alvarion®
Your Open WiMAX Choice

BreezeCONFIG™ for BreezeACCESS® VL and BreezeACCESS® 4900

User Manual

SW Version 4.5
August 2007
P/N 214657

Document History

Topic	Description	Version/Date Issued
Gateways tab Section 2.2.5	New tab, displaying information on Voice/Networking Gateways behind SUs when DRAP feature is enabled	SW Version 4.0, July 2006
Per SU Distance Learning Section 2.4.1	A change in Air Interface General tab (AU): A new mode of calculating the ACK timeout parameter.	SW Version 4.0, July 2006
Beacon Watchdog Section 2.4.1	A change in Air Interface General tab: A new feature for resetting AU when it is not able to send beacons for a certain period of time	SW Version 4.0, July 2006
Frequency tab Section 2.4.2	Enhanced User Interface for the Planned Frequency Definition table.	SW Version 4.0, July 2006
Power Tables tab Section 2.4.3	New parameters to simplify settings of power parameters: Transmit Power, Maximum Tx Power (SU). Revised functionality of the tables (read-only). Enhanced functionality of Tx Control.	SW Version 4.0, July 2006
Low Priority Traffic Minimum Percent Section 2.7.1	A new parameter in Bridging General tab: Defining percentage of guaranteed low priority traffic.	SW Version 4.0, July 2006
Service Provider Link Section 2.7.2	Changes in Bridging VLAN tab: A new option in Ethernet Link Type parameter, new Q in Q parameters for Service Provider link.	SW Version 4.0, July 2006
Allow/Deny List Section 2.7.3	A change of functionality: The list is now a Deny or Allow list, according to the configuration of the new List Type parameter.	SW Version 4.0, July 2006
Maximum Concatenated Frame Size Section 2.8	Changes in Performance tab: New concatenation parameter replacing the Maximum Number of Frames parameter.	SW Version 4.0, July 2006
DRAP Section 2.9.3	New tab: Implementation of the DRAP protocol used by AUs to communicate with Voice/Networking Gateways and to manage voice calls	SW Version 4.0, July 2006
WL Priority Section 2.9.4	New tab: Wireless Link Prioritization parameters (a licensed feature)	SW Version 4.0, July 2006
FIPS-197 Section 2.10	A change in Security tab: A new Security Mode option (a license feature, applicable only for units with HW C or higher)	SW Version 4.0, July 2006

Topic	Description	Version/Date Issued
SW Version in Trap Monitor Section 2.12	New trap variable added	SW Version 4.0, July 2006
Maximum Num of Associations Limit Section 2.4.1	The range of Maximum Num of Associations Limit parameter (in the Air Interface General tab) for an upgraded AUS is from 0 to 25.	SW Version 4.0, October 2006
Q in Q Ethertype Section 2.7.2	VLAN Q in Q Ethertype supports also the Ethertypes 9100 and 9200 (hex)	SW Version 4.0, October 2006
Unit Control Section 2.1	Added ATE Test Result and Serial No.	SW Version 4.5, July 2007
Unit Status Section 2.2.1	Added AP Working Mode (not applicable for current release)	SW Version 4.5, July 2007
Country Parameters Section 2.4.4	Added Re-apply Country Code Values. Updated description of Sub-Band Index.	SW Version 4.5 July 2007
DFS Parameters Section 2.4.6	DFS Option changed to DFS Required by Regulations (options are No or Yes)	SW Version 4.5 July 2007
General Network Management Parameters Section 2.6.1	Added AP Client IP, changed table's name to Network Management IP Address Ranges	SW Version 4.5 July 2007
General Service Parameters Section 2.9.1	Added MIR Threshold (%) parameter (AU)	SW Version 4.5 July 2007
General Bridging Parameters Section 2.7.1	Broadcast/Multicast Relaying – changed name and functionality	SW Version 4.5 July 2007
Scan Period parameter in Spectrum Analysis Section 2.4.5	Updated description	SW Version 4.5 July 2007
HTTP Browse Sections 1.2, 1.3.4	New feature of the Configuration Utility	SW Version 4.5 August 2007

Legal Rights

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

Trade Names

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

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

Statement of Conditions

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

Warranties and Disclaimers

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

Exclusive Warranty

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

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 is intended for BreezeACCESS VL and BreezeACCESS 4900 System Administrators.

The BreezeCONFIG for BreezeACCESS VL, BreezeACCESS 4900 and BreezeNET B is an SNMP-based (Simple Network Management Protocol) application designed to manage BreezeACCESS VL, BreezeACCESS 4900 and BreezeNET B system components. The system administrator can use the BreezeCONFIG utility to control a large number of units from a single location. This guide provides information on using the BreezeCONFIG for configuring, monitoring and upgrading BreezeACCESS VL and BreezeACCESS 4900 units.

The BreezeCONFIG utility features:

- Unit status and current configuration verification
- Selected unit configuration modification
- Simultaneous configuration modification of multiple units
- Firmware upgrading for single or multiple units
- Traffic statistics and performance data monitoring
- Trap monitoring

Contents

Figures

1

Chapter 1 - Getting Started

In This Chapter:

1.1 Installing the BreezeCONFIG Utility

The executable BreezeCONFIG file (BreezeCONFIG_X_Y_Z.exe, where X_Y_Z is the version number) is available in the BreezeCONFIG folder in the BreezeACCESS VL or BreezeACCESS 4900 documentation CD. It is also recommended to check the Alvarion web site for the most updated version.

Run the executable program and follow the instructions to install the BreezeCONFIG utility on your PC.

1.2 Introducing the Configuration Utility Window

The main BreezeCONFIG window, which is referred to as the *Configuration Utility* window, enables you to access a wide array of monitoring and configuration options, which are described in the following sections.

This section describes how to access the *Configuration Utility* window and provides a brief description of each window component.

To access the Configuration Utility window:

1 From the Windows *Start* menu, select ***Programs*** and then select ***BreezeCONFIG***.

2 From the displayed menu, select ***BreezeCONFIG***. The *Configuration Utility* window is displayed, as shown below.

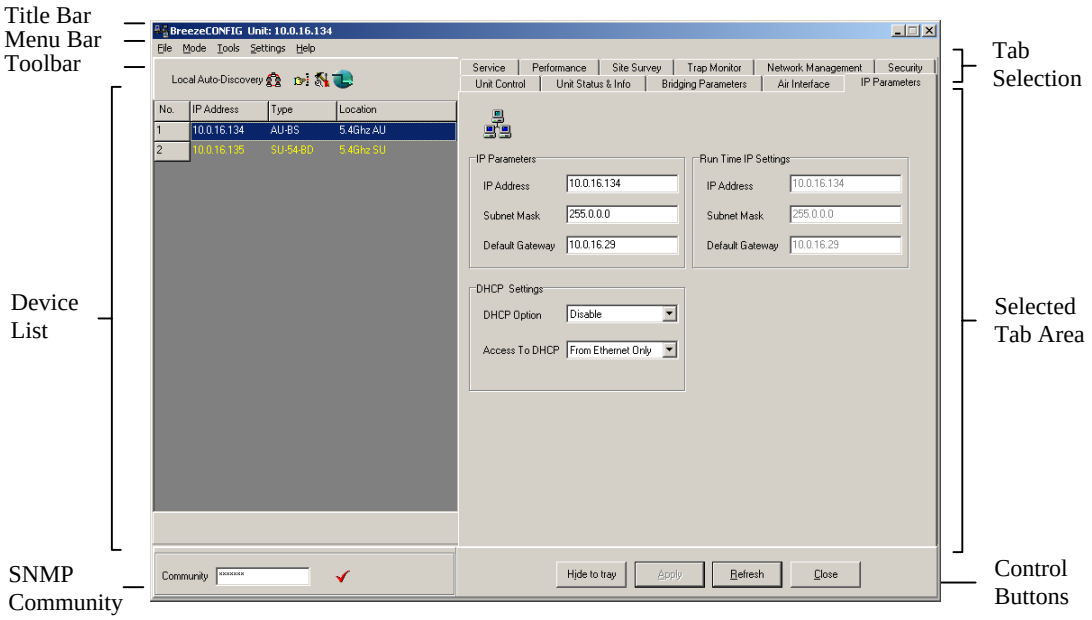


Figure1-1: Configuration Utility Window

The *Configuration Utility* window is comprised of the following components:

- **Title Bar:** Identifies the application's name and the IP address of the selected unit (in Unit Configuration mode). It also includes standard icons for minimizing or closing the application.

- **Menu Bar:** Enables you to access multiple options and application functionality. For more information, refer to section 1.4.

- **Toolbar:** The toolbar is comprised of the following four buttons:

  Local Network Autodiscovery: Automatically discovers stations connected to the local (Ethernet) network.

  Locate Device: Locates an individual unit by its IP address.

  Set IP: Sets a unit's IP address based on its MAC address.

  HTTP Browse: Supports easy access to management of devices with a built-in web interface such as Gateways and WI2 Access Points.

  For more information, refer to section 1.3.

- **Device List:** The Device List displays the units that can currently be managed by the BreezeCONFIG utility.

  Each unit is displayed according to the unit's IP address and unit type as well as the unit location, which is defined in the *Unit Status & Info* tab.

  The Device List can be sorted by clicking one of the column headers, for example Type. The list is sorted in ascending order according to the selected column. Click the column header again to sort in descending order.

  Units are selected from this list for configuration. To select a unit, double-click the relevant row in the Device List. The entry is highlighted in black when it is selected. Information is then gathered from the device and displayed in the selected tab area. Once all information is loaded, the entry is highlighted in blue; therefore, wait until the entry highlighting turns from black to blue before reviewing or modifying the configuration.

  In Multiple Configuration mode you can use the standard Windows ***Shift*** or ***Ctrl*** key commands to select multiple units.

- **SNMP Community:** The SNMP Community area enables you to enter an SNMP community string, which is used by BreezeCONFIG when sending an SNMP request to the selected device(s).

  Unit information can be viewed only when using its Read or Read/Write community string. Otherwise the unit does not appear in the Device List. Configurable parameters can be changed only when using the Read/Write community string.

To change the community string, type the community string in the ***Community*** field. Then, click  or press Enter to confirm the new community string.

A unit's community string can be modified in the *Network Management* tab.

- **Tab Selection:** The Tab Selection area is comprised of several tabs, each corresponding to a workspace containing a specific group of parameters. The tabs and parameters contained in several of the tabs vary according to unit type. If no device is selected, the Tab Selection area comprises all possible tabs for all unit types.

- **Selected Tab Area:** The Selected Tab Area is a workspace that varies according to the selected tab, enabling you to view status or performance data and modify specific parameters.

- **Secondary Tabs:** Certain Selected Tab areas are further divided into multiple workspaces, to provide all required parameters in the selected tab category. In these cases, the Selected Tab area contains a Secondary Tabs area, as shown below.

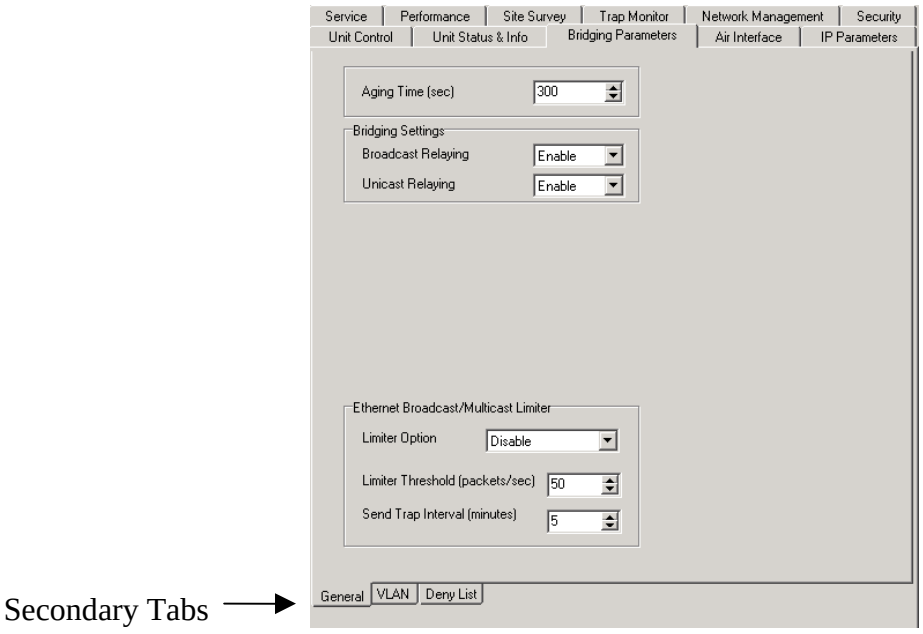
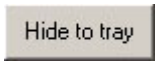
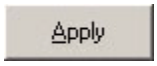


Figure 1-2: Secondary Tabs

- **Control Buttons:** *All Configuration Utility* windows contain the following buttons.



Minimizes the BreezeCONFIG. The application is minimized and displayed as  icon in the system tray. Click the icon to restore the application.



Implements the current modifications.

Updates the information displayed in the window using current values acquired from the unit.

Closes the application without implementing any modifications.

1.3 Working with the Toolbar Options

This section describes how to work with the options available through the BreezeCONFIG utility toolbar.

1.3.1 Local Network Autodiscovery

To initiate the Autodiscovery process, in the toolbar, click  . The Autodiscovery mechanism detects all stations connected to the local (Ethernet) network. The Device List is updated to reflect the devices/stations identified by the Autodiscovery process.

1.3.2 Locating a Device Based on IP Address

The Locate Device feature enables you to find an individual unit using its IP address. This includes units located behind a router, which cannot be detected by the Local Network Autodiscovery mechanism.

To locate a unit using its IP address:

3 In the toolbar, click  , or select Locate Device from the Tools menu. The *Locate Device* window is displayed, as shown below.

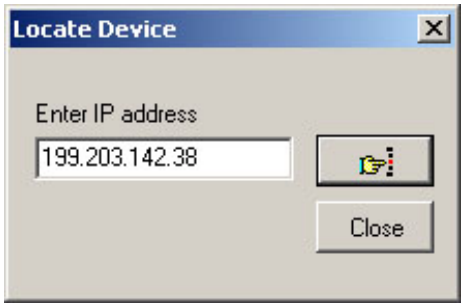
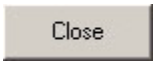


Figure 1-3: Locate Device Window

4 In the *Enter IP address field*, enter the IP address of the unit to be located and click  . Once located, the unit information is displayed in the Device List.

5 Click on 

to close the Locate Device window.

1.3.3 Setting an IP Address Based on the MAC Address

The Set IP Address feature simplifies the procedure for defining IP address information for newly added units that are still defined by their default IP settings. This feature can only be used if the management station is on the same Ethernet segment as the unit and not behind the router.

To set an IP address:

1 In the toolbar, click  , or select ***Set IP*** from the Tools menu. The *Set IP* window is displayed, as shown below.

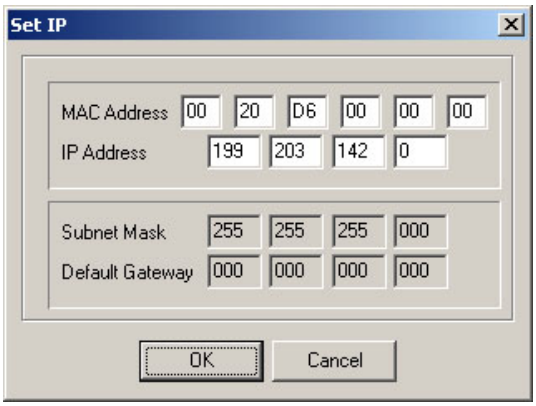


Figure 1-4: Set IP Window

2 In the **MAC Address** field, enter the unit's MAC address.

3 In the **IP Address** field, enter the required IP address for the unit.

4 In the **Subnet Mask** field, enter the required subnet mask.

5 In the **Default Gateway** field, enter the unit's default gateway.

6 Click on  to activate the changes. The unit will be reset automatically.

NOTE

In order to see the unit after assigning the IP address, the assigned IP address must be on the same IP subnet as the management station of the BreezeCONFIG utility. Otherwise, use the Locate Device feature, as described in section 1.3.2, to find the unit.

1.3.4 Opening a web-browser for a selected device

The HTTP Browser feature enables immediate access for http-based management of devices with a built-in web-interface, such as Gateways or WI² Access Points.

To open an http browser for a selected device:

1 In the toolbar, click  . The *Enter IP Address* window is displayed,.

2 Enter the IP address of the device you wish to manage using an http browser, and click OK.

3 An http browser to the selected address will be opened, enabling web-based management of the selected device.

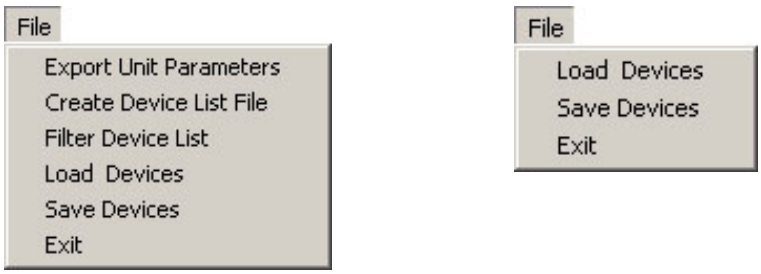
1.4 Working with the Menu Options

The following sections describe the various options available through the BreezeCONFIG menu bar. Note that the menus differ depending on the selected mode.

