164
  - Sector Heading, 99
  - Sector ID, 112
  - Select
    - AU, 107
    - Authorized Managers, 93
    - Channel, 114
    - ODU, 102
    - Radio Cluster, 98
  - Select by MAC Address
    - SU, 123
  - Select by Name
    - SU, 123
  - Send Traps (Authorized Manager), 93
  - Service
    - Access VLAN, 150
    - Admin Status, 151
    - Best Effort, 162
    - Continuous Grant, 162
    - Definition, 137
    - General Parameters, 147
    - Generic VoIP (non DRAP-based), 140
    - Hybrid VLAN Mode, 149
    - L2, 138
    - Menu, 148
    - Name, 148
    - Non Real Time, 162
    - Operation Status, 151
    - Performance, 151
    - PPPoE, 138
    - Real Time, 162
    - SU MAC Address, 149
    - Types, 138
    - VLAN Classification Mode, 150
    - VLAN List, 149
  - Service Fault Status, 121
  - Service Mode, 147
    - Definition, 140
  - Service Profile

- Definition, 137
- Maximum Number of Voice Calls, 158
- Menu, 153
- Name, 153
- Priority Marking Mode, 155
- Priority Marking Value, 157
- Service Type, 153
- VLAN Transparency Mode, 153
- VPL ID, 154
- Service Profile Name, 153
- Service Type
  - L2, 138
  - PPPoE, 138
  - Voice, 139
- Services
  - Defining, 170
  - Voice (DRAP-based), 139
- Set as Main
  - AU, 111
  - NPU, 85
  - SU, 128
- Set Factory Defaults
  - AU, 109
  - NPU, 84
  - SU, 126
- Set Rates, 131
- Severity
  - Trap Configuration, 77
- Show
  - AU Slot #, 107
  - Base Station Licenses, 79
  - Base Station Parameters, 72
  - CPEs License Bank Status, 79
  - General Service Parameters, 147
  - Grace Licenses, 79
  - NPU Parameters, 81
  - ODU, 102
  - SU #, 123
  - Temporary Grace Licenses, 79
- Show Active Alarms, 75
- Show All
  - Authorized Managers, 93
  - Show MAC Addresses Behind SU, 136
- Show Summary
  - AU, 106
  - Multi Channel, 113
  - ODU, 101
  - Radio Cluster, 98
  - SU, 120
  - SUs by AU, 122
- Show Traps Log, 76
- Silver Lan-to-Lan Pre-configured Profile, 171
- Silver Teleworking Pre-configured Profile, 171
- Software Upgrade, 189
- Speed
  - Data Port, 91
- SU
  - Add New SU, 136
  - Address, 129
  - Bandwidth, 130
  - Base Station ID, 130
  - Base Station ID Mask, 130
  - Bridge Aging Time, 133
  - Bridging Parameters, 133
  - Configuration Menu, 128
  - Configured Operation, 121
  - Configured SW File Name, 120
  - Configured SW Version, 120
  - Country, 129
  - Default Action, 122
  - Default File Name, 122
  - Delete, 136
  - Delete SW File, 123
  - Duplicate SU Name, 121
  - Ethernet Port, 132
  - IDU Type, 121
  - Installer Password, 133
  - Loop, 121
  - MAC Parameters, 129
  - Menu, 120
  - Multirate and ATPC Parameters, 131
  - Number of Gateways, 121
  - Organization Name, 129
  - Performance Monitoring, 133

- Phy Parameters, 130
- Registration Parameters, 129
- Reset Unit, 126
- Select by MAC Address, 123
- Select by Name, 123
- Service Fault Status, 121
- Set Factory Defaults, 126
- Set Rates, 131
- Show Summary, 120
- Status, 126
- SU Name, 129
- SW Files in NPU, 122
- SW Versions Control, 126
- Unit Control, 125
- Uplink (Tx) Frequency, 130
- Voice/Networking Gateways, 131
- SU #
  - Menu, 123
  - Show, 123
- SU Ethernet Port Counters, 134
- SU MAC Address
  - Service, 149
- SU Name, 129
- SU Ports Counters, 134
- SU Status, 126
- SU Wireless Port Counters, 134
- Subnet Mask
  - Data Port, 91
  - Management Port, 89
- Subscriber
  - Admin Status, 148
  - Definition, 137
  - Description, 148
  - First Name, 148
  - Last Name, 148
  - Menu, 147
  - Name, 147
- Subscriber Name, 148
- Suppression Interval, 77
- SW Files in NPU
  - AU, 107
  - SU, 122

- SW Versions Control
  - AU, 109
  - NPU, 84
  - SU, 126

## T

- Temporary Grace Licenses, 79
- Temporary SU
  - Definition, 140
- Transparent Marking Mode, 156
- Trap Configuration, 76
  - Admin Status, 77
  - Severity, 77
  - Suppression Interval, 77
- Traps
  - Display Filter, 75
  - Log, 76
- Traps Display Filter
  - Days, 76
  - Minimum Severity, 75
- Tx Power (ODU), 103

## U

- Unicast Relaying, 159
- Unit Control
  - AU, 109
  - NPU, 83
  - SU, 125
- Unknown Forwarding Policy, 159
- Update
  - General Service Parameters, 147
  - ODU, 102
- Uplink (Tx) Frequency
  - SU, 130
- Uplink Basic Rate (AU), 117
- Uplink QoS Profiles, 161
- Uplink Upper Priority Limits, 161

## V

- VLAN Classification Mode, 150
- VLAN List, 149

VLAN Transparency Mode, 153

Voice Parameters (AU), 117

Voice Service, 139

Voice/Networking Gateways (SU), 131

VoIP 1V Pre-configured Profile, 172

VoIP 2V Pre-configured Profile, 172

VPL ID, 154

## W

Write Community (Authorized Manager), 93