1.4.1 File Menu

The *File* menu available in Unit Configuration mode is different than the menu available in Multiple Configuration mode, as shown below.

The *File* menu enables you to access various operations that support the featured functionality of the BreezeCONFIG utility, as shown below.



Unit Configuration Mode **Multiple Configuration Mode**

Figure 1-5: File Menus

The File menu is comprised of the following options:

- **Export Unit Parameters:** In Unit Configuration mode, this option enables you to save the configuration of a selected unit to a file. By selecting ***Export Unit Parameters*** from the *File* menu or by clicking the ***Export*** button in the *Unit Control tab*, the *Save As* window is displayed. Enter a file name and select a directory to save the configuration file as a BreezeACCESS configuration file, with the extension .acc.

- **Create Device List File:** This option enables you to create a site file based on a range of IP addresses.

To create a device list file:

1 From the *File* menu, select ***Create Device List File***. The *Create Device List File* window is displayed.

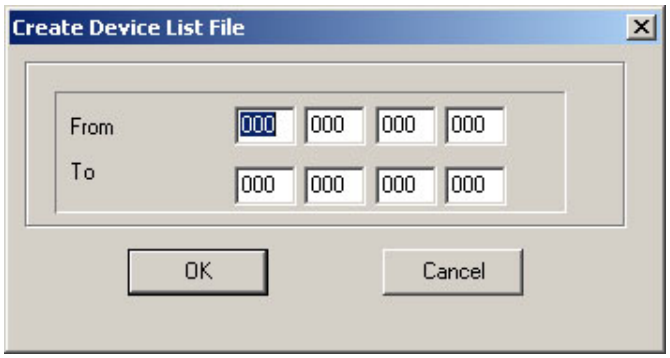


Figure 1-6: Create Device List Window

2 In the ***From*** field, enter the first IP address to be included in the range.

3 In the ***To*** field, enter the last IP address in the range.

NOTE

It is recommended to include in the defined range only IP addresses of existing devices. When the list is loaded, the application searches for each unit included in the list. If non-existent addresses are included, this prolongs the searching process. Therefore, it is recommended that, if necessary, two or several lists be created to limit the number of invalid IP addresses for which the application must search.

4 Click on ***OK***. The **Save As** window is displayed, where you can enter a file name and select a directory to save the site file. The file is saved as an .ste file.

- **Filter Device List:** This option enables you to view selected units in the Device List based on defined criteria. The Device Filter enables you to view only those files selected or to exclude certain files, as follows:

To filter devices:

1 From the *File* menu, select ***Filter Device List***. The *Filter Settings* window is displayed.

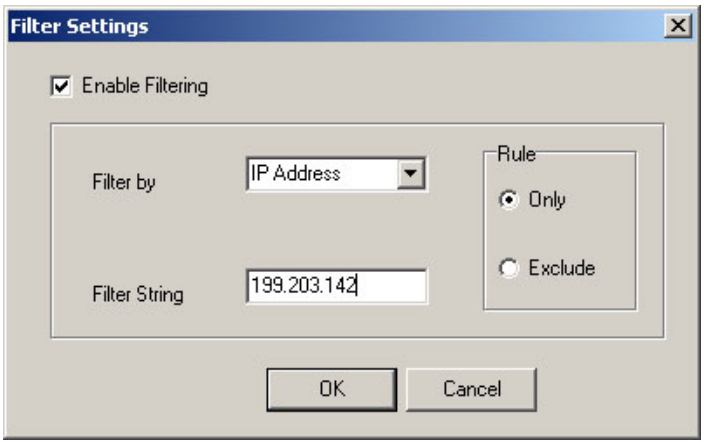


Figure 1-7: Filter Settings Window

2. Mark the ***Enable Filtering*** field to activate the Device List Filter.
3. In the ***Filter by*** field, from the dropdown list, select the criteria by which the Device List will be filtered.
4. In the ***Filter String*** field, enter the criterion by which the Device List is to be filtered. For example, enter a specific location or set of locations. You can enter more than one criterion in the ***Filter String*** field, divided by commas. In addition, you can enter the beginning of a string to exclude or include a set of devices. For example, if you select **IP address** as the ***Filter by*** option and enter the first one or several digits (in the correct format), then all devices beginning with those digits in their IP addresses are included or excluded.

- **Load Devices:** The option enables you to load a list of units that are saved as a site file. The list of devices can be loaded either into the Device List of the main *Configuration Utility* window or to the *File Loading* window. The Select Site window is displayed, enabling you to select the required site file, which is saved with the extension .ste. Once the devices in the file are added to the Device List of the main *Configuration Utility* window, the application attempts to locate each device in turn. After a device is located, its ***Type*** and ***Location*** fields are updated. This process may take several minutes, depending on the number of devices included in the list. If a device is not located, it remains in the list and the ***Type*** and ***Location*** fields are not updated. This automatic location mechanism is not activated when loading a list to the *File Loading* window.

- **Save Devices:** This option enables you to save the units displayed in the Device List as a site file. To support management of units that may be moved, the MAC address of each unit is also included in the file. The Save As window is displayed, enabling you to save the list of devices as a site file, with the .ste extension.

NOTE

Following each autodiscovery cycle, a device list (including MAC addresses) is automatically saved. The default file name is locatedUnits.ste. This automatically saved file is saved in the folder that includes the short cut to the application (typically the Desktop).

- **Exit:** This option closes the BreezeCONFIG utility.

1.4.2 Mode Menu

There are several modes in which you can operate the BreezeCONFIG utility. These modes are selected through the *Mode* menu, which is shown below. The selected option(s) is indicated by a dot or checkmark.

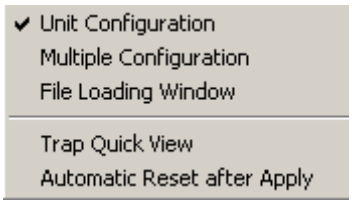


Figure 1-8: Mode Menu

The *Mode* menu is comprised of the following options:

- **Unit Configuration:** This is the default mode, which is used for viewing and/or setting the parameters of a single selected unit. For more information, refer to section 1.5.

- **Multiple Configuration:** This mode is used for preparing and downloading configuration parameters to multiple units simultaneously. For more information, refer to section 1.6.

- **File Loading Window:** Select this mode to launch the File Loading utility, which enables you to upgrade the embedded software in managed units or to load new feature license or country code files. For more information, refer to section 1.7.

- **Trap Quick View:** When set to this mode, the application switches automatically to the *Trap Monitor* tab, if a trap message is received and if the management station is included in the list of trap host stations for the selected device. The trap host stations for a selected device can be defined in the *Network Management – Send Traps* tab. In addition, to view the traps, the trap sending option in the *Network Management – Send Traps* tab for the selected device must be enabled. The Trap Quick View option is only operational in Unit Configuration mode. The default is deselected, which means not active.

- **Automatic Reset after Apply:** When this option is enabled, the selected device is reset each time you click the ***Apply*** button after a configuration modification. During the reset the device's operation is interrupted and it cannot be accessed by BreezeCONFIG. Deselecting this option minimizes the number of times the unit is reset and enables continuous operation of BreezeCONFIG without waiting until the device is active again. The default is deselected, which means not active.

NOTE

New values of some parameters come into effect only after the unit is reset (refer to the System Manual for more details). If the ***Automatic Reset After Apply*** option is deselected, the unit must be reset through the Unit Control window to apply modifications to these parameters.

1.4.3 Tools Menu

The *Tools* menu, which is only present in Unit Configuration mode, provides access to unit definition and location functions that are also available through the toolbar, as shown below.

Figure 1-9: Tools Menu

The *Tools* menu is comprised of the following options:

- **Locate Device:** This option enables you to find an individual unit using its IP address. This includes units located behind a router. For more information, refer to section 1.3.2.

- **Set IP Address:** This option enables you to set the IP address for a unit based on its MAC address. For more information, refer section 1.3.3.

1.4.4 Settings Menu

The *Settings* menu comprises a single option and sub-menu, as shown below:

Figure 1-10: Settings Menu

Select ***Discovery Timeout*** and then select ***10 sec***, ***5 sec*** or ***2 sec*** to define the maximum amount of time, in seconds, for which the system searches for each device when using the Load Devices feature. For more information on using the Load Devices feature, refer to section 1.4.1.

1.4.5 Help Menu

Selecting ***About*** from the *Help* menu enables you to view version and product information regarding the current BreezeCONFIG application. In addition, the *About* window provides a link to the Alvarion technical support website.

1.5 Working in Unit Configuration Mode

The Unit Configuration mode enables you to view the current configuration of a selected device and to modify the values of all relevant device parameters. For a description of each configurable parameter, refer to *Chapter 3, Working with Unit Configurations*.

The Device List on the left side of the main *Configuration Utility* window can be loaded with updated device information using any one of the following mechanisms:

- **Local Network Autodiscovery:** For a description of how to work with this feature, refer to section 1.3.1.
- **Locate Device:** For a description of how to work with this feature, refer to section 1.3.2.
- **Load Devices:** For a description of how to work with this feature, refer to section 1.4.1.

Each time you implement the Local Network Autodiscovery feature, the Device List is reset. Therefore, it is recommended that you start by selecting the Local Network Autodiscovery feature. Then, you can add more devices using the Locate Device and Load Devices features. Alternatively, you can choose not to use the Local Network Autodiscovery feature and create the Device List using the Locate Device and/or Load Devices features.

To select a unit to review or update its configuration, double-click the relevant row in the Device List. When selected, the entry is highlighted in dark blue. Information is then gathered from the device and displayed in the selected tab area. Once all information is loaded, the device is highlighted in blue.

NOTE

Wait until the Device List entry for the selected unit has turned blue before reviewing or modifying any parameters.

1.6 Working in Multiple Configuration Mode

The Multiple Configuration mode enables you to download configuration parameters to multiple units simultaneously, including different unit types, such as Subscriber and Access units.

When this option is selected in the *Mode* menu, all fields of configurable parameters become write-only. Fields that in Unit Configuration mode are read-only are not available in Multiple Configuration mode.

In single Unit Configuration mode, some tabs may include only those parameters that are applicable to the specific device selected. For example, parameters that are specific to Access Units are not displayed if the selected device is a Subscriber Unit.

In Multiple Configuration mode, all tabs except the *Site Survey* and the *Trap Monitor* tabs are available, including those that are only available for specific unit types in Unit Configuration mode. Each configuration tab includes all configurable parameters, including those that are only applicable to specific unit types. The *Site Survey* and *Trap Monitor* tabs are not included, since these tabs include only read-only information for monitoring purposes.

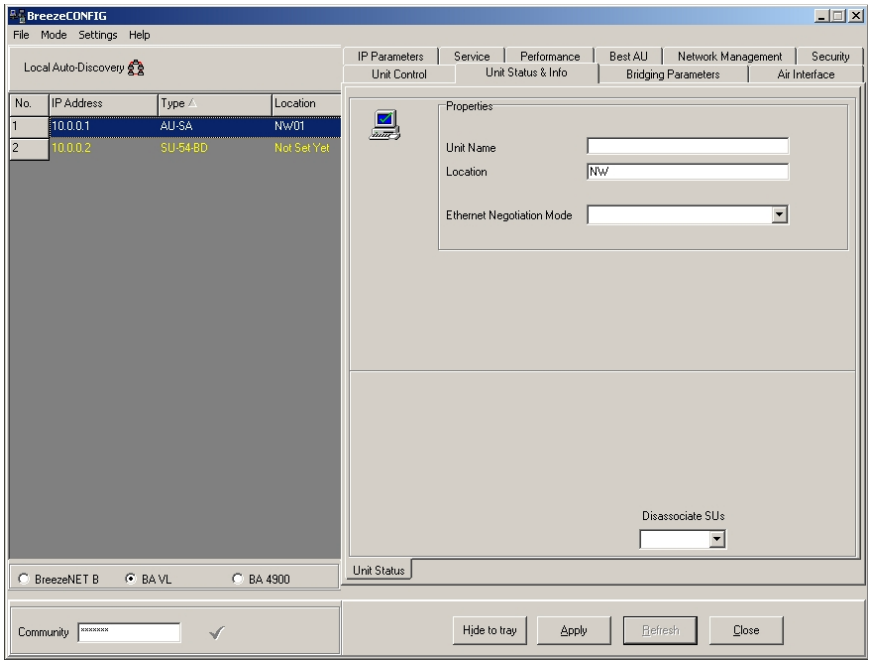


Figure 1-11: Multiple Configuration Mode

NOTE

If a parameter that is not applicable to a certain unit type is configured, the unit will not be configured successfully. For example, if the ***Broadcast/Multicast Relaying*** parameter is configured and uploaded to SU units, which do not support this parameter, then the configuration change for all SU units will fail.

The Device List on the left side of the main *Configuration Utility* window can be populated with updated device information using any of the following mechanisms:

- **Local Network Autodiscovery:** For a description of how to work with this feature, refer to section 1.3.1.
- **Load Devices:** For a description of how to work with this feature, refer to section 1.4.1.

You can use one or both of these features to create a list based on multiple sources. Since the Local Network Autodiscovery feature causes the Device List to be refreshed, first apply the Local Network Autodiscovery and then use the Load Devices feature to add more units to the Device List, as required.

To modify multiple unit configurations:

1. From the Device List of the main *Configuration Utility* window, select the units for which a modified configuration is required. Use the standard Windows ***Shift*** or ***Ctrl*** key commands to select multiple units.
2. Select the product family option at the bottom of the Device List. The Multiple Configuration mode can be used for either BreezeACCESS VL (BA VL), BreezeACCESS 4900 (BA 4900) or BreezeNET B units; it cannot be used simultaneously for two or more product families.
3. In the relevant configuration tabs, modify the required parameters and click Apply. For a description of each configurable parameter, refer to Chapter 3, *Working with Unit Configurations*. The *Multiple Configuration* window is displayed.

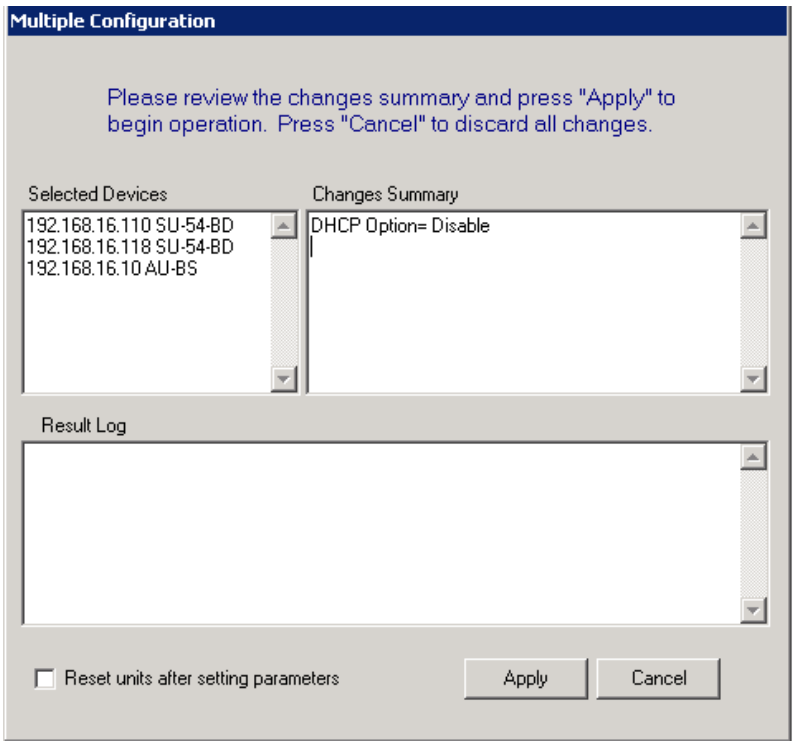
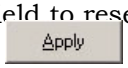


Figure 1-12: Multiple Configuration Window

4 The *Multiple Configuration* window displays the selected units and a list of the modifications made during the current multiple configuration session. Check the ***Reset units after settings parameters*** field to reset all affected units after loading the modified configuration. Click 

to load the modifications to the selected units. A log of the multiple configuration session is displayed during and after the operation.

1.7 Working with the File Loading Utility

The File Loading utility enables you to upgrade the embedded unit software and determine the current active software version for multiple managed units. It also enables you to load new country code files, feature license files, configuration files or operator defaults files. The files can be simultaneously downloaded to multiple units of any type, such as AUs and SUs.

To access the File Loading utility, from the Mode menu, select ***File Loading Window***. The *File Loading Window* is displayed, as shown below.

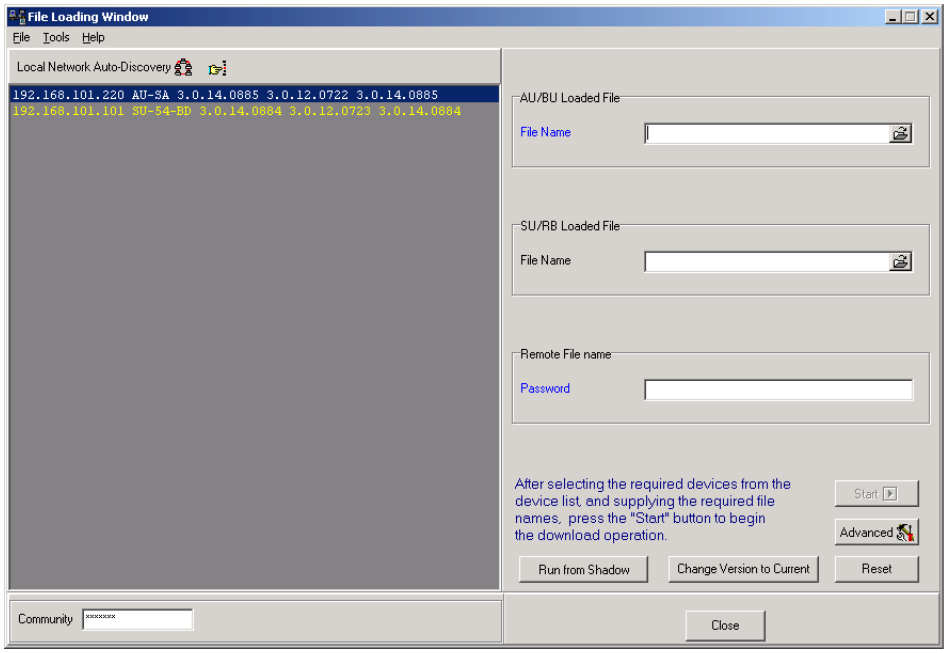


Figure 1-13: File Loading Window

The Device List is displayed in the left side of the window. Each entry includes the device IP address, unit type, current software version, shadow software version and the software version to be used after the next reset.

When the File Loading utility is accessed, the current Device List in the main *Configuration Utility* window is automatically loaded to the Device List of the File Loading utility. The Device List can also be loaded with device information using any combination of the following alternatives:

- **Local Network Autodiscovery:** For a description of how to work with this feature, refer to section 1.3.1.
- **Locate Device:** For a description of how to work with this feature, refer to section 1.3.2.

- **Load Devices:** For a description of how to work with this feature, refer to section 1.4.1.

You can use one or several of these alternatives to create a list based on multiple sources. Note that the Local Network Autodiscovery causes the Device List to be reset. Since there are additional features available in the main Configuration Utility window, such as the Filter Device List feature, it is recommended to prepare the required list of devices in the main *Configuration Utility* window. Then, simply open the File Loading utility and the list is automatically loaded.

1.7.1 File Menu

The File menu in the File Loading Utility includes the following options:

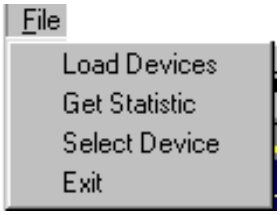


Figure 1-14: File Menu-File Loading Utility

- **Load Devices:** For a description of how to work with this feature, refer to section 1.4.1.

- **Get Statistic:** Displays statistics information on the active and shadow versions in the selected devices, as shown below.

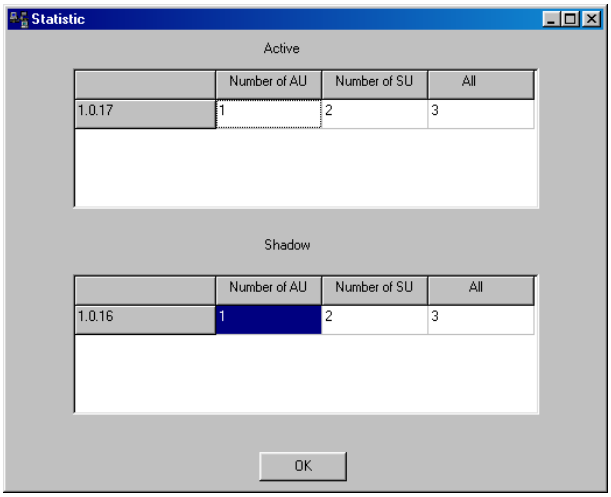


Figure 1-15: Get Statistic Window

- **Select Device:** This option enables version-based filtering of the selected devices, as shown in Figure 1-16. You can select devices according to either the Active or Shadow version. The selection rule can be either to include only

the devices with the specified version (by selecting the **Only** option), or to select all devices excluding those with the specified version (by selecting the **Exclude** option).

Figure 1-16: Select Device Window

To load new files:

1 From the Device List on the left side the window, select the units to which a new file should be loaded. Use the standard Windows ***Shift*** and ***Ctrl*** key commands to select multiple units.

2 Enter the applicable remote filename password for the file to be loaded. The password is <read/write community string>.<file extension>. The default read/write community string is **private**. The extension is:

- For compressed SW files: .bz.
- For country code files: .ccf.
- For Feature License files: .fln
- For Configuration files: .cfg
- For Operator Defaults files: .cmr

3 You can define the path to the required upgrade file in the applicable selection boxes, or click the button on the right side of each of the selection fields to open the *Select filename* window. There are separate selection fields for AU files and SU files. The available fields correspond to the devices selected from the Device List. For example, if the devices selected do not include any AUs, the relevant AU selection field is disabled.

4 Click on Start to initiate the file loading. A log of the upgrade process is displayed during and after the operation.

5 Click on Advanced to modify the settings of the TFTP session used in the upgrade download, as follows:

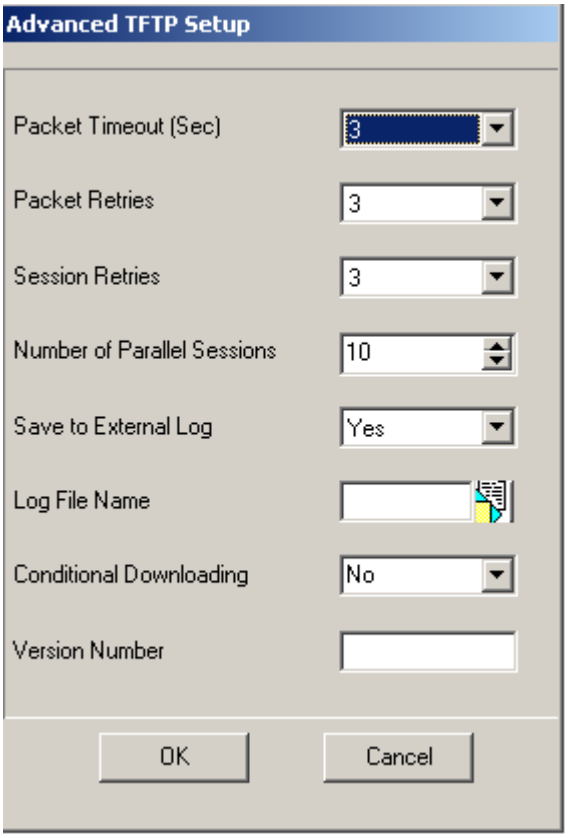


Figure 1-17: Advanced TFTP Setup

- **Packet Timeout**: Defines the time, in seconds, for which the upgrade process waits for an acknowledgement message. The range is 1 to 30 seconds and the default is 3 seconds.

- **Packet Retries**: Defines the maximum number of retries, which is the number of times a packet is retransmitted when an acknowledgement is not received within the defined timeout period. The range is 1 to 5 and the default is 3 retries.

- **Session Retries**: Defines the number of times the TFTP session is restarted before determining that the upgrade procedure has failed. The range is 1 to 5 and the default is 3 retries.

- **Number of Parallel Sessions**: Defines the maximum number of TFTP sessions that can be conducted simultaneously. The range is 1 to 10 and the default is 10. In the event of too many failures in the upgrade process it is advised to reduce the value of this parameter.

- **Save to External Log**: Defines whether the results of the upgrade process are saved to a Log File. The default is Yes.

- **Log File Name**: Enables you to define the name and path to the external Log File. Click the  icon on the right to open a Save As window, which enables you to navigate to the required location and/or file.

- **Conditional Downloading**: If the number in the Version Number field (see below) is identical the number of the Main version in the target device, the downloading of a SW file to this device shall not be performed, regardless of the option selected for Conditional Downloading. If the number in the Version Number field is identical the number of the Shadow version in the target device, the downloading of a SW file to this device shall be performed only if the Conditional Downloading option is set to No. If it is set to Yes, the numbers will be compared prior to starting the download process, and downloading shall be performed only if the number in the Version Number field is different from both the Main and Shadow versions.

- **Version Number**: This is an optional field. Enter the version number of the firmware to be downloaded to enable version numbers comparison for conditional downloading.

To work with the current and shadow software versions:

The active firmware version of multiple units can be managed as follows:

- Click on Run FromShadow to use the Shadow software version in the selected devices. Note that this is only temporary, since the device(s) revert to the Current version after the next reset.

- Click on Change Version to Current to define the currently active version as the new Main version in the selected devices. The previous Main version will become the new Shadow version.

The typical process is to run the Shadow version, and swap the Shadow and Main versions only after verifying that the new version operates properly.

2

Chapter 2 - Unit Configuration

Many configuration parameters provided by BreezeCONFIG depend on the type of device being configured. This means that there are different windows and parameters depending on whether an Access Unit (AU) or a Subscriber Unit (SU) is selected. Each parameter is described according to the applicable unit type, unless the parameter is applicable to all unit types. For detailed information on each of the parameters refer to the relevant System Manual.

In This Chapter:

2.1 Unit Control Parameters

The *Unit Control* tab enables you to reset the unit and manage the software versions in the selected unit(s), as shown below.

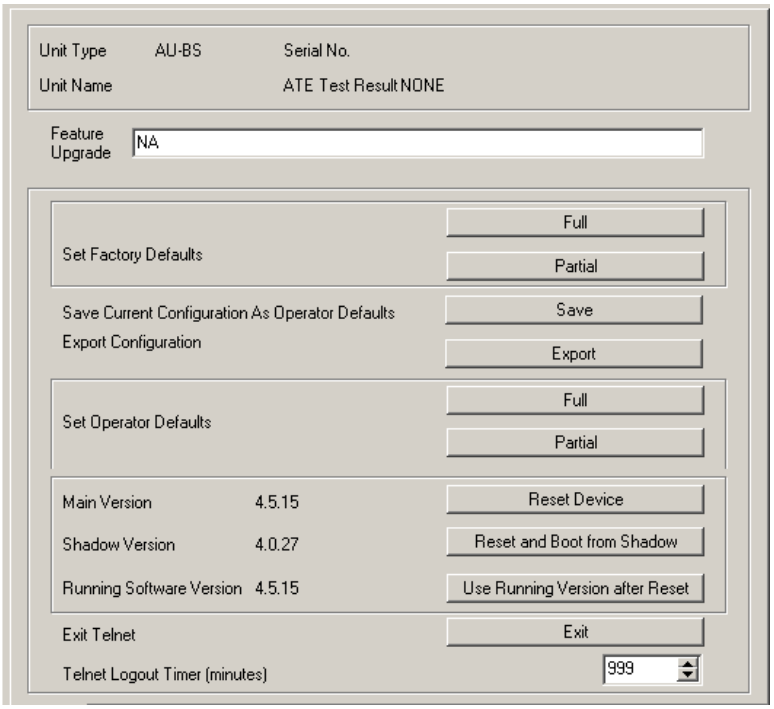


Figure 2-1: Unit Control Parameters (AU)

The *Unit Control* tab is comprised of the following components:

- **Unit Type:** Displays the unit's functionality.
- **Unit Name:** Displays the name of the selected device, which can be modified in the *Unit Status & Info* tab.
- **ATE Test Result:** Indicates the result of the unit's final testing in production. In units supplied with SW version 4.5 and higher should always be PASS. In units upgraded from a version below 4.5 this parameter will be NONE.
- **Serial NO.:** The Serial Number of the unit. Applicable only to units supplied with SW version 4.5 and higher. In units upgraded from a version below 4.5 this parameter will be none (empty).
- **Feature Upgrade:** A write-only text box enabling to enter a feature upgrade license string. A feature license string to be provided by Alvarion comprises between 32 to 64 hexadecimal digits and is MAC address dependent.

- **Set Factory Defaults:** Reverts the system parameters to the original factory defaults, as follows.

  - Click Full to revert most parameters to the selected set of factory default values (refer to the System Manual for details on the parameters that are not changed).

NOTE

You may lose connectivity to the unit.

  - Click Partial to revert all parameters to the factory default values except for those parameters that are necessary to ensure connectivity and management access (refer to the System Manual for details on the parameters that are not changed).

- **Set Operator Defaults:** Reverts the system parameters to the configuration defined as the Operator's defaults. The Operator can define a configuration file as the Operator's default, as described in ***Save Current Configuration as Operator Defaults*** below.

  - Click Full to revert most parameters to the selected set of Operator default values (refer to the System Manual for details on the parameters that are not changed).

NOTE

You may lose connectivity to the unit.

  - Click Partial to revert all parameters to the Operator default values except for the parameters necessary to ensure connectivity and management access (refer to the System Manual for details on the parameters that are not changed).

- **Save Current Configuration as Operator Defaults:** Enables you to save the current configuration as a configuration file to be used as the Operator defaults. To activate the Operator defaults refer to ***Set Operator Defaults*** above.

- **Export Configuration:** Click **Export** to save the unit's configuration as a BreezeACCESS configuration file, with the extension .acc. The *Save As*

window is displayed, enabling you to select a location for the file and to define a file name.

- **Main Version:** Shows the version defined as the Main Version. This is the version that will be used after the next reset.
  Click **Reset Device** to reset the selected unit and apply any modifications made to the system parameters.

- **Shadow Version:** Shows the version defined as the Shadow Version. Click **Reset and Boot from Shadow Version** to activate the shadow software version. The unit is reset and the shadow version becomes active.

- **Running Software Version:** Shows the currently active version. Click **Use Current Version After Reset** to define the currently active version as the version to be defined as the Main Version and used after the next reset.

NOTE

To replace the Main version with the Shadow version, you must first click **Reset and Boot from Shadow Version** and then click **Use Current Version After Reset**.

- **Exit Telnet:** Click **Exit** to log off from the current Telnet session.

- **Telnet Logout Timer:** Click the up and down arrows or enter a number to define the number of minutes that the Monitor program can remain inactive before the unit automatically exits from the program. The time-out value can range from 1 to 999 minutes.

2.2 Unit Status and Info Parameters

The Unit Status and Info tab is comprised of the following secondary tabs:

- Unit Status (AU and SU)
- SUs Info (AU)
- SUs Capabilities (AU) or AUs capabilities (SU)
- MAC Pinpoint (AU)
- Gateways (AU)

2.2.1 Unit Status Tab

The Unit status tab enables you to define the name and location of the selected unit and to view details regarding the unit's firmware and hardware versions. For an SU, information regarding its associated AU is displayed, and for an AU information regarding its associated SUs is displayed.

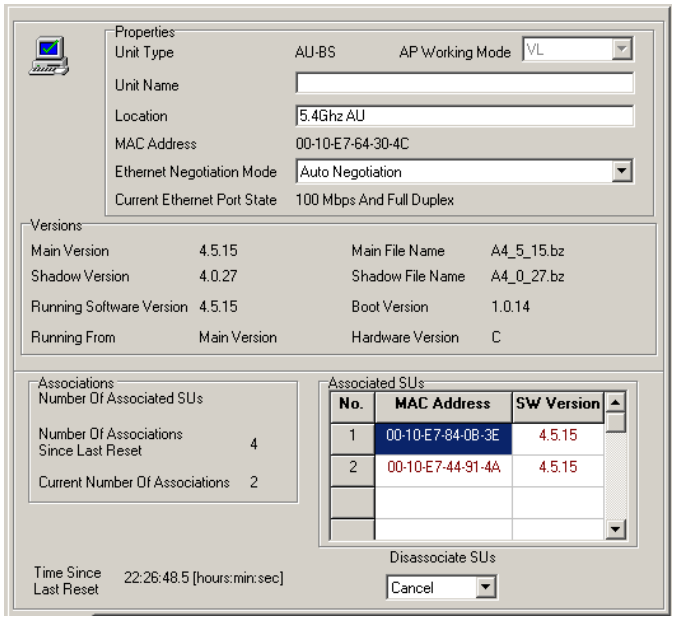


Figure 2-2: Unit Status Tab – Access Unit

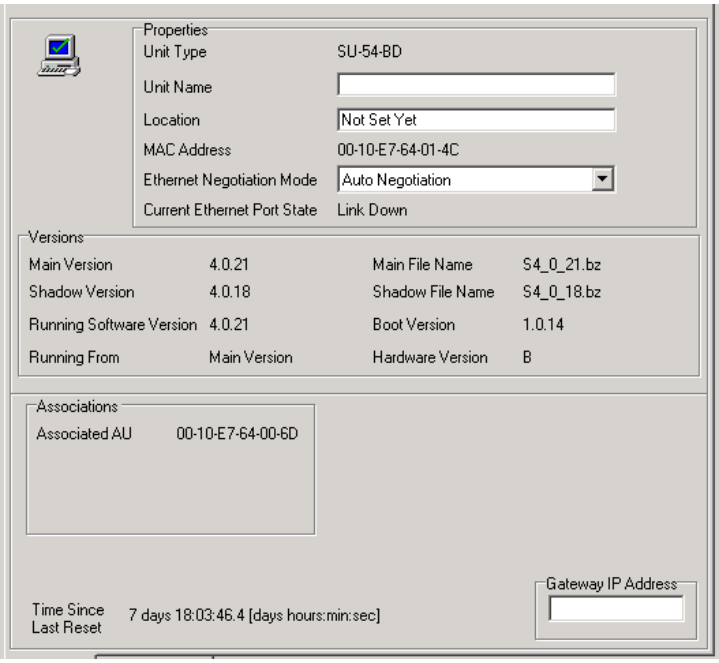


Figure 2-3: Unit Status Tab – Subscriber Unit

The *Unit Status* tab is comprised of the following components:

2.2.1.1 Properties

- **Unit Type:** Identifies the unit's functionality.
- **AP Working Mode (AU only):** Not applicable for current version.
- **Unit Name:** Enter a name for the selected unit.
- **Location:** A descriptive geographical or site location for the selected unit. A string of up to 35 printable characters.
- **MAC Address:** Displays the unit's MAC address.
- **Ethernet Negotiation Mode:** Enter the Ethernet port negotiation mode. The available options are:
  - Auto Negotiation
  - Force 10 Mbps and Half-Duplex
  - Force 10 Mbps and Full-Duplex
  - Force 100 Mbps and Half-Duplex
  - Force 100 Mbps and Full-Duplex

- **Current Ethernet Port State:** Displays the actual state of the Ethernet port.

2.2.1.2 Versions and Flash Memory

- **Main Version:** Displays the version number of the unit's current main software version (the version to be used after next reset).
- **Shadow Version**: Displays the version number of the unit's backup software.
- **Running Software Version:** Displays the version number of the current running software version.
- **Running From:** Displays the source (Main or Shadow) of the current running version.
- **Main File Name:** Displays the name of the compressed file containing the Main Version.
- **Shadow File Name:** Displays the name of the compressed file containing the Shadow Version.
- **Boot Version:** Displays the version number of the Boot software.
- **Hardware Version:** Displays the model identification of the unit hardware.

2.2.1.3 Associations

- **Current Number of Associations (AU only):** Displays the number of Subscriber Units that are currently associated with the Access Unit.
- **Number of Associations Since Last Reset (AU only):** Displays the number of Subscriber Units that were associated with the Access Unit since the last reset, including re-associations.
- **Associated AU (SU only):** Displays the MAC address of the Access Unit with which the Subscriber Unit is currently associated.

2.2.1.4 Associated SUs (AU Only)

A table listing the MAC addresses and running software versions of all Subscriber Units currently associated with the selected Access Unit.

2.2.1.5 Disassociate SUs (AU only)

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

The Disassociate drop-down menu includes three options:

- **Cancel**
- **All SUs**: select this option and click Apply to disassociate all SUs served by the AU.
- **Selected SU**: Select an entry (MAC Address) in the Associated SUs table, select the Selected SU option and click Apply to disassociate the selected SU.

2.2.1.6 Time Since Last Reset

The time elapsed since the last reset of the unit.

2.2.1.7 Gateway IP Address (SU Only)

This feature is included to support management of a DRAP enabled Gateway connected to the SU using a web browser. Enter the IP address of the Gateway and double-click on the address to open a web browser and connect to the specified address.

2.2.2 SUs Info Tab (AU only)

Applicable to Access Units only, the *SUs Info* secondary tab of the *Unit Status & Info* tab provides association and additional information regarding the SUs associated with the selected AU.

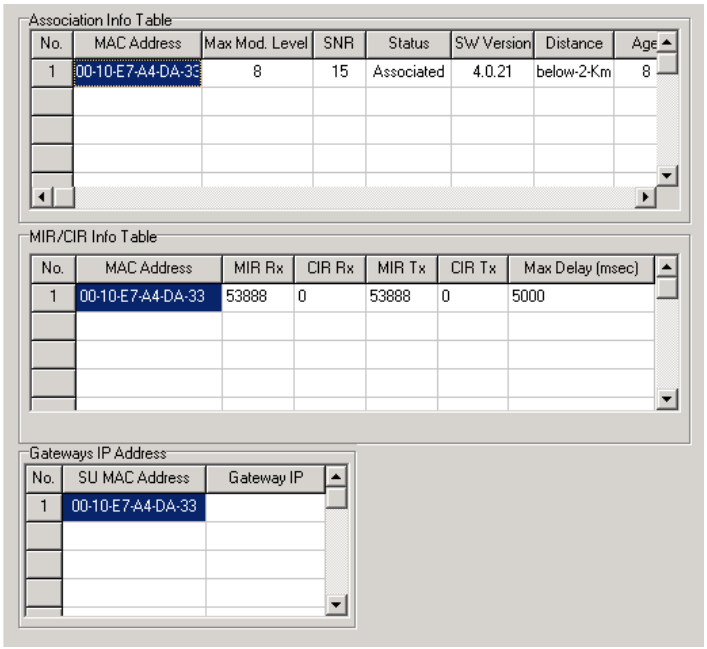


Figure 2-4: Unit Status & Info, SUs Info Tab

The *SUs Info* tab is comprised of the following components:

2.2.2.1 Association Info Table

A table that provides the following information for each SU in the associated SUs database:

- **MAC Address:** The MAC address of the associated Subscriber Unit.
- **Max Mod. Level:** The value configured for the ***Maximum Modulation Level*** parameter (see section 2.8) of the SU.
- **SNR:** The quality (Signal to Noise Ratio) in dB at which the AU receives the SU.
- **Status:** The current association status of the relevant SU. The value can be Associated, Authenticated or Not Authenticated.
- **SW Version:** The version of the software that is currently in use by the SU.

- **Distance:** The distance of the unit from the AU as measured by the automatic cell distance mechanism.
- **Age:** The time in seconds since receiving the last packet from the SU.
- **SU Name:** The Unit Name of the SU.

2.2.2.2 MIR/CIR Info Table

A table that provides the following information for each SU in the associated SUs database:

- **MAC Address:** The MAC address of the associated Subscriber Unit.
- **MIR Rx:** The value configured for the MIR: SU to AU parameter of the SU.
- **CIR Rx:** The value configured for the CIR: SU to AU parameter of the SU.
- **MIR Tx:** The value configured for the MIR: AU to SU parameter of the SU.
- **CIR Tx:** The value configured for the CIR: AU to SU parameter of the SU.
- **Max Delay (msec):** The value configured for the Maximum Delay parameter of the SU.

2.2.3 SUs Capabilities Tab (in AU) and AUs Capabilities Tab (in SU)

The SUs/AUs Capabilities tabs provide information on HW and SW capabilities of relevant units. For an AU, the information provided in the tab is for all associated SUs. For an SU, the tab includes information on all AUs in the neighboring AUs table (all AUs with whom the SU can communicate).

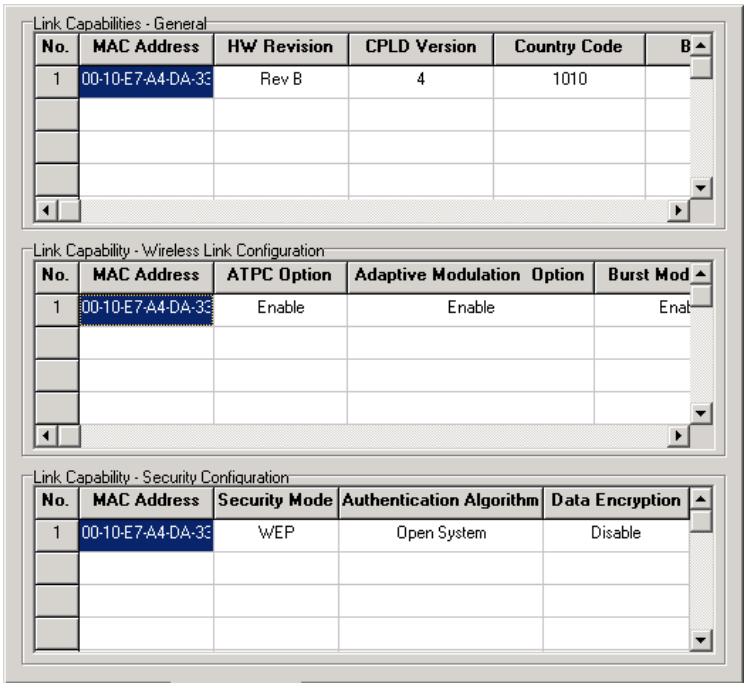


Figure 2-5: SUs Capabilities Tab (AU)

The SUs/AUs Capabilities tabs include the following components:

2.2.3.1 Link Capabilities-General

The Link Capabilities – General table provides information on general parameters of relevant units. For each relevant unit, identified by its MAC address, the following details are displayed:

- **HW Revision**: the hardware revision of the unit.
- **CPLD Version** (AU only): The version of the Complex Programmable Logic Device (CPLD) used in the SU.
- **Country Code**: The 3 or 4 digits country code supported by the unit.
- **SW Version** (SU only): The SW version used by the AU.
- **Boot Version** (AU only): The Boot Version of the SU.

2.2.3.2 Link Capability-Wireless Link Configuration

The Link Capability-Wireless Link Configuration table provides information on current wireless link parameters of relevant units. For each relevant unit, identified by its MAC address, the following details are displayed:

- **ATPC Option**: The status of the ATPC Option. Enable or Disable.
- **Adaptive Mod. Option**: The status of the Adaptive Modulation Option. Enable or Disable.
- **Burst Mode Option**: The status of the Burst Mode Option. Enable or Disable.
- **DFS Option** (SU only): The status of the DFS Option in the AU.
- **Concatenation Option**: The status of the Concatenation Option. Enable or Disable.
- **Learn Country Code by SU** (SU only): The status of the Country Code Learning By SU option in the AU. Enable or Disable.

2.2.3.3 Link Capability-Security Configuration

The Link Capability-Security Configuration table provides information on current security related parameters of relevant units. For each relevant unit, identified by its MAC address, the following details are displayed:

- **Security Mode**: WEP, or AES OCB or FIPS-197 (if supported).
- **Authentication Algorithm**: Shared Key or Open System.
- **Data Encryption**: Enable or Disable.

2.2.4 MAC Pinpoint Tab (AU)

The MAC Pinpoint feature enables to identify the BreezeACCESS unit through which a specified Ethernet station is connected to the wireless medium.

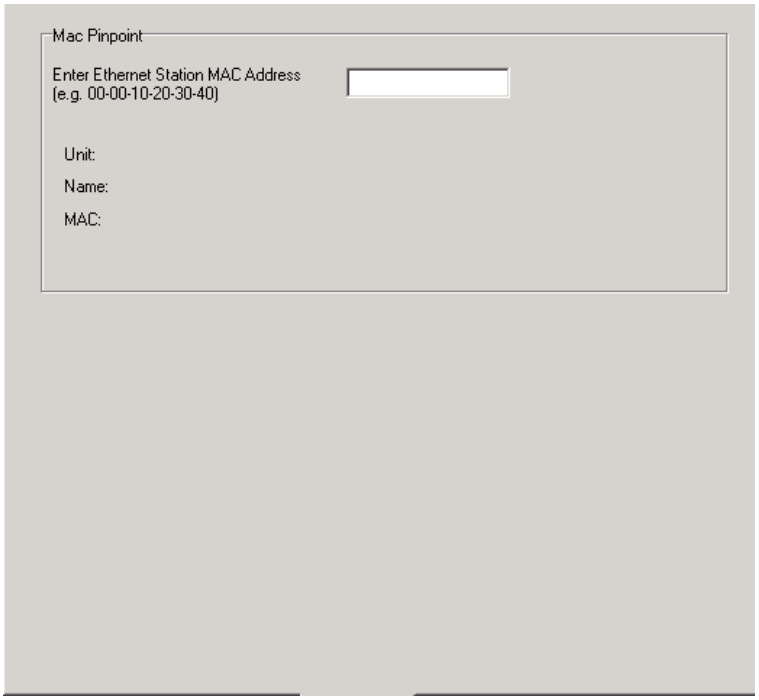


Figure 2-6: MAC Pinpoint Tab

To identify the unit to which a station is connected:

In the text field, enter the MAC address of the station using the format xx-xx-xx-xx-xx-xx.

After clicking Apply, the identification details (Unit Type, Unit Name and MAC Address) of the BreezeACCESS unit through which the station is connected to the wireless medium will be displayed.

2.2.5 Gateways (AU)

When the DRAP option is supported, the Gateways tab provides details on the active DRAP-enabled Gateways connected to any of the SUs served by the AU.

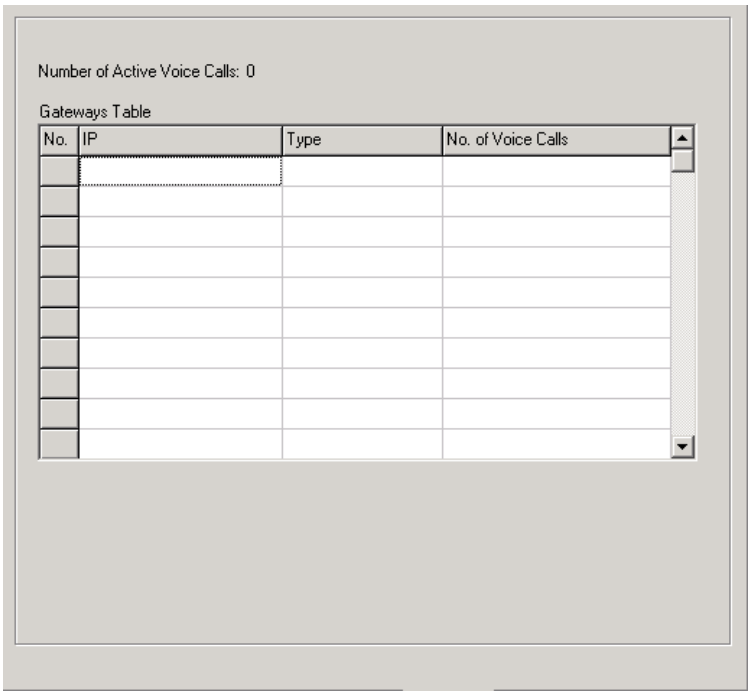


Figure 2-7: Gateways Tab

- **Number of Active Voice Calls**: The total current number of Voice Calls in the sector.
- **Gateways Table**: For each Gateway unit the following information is displayed:
  - **IP**: The IP address of the unit.
  - **Type:** The unit type: VG-1D1V, VG-1D2V, or NG-4D1W.
  - **No. of Voice calls:** The number of active voice calls for the selected gateway (applicable only to Voice Gateways).

2.3 IP Parameters

The *IP Parameters* tab enables you to define IP parameters for the selected unit and determine its method of IP parameter acquisition.

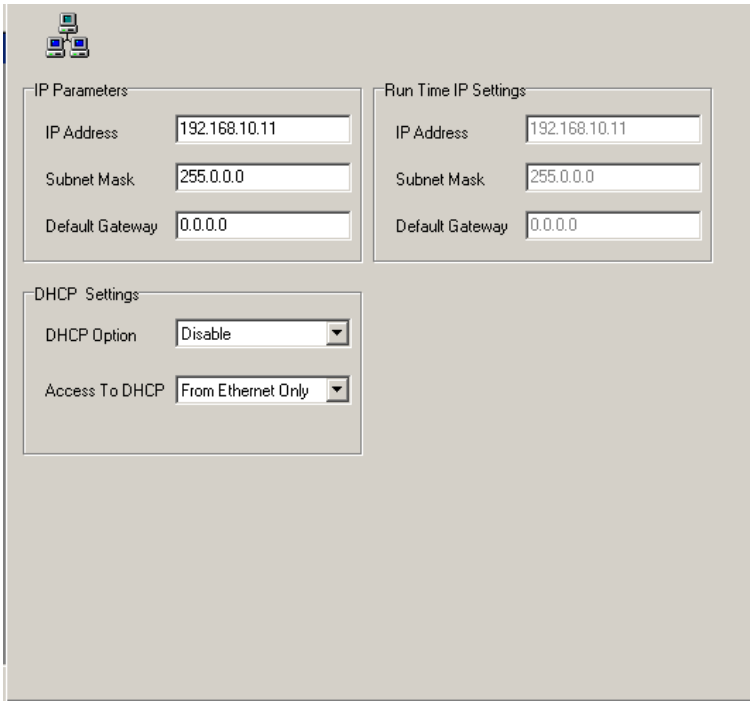


Figure 2-8: IP Parameters Tab

The *IP Parameters* tab is comprised of the following components:

2.3.1 IP Parameters

- **IP Address:** Enter a static IP address for the selected unit.
- **Subnet Mask:** Enter a static subnet mask for the selected unit.
- **Default Gateway:** Enter an address for the unit's default gateway.

2.3.2 DHCP Settings

- **DHCP Option:** From the dropdown list, select an operational mode for the DHCP mechanism, from the following options:
  - ◇ Select **Disable** to configure the IP parameters manually. The unit then operates using the defined static IP parameters.

- Select **DHCP Only** to enable the unit to search for and acquire its IP parameters, including the IP address, subnet mask and default gateway, from a DHCP server. If this option is selected, configuring the static IP parameters is not required.

- Select **Automatic** to enable the unit to search for a DHCP server and acquire its IP parameters from the server. If a DHCP server is not located within approximately 40 seconds, the current static parameters are used.

- **Access to DHCP:** From the dropdown list, select the port through which the unit searches for and communicates with a DHCP server, from the following options:

  - From Wireless Only

  - From Ethernet Only

  - From Both

2.3.3 Run Time IP Settings

- **IP Address:** Displays the unit's current IP address.

- **Subnet Mask:** Displays the unit's current subnet mask.

- **Default Gateway:** Displays the unit's current default gateway.

2.4 Air Interface Parameters

The *Air Interface* tab enables you to define parameters relating to the communication between Access Units and Subscriber Units. Many parameters vary between unit types. The applicable unit type is clearly identified throughout the parameter explanations, as required.

The Air Interface tab is comprised of the following secondary tabs:

- General
- Frequency
- Power Tables
- Country Parameters
- Spectrum Analysis
- DFS (AU, only if DFS is supported by the Country Code)

2.4.1 Air Interface General Tab

The *General* tab of the *Air Interface* tab enables you to define ESSID, ATPC and other parameters.

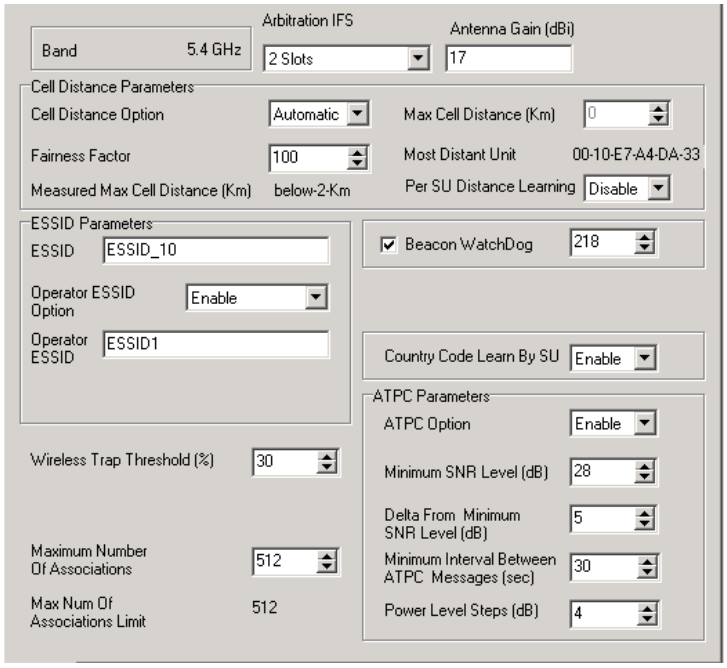


Figure 2-9: Air Interface General Tab – Access Unit

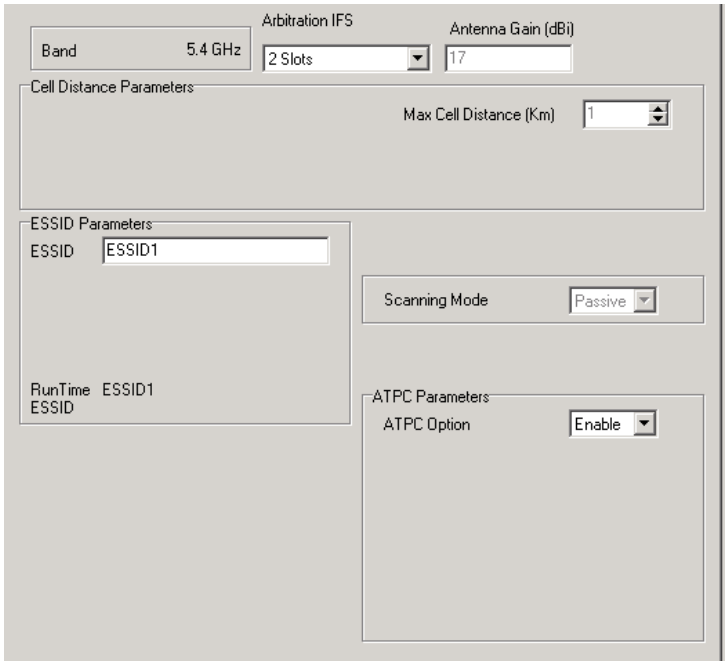


Figure 2-10: Air Interface General Tab – Subscriber Unit

The *General* tab is comprised of the following components:

- **Band:** A read-only field that displays the frequency band of the selected unit.
- **Arbitration IFS:** The Arbitration Inter-Frame Spacing. Defines the typical minimum time (DIFS) between consecutive transmissions. The available options are:
  - ◇ 1 Slot
  - ◇ 2 Slots

  A value of 1 should be used only in point-to-point applications to define the unit that should have advantage over the other one.

NOTE

The AIFS parameter is not applicable when the Wireless Link Prioritization Option is enabled.

- **Antenna Gain:** The net gain of the antenna, including attenuation of the RF cable, to be used for calculating the maximum permitted transmit power where there are limitations set by local regulations. In certain units with an integral antenna the value is pre-configured at the factory and cannot be changed. A value of Not Set Yet indicates that the actual value must be entered (as long as the value remains Not Set Yet the unit will not transmit). A value of Don't Care means that there are no transmit power limitations.

  The configurable range is 0 to 50.

- **Maximum Number of Associations (AU only):** The maximum number of Subscriber Units that can associate with the selected Access Unit. The available values range from 0 to 512.

- **Maximum Num of Associations Limit (AU only):** The Maximum Number of Associations parameter defines the maximum number of Subscriber Units that can be associated with the selected AU, while still guaranteeing the required quality of service to customers.

  Available values for AU-BS and AU-SA range from 0 to 512. For AUS-BS and AUS-SA the range is from 0 to 8. For AUS-BS and AUS-SA that were upgraded to support up to 25 SUs, the range is from 0 to 25. When data encryption is enabled, the maximum number of SUs that can be served by AU-BS or AU-SA is 124.

NOTE

The Maximum Number of Associations parameter in AU-BS or AU-SA may be configured to a value that is higher than the actual limit (124) when data encryption is enabled.

- **Wireless Trap Threshold (AU only):** The threshold for sending the AU Wireless Quality Trap, which indicates that the quality of the wireless link has dropped below (off), or has increased above (on), the specified threshold. The ***Wireless Trap Threshold*** is in percentage of retransmissions compared to total transmissions. The range is from 1% to 100%.

- **Scanning Mode (SU only):** Defines whether the SU will use Passive or Active scanning when searching for an AU. When DFS Option is enabled, Scanning Mode is forced to Passive.

- **Country Code Learning by SU (AU only)**: Defines whether the SU should learn the country code advertised by the AU, and use the parameters of the advertised country code if it differs from the one configured in the SU.

- **Beacon Watchdog (AU only)**: When it is not able to send beacon frames for a predetermined number of beacons, such as in the case of interferences, an AU resets itself. The Beacons Watchdog parameter represents the number of consecutive lost beacons, after which the unit will reset itself.

  The range is from 100 to 1000 (lost beacons). When the parameter is set to 0, or when the check box next to it is not marked, this feature is disabled, i.e AU internal refresh will never be performed.

2.4.1.1 Cell Distance Parameters

- **Cell Distance Option (AU only):** Defines whether the maximum distance of the AU from any of the SUs it serves will be determined manually (using the Maximum Cell Distance parameter) or automatically.

- **Max Cell Distance:** The distance from the AU of the farthest SU served by it. Configurable only in AU, and only if the Cell Distance Option is set to Manual; otherwise it is read-only. The Max Cell Distance affects the maximum time that the AU and all units served by it unit will wait for a response message (including Acknowledgements of unicasts and response messages during the authentication and association process). This parameter also affects the size of time slots, to ensure fairness in the contention back-off algorithm between SUs located at different distances from the AU.

  The available values are 1 to 54 (kilometers) or 0 for no compensation (minimum slot size, maximum time-out when expecting a response message)

- **Per SU Distance learning (AU only):** Defines the mode in which SUs calculate the Acknowledge (ACK) timeout: based on the maximum cell distance or on the actual distance from the AU. When this feature is disabled, all SUs in the cell use the maximum cell distance for the calculation of the ACK timeout; when enabled, each SU uses instead its actual distance from the AU.

NOTE

The Per SU Distance Learning feature is supported only when the **Cell Distance Option** is set to Automatic.

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

  The range is 0 to 100 (%).

- **Most Distant Unit (AU only):** The MAC Address of the unit which the Automatic Cell Distance algorithm identified as being the farthest from the AU.

- **Measured Max Cell Distance (AU only):** The distance of the farthest SU served by the AU, as measured by the Automatic Cell Distance mechanism.

2.4.1.2 ESSID Parameters

- **ESSID:** The Extended Service Set ID for the selected unit. The ESSID identifies the wireless network, which prevents the unintentional merging of two collocated wireless networks, since an SU can only associate with an AU that has the identical ESSID. The ESSID can be a string of up to 31 case-sensitive printable ASCII characters.

- **Operator ESSID Option (AU only):** From the dropdown list, select whether to **Enable** or **Disable** the Operator ESSID Option. The Operator ESSID is a secondary ESSID to be used when adding additional Subscriber Units to existing deployments, where the primary ESSID may differ among neighboring AUs. It is also used to support the Best AU feature.

- **Operator ESSID (AU only):** The secondary Extended Service Set ID for the selected Access Unit. The ESSID can be a string of up to 31 case-sensitive printable ASCII characters.

- **RunTime ESSID (SU only):** A read-only field that displays the ESSID currently used by the selected SUnit to associate with an AU.

2.4.1.3 ATPC Parameters

- **ATPC Option:** From the dropdown list, select whether to **Enable** or **Disable** the Automatic Transmit Power Control algorithm.

- **Minimum SNR Level (AU only):** The minimum desired level in dB of the average SNR at the AU for each SU. This value reflects the lower limit of the optimal reception level range. Available values range from 4 to 60 dB.

- **Delta From Minimum SNR Level (AU only):** The ***Minimum SNR Level*** plus the value of this parameter define the maximum desired level of the average SNR at the AU. This value reflects the upper limit of the optimal reception level range. Available values range from 4 to 20 dB.

- **Level Steps (AU only):** The step size in dB that the SU will use when receiving an ATPC Power-Up/Power-Down message. The available values range from 1 to 20 dB.

- **Minimum Interval Between ATPC Messages (AU only):** The minimum permitted time, in seconds, between consecutive power-up/power-down messages. Available values range from 1 to 3600 seconds.

2.4.2 Air Interface Frequency Tab

The Frequency tab enables you to configure frequency parameters for the unit.

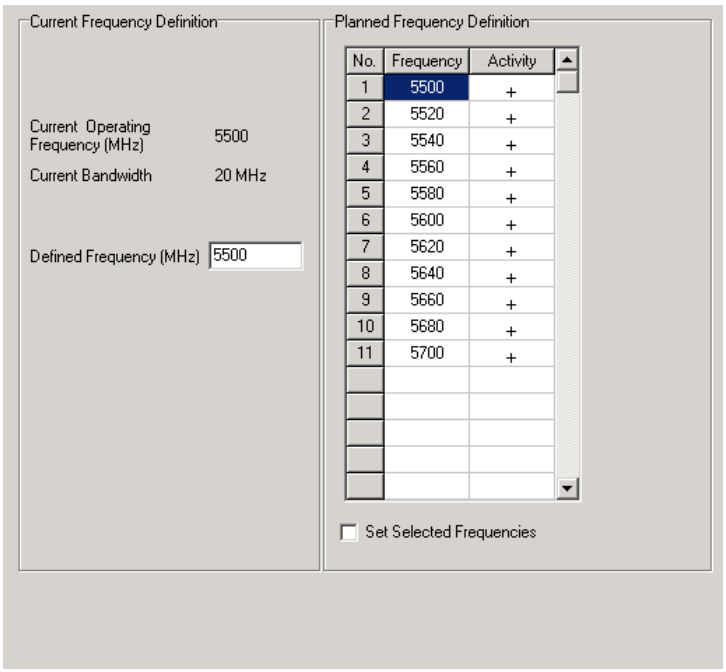


Figure 2-11: Air Interface Frequency Tab – Access Unit

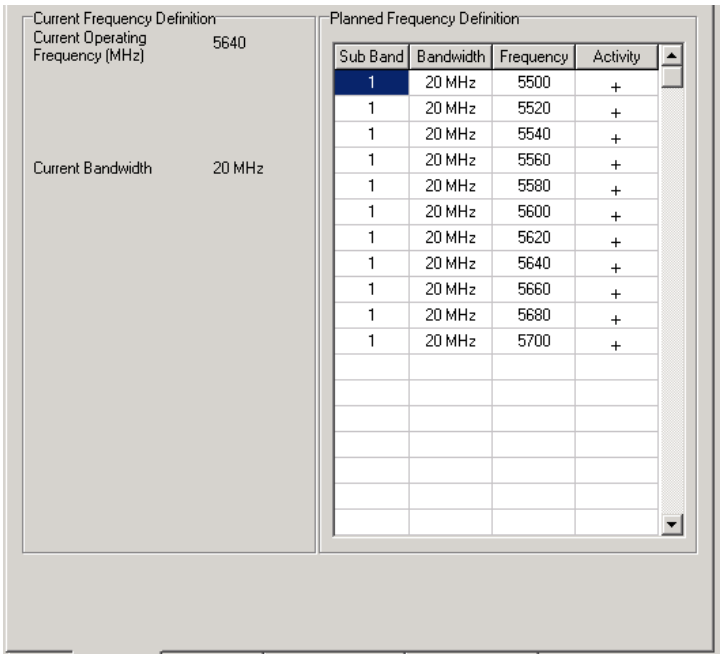


Figure 2-12: Air Interface Frequency Tab – Subscriber Unit

The *Frequency* tab is comprised of the following components:

2.4.2.1 Current Frequency Definition

- **Current Operating Frequency:** A read-only field that displays the current operating frequency in MHz.
- **Current Bandwidth:** A read-only field that displays the current bandwidth in MHz.
- **Defined Frequency (AU only):** The fixed operating frequency in MHz to be used if the DFS option is disabled. This is also the first frequency to be used by the DFS mechanism the first time it starts functioning. The available values depend on the selected Sub-Band.

2.4.2.2 Planned Frequency Definition

In AU: The **Planned Frequency Definition** table enables defining the frequencies that will be used in the DFS mechanism (if applicable). The available frequencies according to the Sub-Band selected in the Country Code tab (if more than one Sub Band is available) are displayed. Clicking the **Activity** field of the desired frequency entry opens the selection/de-selection drop-down menu. A '+' indicates a selected frequency, while a '-' denominates an unselected one. Check the **Set Selected Frequencies** checkbox to use the selected frequencies as the subset to become effective after the next reset.

In SU: The **Planned Frequency Definition** table enables defining for each of the available Sub-Bands the frequencies that will be used by the SU when scanning for an AU. For each available Sub-Band, the available frequencies are displayed. Clicking the **Activity** field of the desired frequency entry opens the selection/de-selection drop-down menu. A '+' indicates a selected frequency, while a '-' denominates an unselected one. A change in frequencies takes effect without the need to reset the unit.

2.4.3 Air Interface Power Tables Tab

The Power Tables tab enables you to configure transmit power parameters.

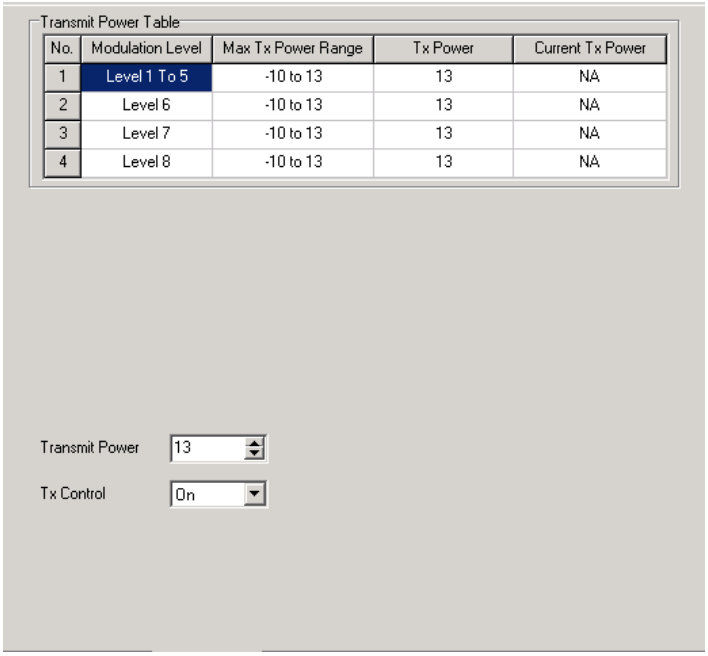


Figure 2-13: Air Interface Power Tables Tab – Access Unit

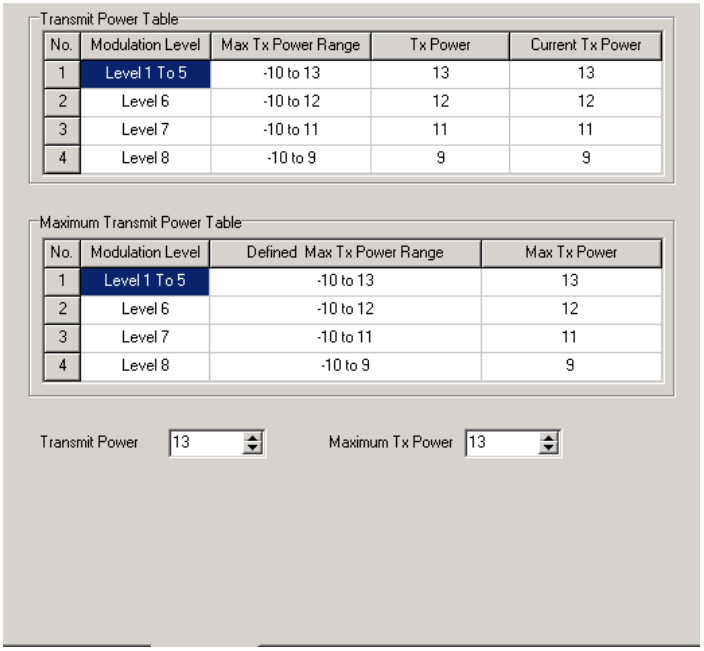


Figure 2-14: Air Interface Power Tables Tab – Subscriber Unit

2.4.3.1 Transmit Power Table

The Transmit Power Table includes the following read-only components for each of the applicable modulation levels:

- **Max Tx Power Range:** The range available for the applicable **Tx Power** parameter.

  In AU, the range is defined by the hardware of the unit. In some cases the upper boundary may be limited by the Maximum Tx Power as defined in the Sub-Band, and/or by the Max EIRP as defined in the Sub-Band together with the Antenna Gain parameter.

  In SU the maximum value is determined by the value of the applicable **Max Tx Power** entry in the **Maximum Transmit Power Table**.

- **Tx Power:** The functionality differs between AU and SU:

  In AU: The transmit power in dBm defined for the applicable modulation level.
  In SU: If ATPC is disabled, this is the transmit power in dBm defined for the applicable modulation level. If ATPC is enabled, it serves as the initial transmit power in dBm for the ATPC algorithm.

  The value of Tx Power for Modulation Level 1 to 5 is set by the **Transmit Power** parameter (below the table). For other modulation levels, the Tx Power is set to the minimum between the value of the **Transmit Power** parameter and the maximum Tx power allowed by the HW and the Country Code for the specific modulation level.

- **Current Tx Power (Applicable in SU only, NA in AU):** The actual transmit power in dBm for the applicable modulation level.

2.4.3.2 Maximum Transmit Power Table (SU only)

The Maximum Transmit Power Table includes the following read-only components for each of the applicable modulation levels:

- **Defined Max Tx Power Range:** The range available for the applicable **Max Tx Power** parameter. The range is defined by the hardware of the unit. In some cases the upper limit may be limited by the Maximum Tx Power as defined in the Sub-Band, and/or by the Max EIRP as defined in the Sub-Band together with the Antenna Gain parameter.

- **Max Tx Power:** The maximum level of the Tx Power. The value for Modulation Level 1 to 5 is set by **Maximum Tx Power** parameter (below the table). For other modulation levels, the Max Tx Power is set to the minimum between the

value of the **Maximum Tx Power** parameter and the maximum Tx power allowed by the HW and the Country Code for the specific modulation level. This parameter also sets the upper boundary for the applicable **Max Tx Power Range** entry in the **Transmit Power Table**. It also sets the maximum level for the ATPC algorithm. The value of **Max Tx Power** cannot be higher than the current value of the applicable **Tx Power** entry in the **Transmit Power Table**.

2.4.3.3 Transmit Power

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

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

The minimum value for the Transmit Power Parameter is –10 dBm (the ATPC may reduce the actual transmit power of the SU to lower values). The maximum value of the Transmit Power Parameter depends on several unit properties and parameters: The HW revision of the unit, the Maximum Allowed Tx Power as defined for the applicable Sub-Band, and the Maximum EIRP as defined for the applicable Sub-Band, together with the value of the Antenna Gain. In the SU, it cannot be higher than the Maximum Tx Power parameter.

For each modulation level, the unit will use as Tx Power (see Transmit Power table) the minimum between this parameter and the maximum Tx power allowed by the HW and the Country Code for the specific modulation level.

2.4.3.4 Maximum Tx Power (SU only)

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

The minimum value for the Maximum Tx Power is -10 dBm. The maximum value depends on several unit properties and parameters: The HW revision of the unit, the Maximum Allowed Tx Power as defined for the applicable Sub-Band, and the Maximum EIRP as defined for the applicable Sub-Band, together with the value of the Antenna Gain.

For each modulation level, the unit will use as Max Tx Power (see Maximum Transmit Power table) the minimum between this parameter and the maximum Tx power allowed by the HW and the Country Code for the specific modulation level.

2.4.3.5 Tx Control (AU only)

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

If the selected option is Ethernet Status Control, then:

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

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

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

2.4.4 Air Interface Country Parameters Tab

The Country Parameters tab displays the country dependent parameters of the available Sub-Band(s). Where more than one Sub-Band is available, it enables Sub-Band selection.

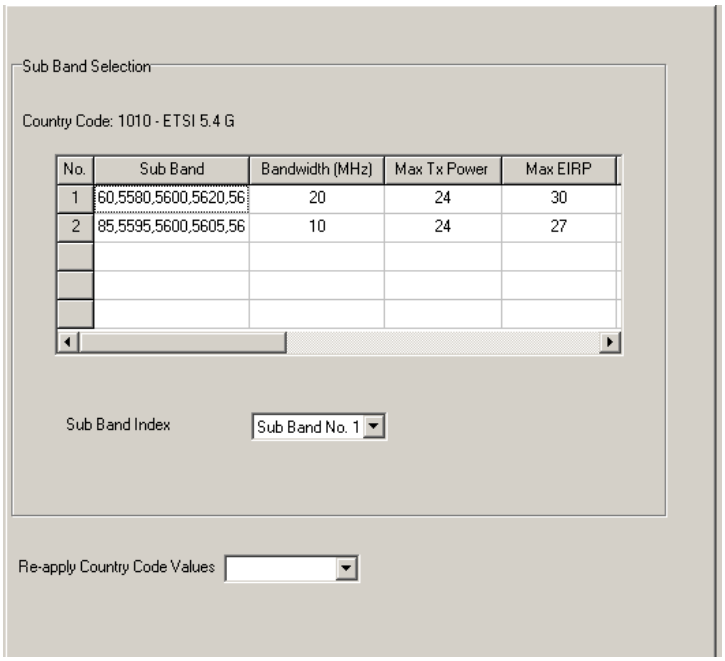


Figure 2-15: Country Parameters Tab

The Country Parameters tab is comprised of the following components:

- **Country Code:** The up to 3 digits country code according to ISO 3166 and the country name. Some regulatory requirements apply to more than one

country. In these cases the Country Code includes a 4 digits proprietary group code and the Country Group name (for example FCC).

- A country dependent parameters table that display the following parameters for each of the available Sub-Bands:
  - **No.**: Sub-Band ID
  - **Sub-Band**: The frequency range available when using the Sub-Band.

NOTE

In some cases, the width of the Sub-Band column is not sufficient to display all available frequencies. Double-click the applicable Sub-Band entry to view the complete list of frequencies in a special pop-up message box.

  - **Bandwidth**: The bandwidth when using the Sub-Band. If more than one bandwidth is allowed, than each bandwidth is associated with a different Sub-Band, since the bandwidth may affect the available frequencies.
  - **Max Tx Power**: The maximum transmit power allowed at the antenna port of the unit.
  - **Max EIRP**: The maximum allowed EIRP (Effective Isotropic Radiated Power).
  - **Min Mod Level**: The lowest allowed modulation level
  - **Max Mod Level**: The highest allowed modulation level
  - **Burst Mode**: Indicates whether Burst Mode operation is supported.
  - **Max Burst Duration**: If Burst Mode is supported, this parameter displays the upper limit for the Maximum Burst Duration parameters.
  - **DFS**: Indicated whether the DFS (Dynamic Frequency Selection) mechanism for identification and avoidance of channels with radar activity is supported.
- **Sub-Band Index:** Available where more than one Sub-Band is available, enabling to select the Sub-Band to be used. In AU, this is the sub-band to be used for planned frequencies in the Frequency tab and for Spectrum Analysis. In SU, this is the sub-band to be used during Spectrum Analysis.

- **Re-apply Country Code Values:** After loading a new SW version with any changes in the relevant Country Code, the Re-apply Country Code Values option must be activated for the changes to take effect.

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

2.4.5 Air Interface Spectrum Analysis Tab

The Spectrum Analysis tab enables you to define the spectrum analysis test parameters, activate a spectrum analysis test and view the spectrum analysis results.

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

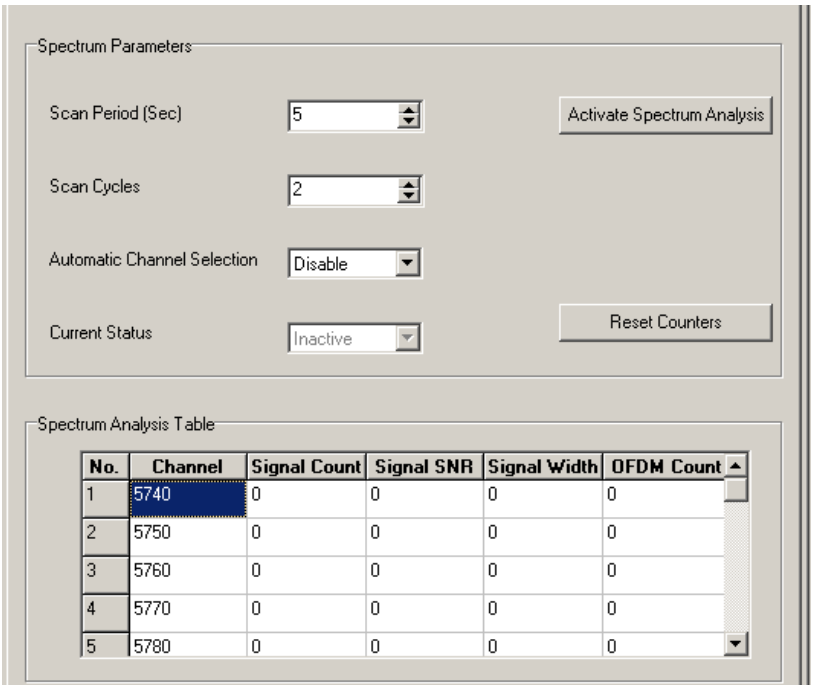


Figure 2-16: Spectrum Analysis Tab

The Spectrum Analysis tab includes the following components:

- **Scan Period**: The Spectrum Analysis Channel Scan Period is the period of staying on each channel belonging to the selected sub-band during each cycle for information gathering when performing spectrum analysis.

  Range: 2-30 seconds.

- **Scan Cycles**: The Spectrum Analysis Scan Cycle is the number of scanning cycles when performing Spectrum Analysis.

  Range: 1-100 cycles.

- **Automatic Channel Selection** (AU only): The Automatic Channel selection option defines weather the AU will choose the best noise free channel upon startup after completion of the spectrum analysis process. The selection is per analysis: once the analysis is completed it will be disabled automatically.

- **Current Status**: A read-only display of the current status of the spectrum analysis test.

- **Activate Spectrum Analysis**: Click on the Activate Spectrum Analysis button to activate the spectrum analysis process. Upon activation, the unit will reset automatically and start-up in spectrum analysis mode.

- **Reset Counters**: Click on the Rest Counters button to clear the spectrum analysis counters.

- **Spectrum Analysis Table**: The Spectrum Analysis Table displays the results of the last analysis process. The displayed information includes the following details for each channel:

  - **Frequency** in MHz

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

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

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

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

2.4.6 Air Interface DFS Tab (AU only)

The DFS tab enables defining the Dynamic Frequency Selection parameters. The DFS tab is available only when managing an AU that uses a Country Code (Sub-Band) with DFS supported.

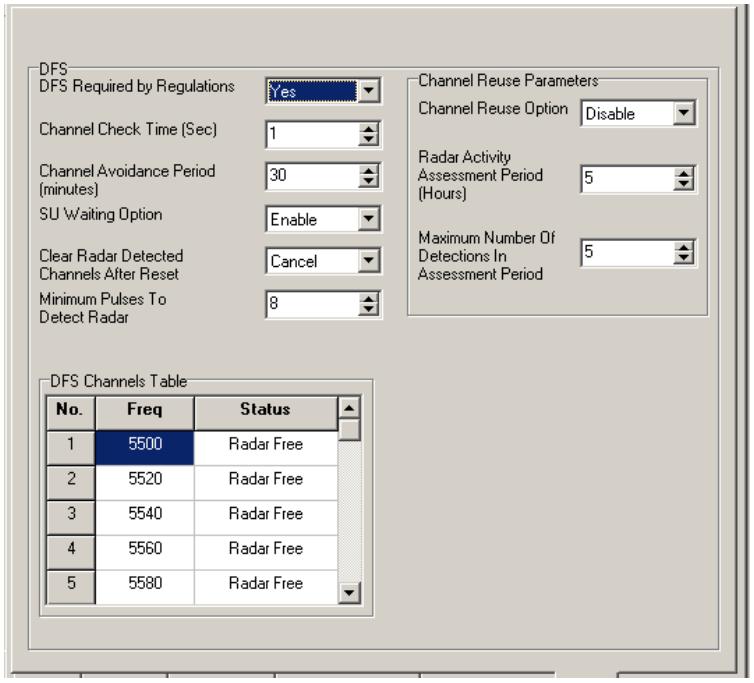


Figure 2-17: DFS Tab

The DFS tab includes the following components:

- **DFS Required by Regulations:** This parameters define whether DFS is required for compliance with applicable local regulations. When set to Yes, the radar detection and dynamic frequency selection mechanism is activated.

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

  The range is 1 to 3600 seconds.

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

  The range is from 1 to 60 minutes.

- **SU Waiting Option:** The SU Waiting Option defines whether the disassociation message sent by the AU after detecting radar activity on the current frequency will include a message instructing the SU to search only for that specific AU before attempting to search for another AU. The message includes also the time period during which the SU should not search for any other AU. The waiting time is the Channel Check Time plus 5 seconds.

- **Clear DFS Channels Table:** When enabled, than after the next reset all viable frequencies will be marked in the database as Radar Free, including frequencies previously marked as either Radar Detected or Adjacent to Radar. In addition, the AU will start operation using its default frequency.

- **Minimum Pulses to Detect Radar:** The minimum number of detected radar pulses before reaching a decision that an active radar is using the channel.

  The range is from 1 to 100 pulses.

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

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

  The range is 1 to 12 hours.

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

  The range is 1 to 10 radar detections.

- **DFS Channels Table:** Displays all the applicable frequencies together with their status in the database (Radar Free, Radar Detected or Adjacent to Radar).

2.5 Best AU Parameters (SU only)

The *Best AU* tab is applicable to Subscriber Units only and enables you to configure parameters related to the Best AU selection algorithm and the preferred AU with which the Subscriber Unit should associate. If the Best AU feature is activated, the SU assigns a grade based on performance level to each AU with which it can associate. The SU then attempts to connect with the best AU, as required.

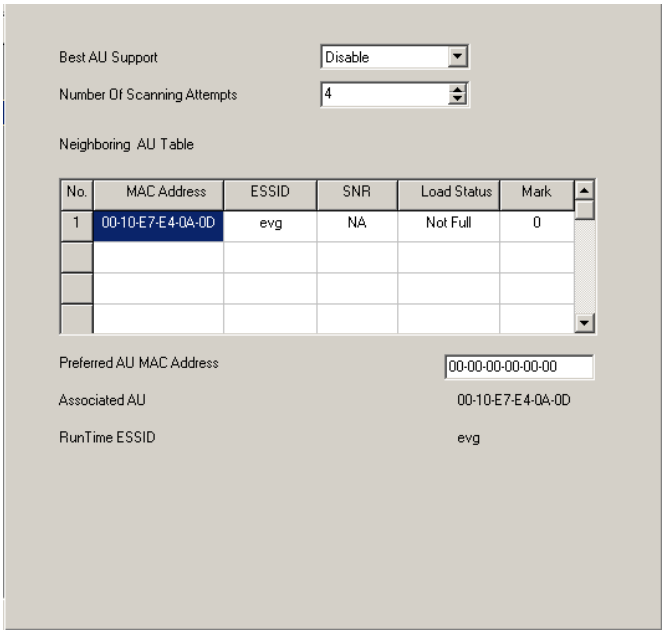


Figure 2-18: Best AU Tab

The *Best AU* tab is comprised of the following components:

- **Best AU Support:** From the dropdown list, select whether to **Enable** or **Disable** the Best AU feature. If disabled, the Subscriber Unit associates with the first Access Unit that it locates with an identical ESSID or Operator ESSID.

- **Number of Scanning Attempts:** Click the up and down arrows or enter a number to the select the number of scanning cycles that the Subscriber Unit uses to gather information regarding the neighboring Access Units. The available values range from 1 to 255.

- **Neighboring AU Table:** A read-only display, the ***Neighboring AU Table*** displays the information gathered by the Subscriber Unit during the last scanning cycle.

- **Preferred AU MAC Address:** In the displayed text box, enter the MAC address of a specific Access Unit with which the Subscriber Unit should associate. Once the SU has identified the preferred AU based on its MAC address, it will associate with it and terminate the scanning process. If the preferred AU is not found, the SU will associate with an AU according to the decision reached using the best BU algorithm.
  The default value is 00-00-00-00-00-00, which means no preferred AU. Enter the required MAC address as 6 groups of two hexadecimal numbers each, separated by either dashes (“-“) or spaces (“ “). For example, 00-11-22-33-44-55 or 00 11 22 33 44 55.

- **Associated AU MAC Address:** A read-only field that displays the MAC address of the Access Unit with which the Subscriber Unit is currently associated.

- **RunTime ESSID:** A read-only field that displays the ESSID currently used by the Subscriber Unit to associate with the Access Unit.

2.6 Network Management Parameters

The *Network Management* tab enables you to protect the unit from unauthorized access by defining a set of IP addresses from which the unit can be managed using protocols such as Telnet, TFTP, SNMP, DHCP or ICMP. This excludes messages generated in the unit, such as SNMP traps or Ping test frames. In addition, you can select from which direction management access is permitted, from the wireless medium, the wired Ethernet, or both.

The *Network Management* tab also enables you to define the management stations to which trap messages are to be sent and to manage the event log.

The *Network Management* tab is divided into two secondary tabs, General and Send Traps.

2.6.1 Network Management General Tab

The *General* tab of the Network Management tab enables you to define management-filtering options.

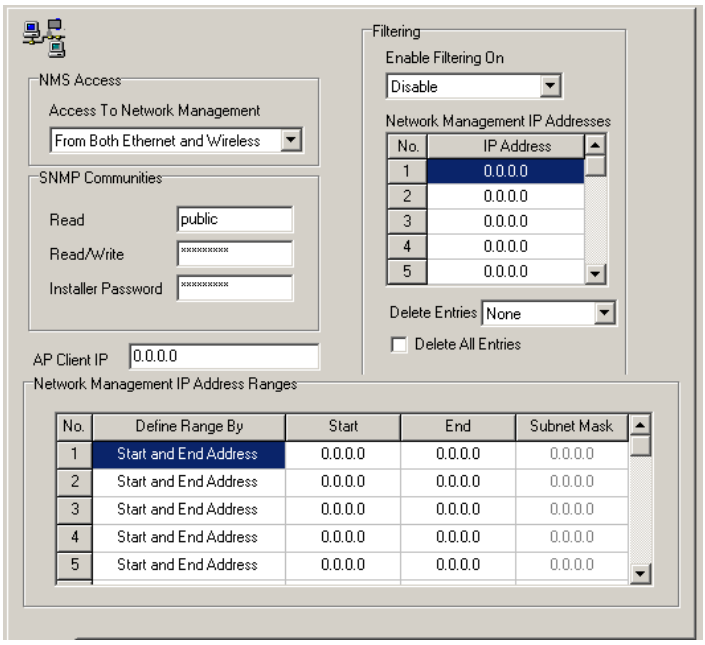


Figure 2-19: Network Management General Tab (SU)

The *General* network management tab is comprised of the following components:

- **Access to Network Management:** From the dropdown list, select the port through which the unit can be managed, from the following options:
  - Wireless Only
  - Ethernet Only
  - Both

CAUTION

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

- **SNMP Communities**
  - Read: Enter the read-only community string, which serves also as the read-only password for the monitor program.
  - Write: Enter the read/write community string, which serves also as the Administrator password.
  - Installer Password: Enter the Installer password.

2.6.1.1 Filtering Parameters

- **Enable Filtering on:** From the dropdown list, select whether to disable or enable the IP address-based management filtering option. If enabled, only stations with an IP address matching one of the entries in the ***Network Management IP Address*** table can manage the unit. When enabling the option, select the port to which the filtering is to be applied, from the following options:
  - Disable
  - Active on Ethernet Port
  - Active on Wireless Port
  - Active on Both
- **Network Management IP Addresses:** To define an IP address through which the unit can be managed, select a row in the IP Address column and enter the required IP address. The table includes up to 10 entries.

- **Delete Entries:** From the dropdown list, select an entry to be deleted from *the* ***Network Management IP Address*** table. The options in the dropdown list relate to the row of the table in which the required IP address is listed.

- **Delete All Entries:** Mark the check box to delete all the entries from the ***Network Management IP Address*** table.

2.6.1.2 AP Client IP (SU only)

The AP Client IP parameter enables configuring in the SU the IP address of a WiFi AP connected to it, providing availability of the IP address information for remote management of the AP. Applicable only for WI2 installations.

2.6.1.3 Network Management IP Address Ranges Table

This table enables defining IP address ranges of stations that are allowed to manage the unit (in addition to the discrete IP addresses that can be defined in the ***Network Management IP Addresses*** table).

The table includes up to 10 entries. Each entry includes:

- **Define Range By**: Indicates whether the range is defined by **Start and End Address** or **Start and Subnet Mask.**

- **Start:** The start IP address.

- **End:** The end IP address. Applicable only for Start and End Address definition method.

- **Subnet Mask:** The subnet mask for the range. Applicable only for Start and Subnet Mask definition method.

To define/modify a management IP range:

1. Click on the required **Define Range By** entry. A drop-down menu will appear, enabling selection between the two definition methods.
2. Select the preferred definition method.
3. Enter the **Start** IP address and the **End** IP address or **Subnet Mask** according to the selected definition method.

2.6.2 Network Management Send Traps Tab

The *Network Management Send Traps* tab enables you to define up to 10 stations that are to receive SNMP trap messages from the unit.

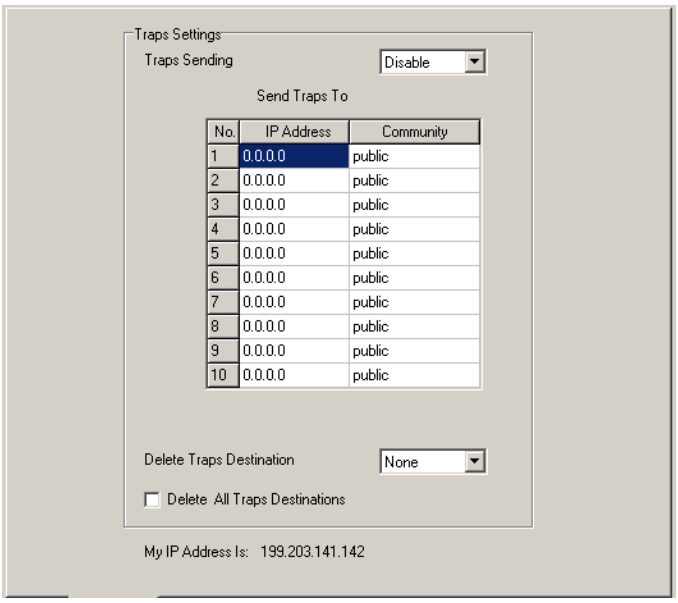


Figure 2-20: Network Management Send Traps Tab

The *Send Traps* tab is comprised of the following components:

- **Trap Sending:** From the dropdown list, select to **Enable** or **Disable** the sending of trap messages from the unit.

- **Send Traps to:** To define a station that is to receive trap messages from the selected unit, select a row in the IP Address column and enter the station's IP address. Then, select the adjoining field in the Community column and enter the required community string.

- **Delete Traps Destination:** From the dropdown list, select an entry to be deleted from the ***Send Traps to*** table. The options in the dropdown list relate to the row of the table in which the required IP address is listed.

- **Delete All Traps Destinations:** Mark the check box to delete all the entries from the ***Send Traps to*** table.

- **My IP Address is:** Displays the IP address of the management station from which you are currently accessing the selected unit.

2.7 Bridging Parameters

The *Bridging Parameters* tab enables you to configure multiple system parameters, including control and filtering options for bridge and broadcast transmissions, VLAN support and Type of Service prioritization. In AUs, it also enables defining the Allow/Deny List, disabling or enabling services to specific SUs.

2.7.1 Bridging Parameters General Tab

The *General* tab enables you to define control mechanisms and filtering options for various types of transmissions.

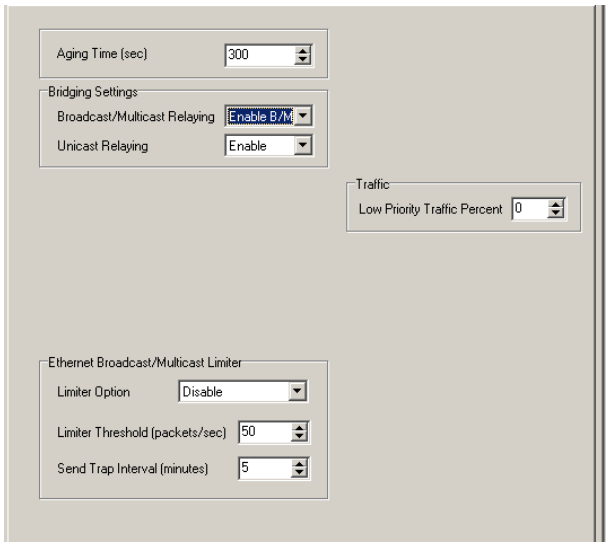


Figure 2-21: Bridging Parameters General Tab – Access Unit

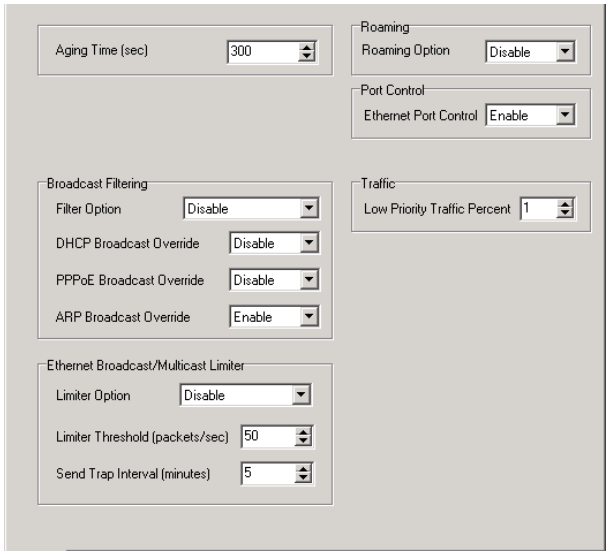


Figure 2-22: Bridging Parameters General Tab – Subscriber Unit

The *Bridging Parameters General* tab is comprised of the following components:

- **Aging Time (sec):** The bridge aging time for addresses of devices on both the wired and wireless sides. This does not include addresses of BreezeACCESS units. The available range is **20 to 2000** seconds.

- **Roaming Option (SU only):** The Roaming Option defines the roaming support of the unit. When set to Enable, the SU will wait only one second before it starts scanning for another AU. In addition, when the Roaming Option is enabled, the SU will send Roaming SNAP messages upon associating with a new AU. This enables fast distribution of the new location for all clients that are behind the SU.

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

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

  The range is between 0 and 100 (%).

2.7.1.1 Broadcast Filtering (SU only)

- **Filter Option:** From the dropdown list, select the Ethernet broadcast filtering functionality for the selected Subscriber Unit. Select from the following options:

  - ◇ Disable, which is the default and means no Ethernet broadcast filtering.

  - ◇ Ethernet only, which filters broadcast messages from the Ethernet port only.

  - ◇ Wireless only, which filters broadcast messages from the wireless link only.

  - ◇ Both, which filters broadcast messages from both the Ethernet and wireless link ports.

- **DHCP Broadcast Override:** From the dropdown list, select whether to **Enable** or **Disable** the override mechanism for DHCP broadcasts. If enabled, DHCP messages are broadcast, even if the ***Filter Options*** parameter is set to filter broadcast messages.

- **PPPoE Broadcast Override:** From the dropdown list, select whether to **Enable** or **Disable** the override mechanism for broadcasting PPPoE messages. If enabled, PPPoE messages are broadcast, even if the ***Filter Options*** parameter is set to filter broadcast messages.

- **ARP Broadcast Override:** From the dropdown list, select whether to **Enable** or **Disable** the override mechanism for broadcasting ARP messages. If enabled, ARP messages are broadcast, even if the ***Filter Options*** parameter is set to filter broadcast messages.

2.7.1.2 Ethernet Broadcast/Multicast Limiter

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

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

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

The Ethernet Broadcast/Multicast Limiter parameters include:

- **Limiter Option**: The Limiter Option defines the limiter's functionality. The available options are:

  - Disable
  - Broadcasts
  - Multicasts No Broadcasts
  - All Multicasts

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

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

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

  The range is from 1 to 60 minutes.

2.7.1.3 Bridging Settings (AU only)

- **Broadcast/Multicast Relaying:** The Broadcast/Multicast Relaying option enables selecting whether the unit performs relaying of broadcasts and/or multicasts. The available options are:

  - Disable
  - Enable B/M (enable relaying of broadcasts and multicasts)
  - Enable B (enable only relaying of broadcasts)
  - Enable M (enable only relaying of multicasts)

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

- **Unicast Relaying:** From the dropdown list, select whether to **Enable** or **Disable** the unicast relaying mechanism. If enabled, unicast packets originating from devices on the wireless link can be transmitted by the AU back to the wireless link devices. If disabled, these packets are not sent back to the wireless link even if they are intended for devices on the wireless link side.

2.7.2 Bridging Parameters VLAN Tab

The *VLAN* tab enables you to define the parameters that control the VLAN support mechanism of the BreezeACCESS units, as shown below.

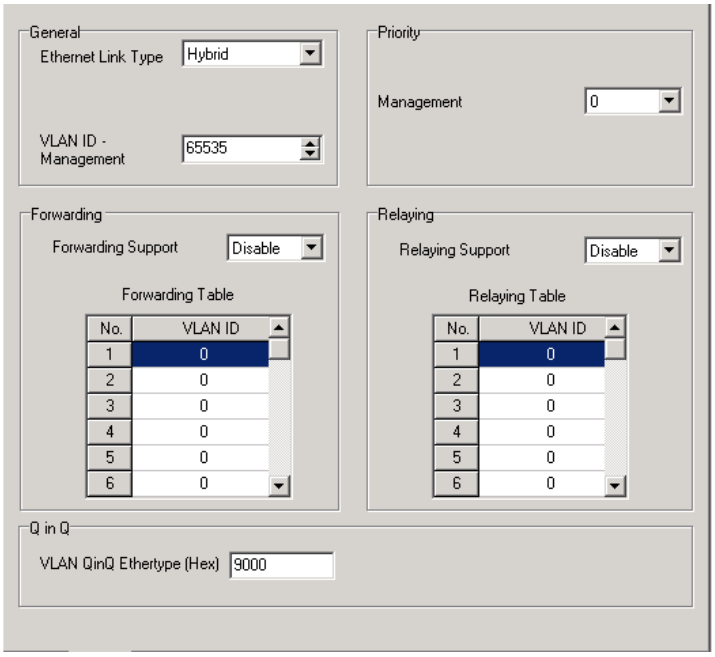


Figure 2-23: VLAN Tab – Access Unit

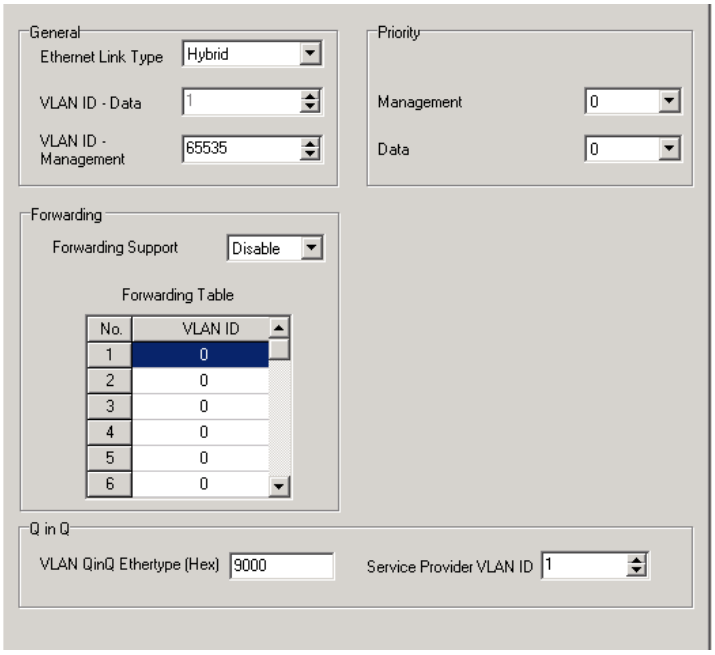


Figure 2-24: VLAN Tab – Subscriber Unit

The *VLAN* tab is comprised of the following components:

2.7.2.1 General

Ethernet Link Type: From the dropdown list, select the functionality of the unit's VLAN-aware capability, from the following options:

- **Access** (available to SUs only): Transfers frames while tagging/untagging them as all devices connected to it are VLAN-unaware. The unit cannot transfer tagged frames.
- **Trunk**: The unit only will transfer tagged (Customer VLAN ID tag) frames, as all devices connected to it are VLAN-aware.
- **Hybrid:** The device will transfer both tagged (Customer VLAN ID tag) and untagged frames as the devices connected to it can be either VLAN-aware or VLAN-unaware.
- **Service Provider**: The device will transfer both single-tagged frames (Service Provider VLAN ID tag) and double-tagged frames (Service Provider VLAN ID tag + Customer VLAN ID tag). The Service Provider tag includes the Service Provider VLAN ID and the VLAN QinQ Ethertype.

- **VLAN ID - Data (SU only):** Applicable for Access links only. The VLAN ID for data frames, which identifies the VLAN to which the Subscriber Unit belongs. The available values range from 1 to 4094.

- **VLAN ID - Management:** The VLAN ID that identifies remote stations for management purposes. This applies to all applications using management protocols such as SNMP, TFTP, DHCP, ICMP (ping) and Telnet. All stations must tag the management frames with the defined ID number. The available values range from 1 to 4094 or 65535 if there is no VLAN.

2.7.2.2 Priority

- **Management:** The value of the user priority field for management frames in units where the ***VLAN ID - Management*** is not set to **65535**. The available values range from 0 to 7.

- **Data (SU only):** Applicable to Access links only. From the dropdown list, select the value of the user priority field for data frames transmitted to the wireless link.
  The available values range from 0 to 7.

2.7.2.3 Forwarding

- **Forwarding Support:** Applicable to Trunk links and Service Provider links. From the dropdown list, select whether to **Enable** or **Disable** the Forwarding Support feature. If enabled, the unit discards any data frame received with a VLAN ID (or a Service Provider VLAN ID) that is not a member of the unit's VLAN Forwarding list, as defined in the ***Forwarding Table***.

- **Forwarding Table:** To add a VLAN ID to the VLAN Forwarding list, select a row in the VLAN ID column and enter a number in the range 1 to 4094. You can enter up to 20 VLAN IDs. Enter 0 to remove an entry.

2.7.2.4 Relaying (AU only)

- **Relaying Support:** Applicable only to Trunk links and Service Provider links. From the dropdown list, select whether to **Enable** or **Disable** the Forwarding Support feature. If enabled, the unit discards any data frame with a VLAN ID (or a Service Provider VLAN ID) relayed from the wireless link, i.e. received from and meant to be transmitted back through the wireless link, and that is not a member of unit's VLAN Relaying list, as defined in the ***Relaying Table***.

- **Relaying Table:** To add a VLAN ID to the VLAN Relaying list, select a row in the VLAN ID column and enter a number in the range 1 to 4094. You can enter up to 20 VLAN IDs. Enter 0 to remove an entry.

2.7.2.5 Q in Q

The Q in Q parameters are applicable only for a Service Provider link. The Q in Q parameters comprise the following components:

- **VLAN Q in Q Ethertype:** Defines the Ethertype of the Service Provider tag.

  The valid values are from 8100 to 9000, 9100 and 9200 (Hex).

- **Service Provider VLAN ID (SU only):** Defines the Service Provider VLAN ID for data frames, identifying the Service Provider VLAN to which the unit belongs.

  The range is from 1 to 4094.

2.7.3 Bridging Parameters Allow/Deny List Tab (AU only)

The Allow/Deny List tab enables to specify SUs that will be either granted or denied services from the AU, based on the value of the MAC Address List Type parameter. When the list is defined as a Deny List, the AU will not provide services to a unit whose MAC address is included in the list, enabling to disconnect units in cases such as when the user had fraudulently succeeded to configure the unit to values different from the subscription plan. When the list is defined as an Allow List, the AU will provide services only to units with a MAC address that is included in the list.

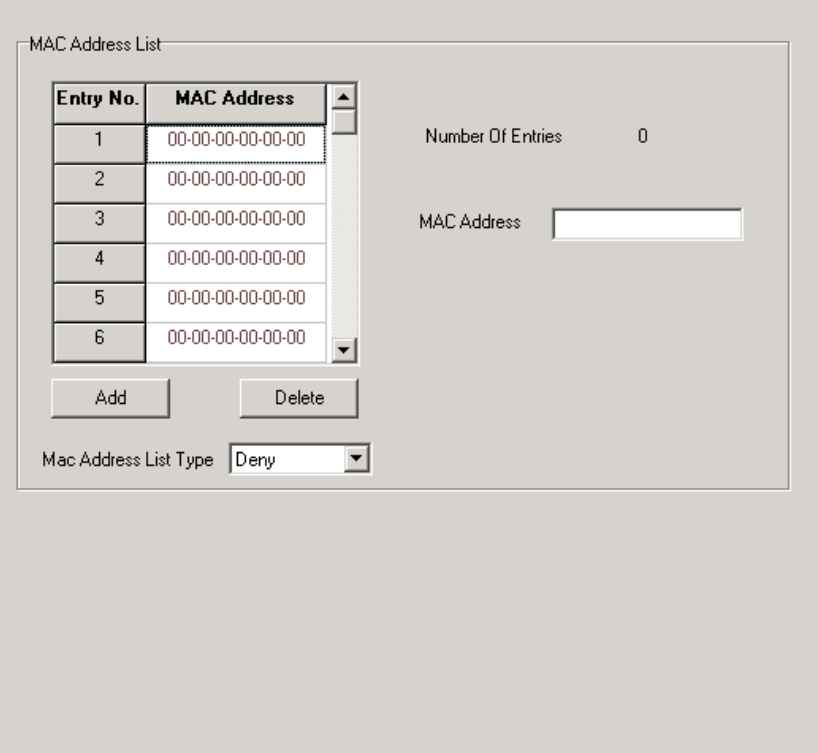


Figure 2-25: Allow/Deny List Tab

The *Allow/Deny List* tab is comprised of the following components:

- **MAC Address List:** A list of up to 100 SUs (specified by the MAC Address).
- **Number Of Entries:** A read-only display of the current number of entries in the MAC Address List.
- **MAC Address** text box: Enter a MAC Address if you wish to add/delete it to/from the MAC Address List.
- **MAC Address List Type:** Defines the working mode of the MAC list:

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

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

- **ADD:** Click to add to the MAC Address List the SU whose MAC Address is entered in the MAC Address text box.

- **Delete:** Click to delete from the MAC Address List the SU whose MAC Address is entered in the MAC Address text box.

2.8 Performance Parameters

The *Performance* tab enables you to control the method by which traffic is transmitted through the BreezeACCESS wireless access network. The *Performance* tab differs slightly between Access Units and Subscriber Units, which is clearly indicated at the relevant parameters.

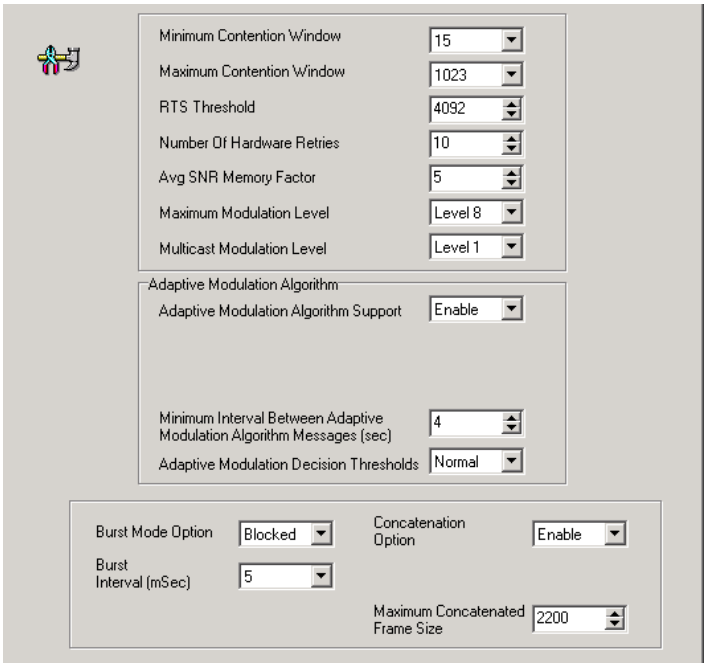


Figure 2-26: Performance Tab – Access Unit

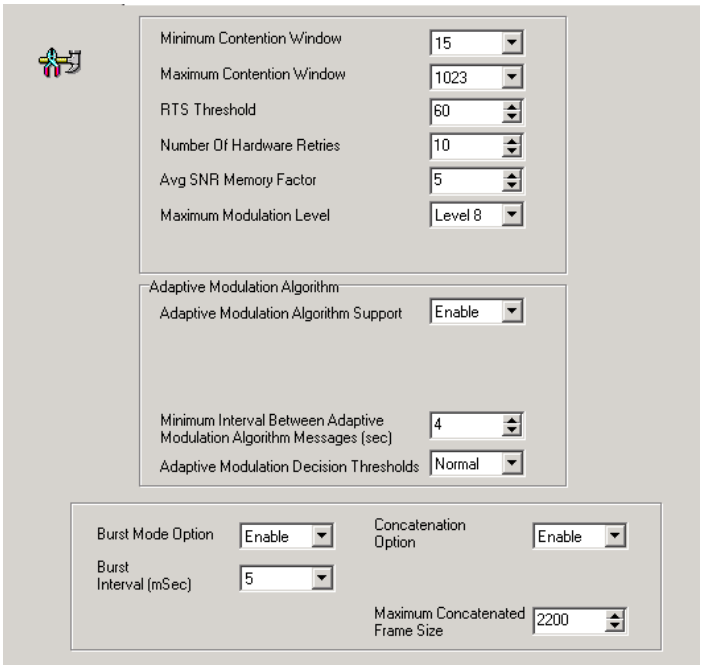


Figure 2-27: Performance Tab – Subscriber Unit

The *Performance* tab is *comprised* of the following components:

- **Minimum Contention Window:** The initial value to be used by the contention window calculation algorithm. The available values are 0, 7, 15, 31, 63, 127, 255, 511 and 1023. 0 disables the contention window back-off algorithm and should be used only in point-to-point applications.

- **Maximum Contention Window:** The maximum value to be used by the contention window calculation algorithm. The available values are 7, 15, 31, 63, 127, 255, 511 and 1023.

- **RTS Threshold:** The minimum frame size that requires an RTS/CTS (Request To Send/Clear To Send) handshake. Frames smaller than the defined value are transmitted directly to the wireless link without the preceding RTS frames. The available values range from 20 to 4032 bytes. 4032 means that the RTS/CTS mechanism is never used.

NOTE

In units with HW revision B or lower running SW Version 3.0 and higher the range is 20 to 2200. In units with HW revision C running SW Version 3.0 the range is 20 to 3400. In all units running SW Version lower than 3.0 the range is 20 to 1600.

- **Number of Hardware Retries:** The maximum number of trials to transmit an unacknowledged frame in each Hardware Retrials phase. The available values range from 1 to 14.

NOTE

The Number of HW Retries parameter is not applicable when the Wireless Link Prioritization Option is enabled.

- **Avg SNR Memory Factor:** The SNR Memory Factor defines the weight of history (value of last calculated average SNR) in the formula used for calculating the current average SNR for received data frames. This average SNR is used by the ATPC algorithm in the AU and is also included in the Adaptive Modulation information messages transmitted by the AU and the SU. The higher the value of this parameter, the higher is the weight of history in the formula.

  Available values: -1 to 32. -1 is for no weight for history, meaning that average SNR equals the last measured SNR.

- **Maximum Modulation Level:** If the Adaptive Modulation algorithm is enabled, it sets the maximum modulation level that can be reached by the

algorithm. If the Adaptive Modulation algorithm is disabled, it sets the fixed modulation level to be used.

- **Multicast Modulation Level (AU only):** The modulation level for transmission of multicast and broadcast data frames. Since multicast and broadcast transmissions are not acknowledged, it is recommended to set a low modulation level to ensure transmission without error.

- **Burst Mode Option:** From the dropdown menu, select whether to Enable or Disable the Burst Mode operation. Burst mode provides an increased throughput by reducing the overhead associated with transmissions in the wireless medium.

NOTE

The Burst Mode parameters are not applicable when the Wireless Link Prioritization Option is enabled.

- **Burst Interval:** The Burst Interval defines the burst size, which is the time in which data frames are sent immediately without contending for the wireless medium. The available values depend on the Sub-Band (Country Code).

- **Concatenation Option**: The Concatenation Option enables or disables the packet concatenation mechanism.

- **Maximum Concatenated Frame Size**: The Maximum Concatenated Frame Size parameter defines the maximum size (in bytes) for a concatenated frame.

  The range is:

  - ◇ 256 to 2200 bytes for units with HW revision A or B.
  - ◇ 256 to 4032 bytes for units with HW revision C or higher.

2.8.1.1 Adaptive Modulation (Multi Rate)

- **Adaptive Modulation Option:** From the dropdown menu, select whether to **Enable** or **Disable** the adaptive modulation decision algorithm.

- **Minimum Interval Between Adaptive Modulation Messages:** The minimum permitted time, in seconds, between consecutive messages carrying information regarding the quality (SNR) of received signals. Available values range from 1 to 3600 seconds.

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

2.9 Service Parameters

The *Service* tab enables you to define user-filtering options (SU only) and MIR/CIR quality of service parameters. It also enables defining various traffic prioritization options and parameters and DRAP parameters (AU only).

The Service Parameters Tab Include:

- General Tab
- Traffic Priority Tab
- DRAP Tab (AU only)
- WL Priority Tab (in units that support the licensed Wireless Link Prioritization feature)

2.9.1 General Service Parameters Tab

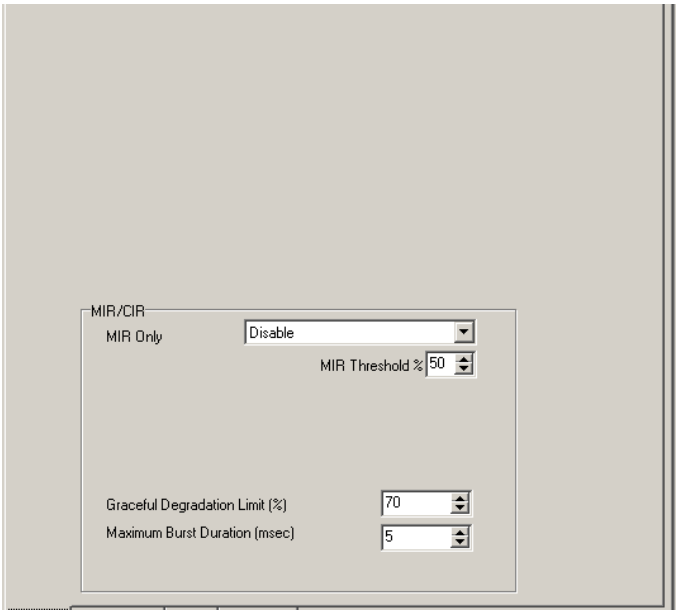


Figure 2-28: Service Tab – Access Unit

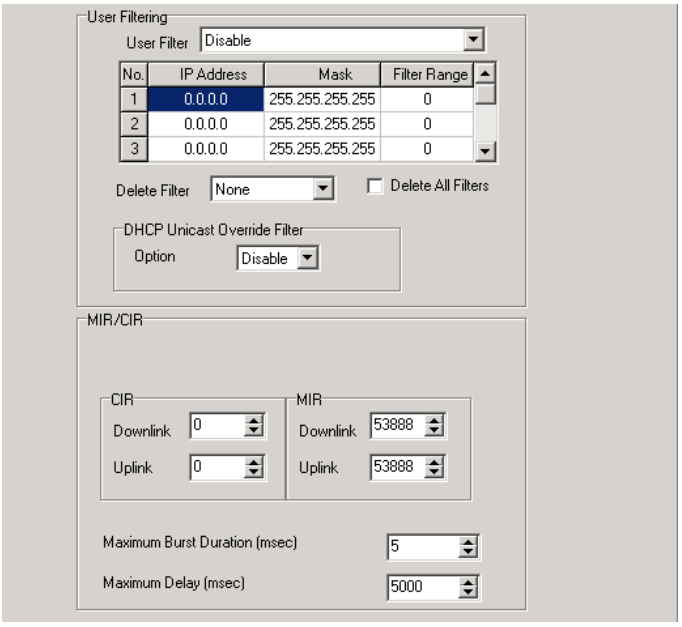


Figure 2-29: Service Tab – Subscriber Unit

The *Service* tab is comprised of the following components:

2.9.1.1 User Filtering Parameters (SU only)

The User Filtering Parameters enable defining the IP addresses of user devices authorized to access the wireless medium for security and/or control purposes.

In addition, they can be used to enable the transmission and reception of specific protocol frames. These filtering options do not affect management frames sent to or generated by the unit.

- **User Filter:** From the dropdown list, select the required user filtering option, as follows:
  - **Disable**, which means no filtering.
  - **IP only**, which means only IP packets pass.
  - **User Defined Address Only**, which means only messages from IP addresses defined in the User Filter table pass.
  - **PPPoE Only**, which means only PPPoE messages pass.
- **User Filter Table:** To define the IP addresses from which data is permitted to pass, select a row in the IP Address column and enter the required IP address. To define a group of addresses, the IP address entered should be the first address in the range. Then, select either the adjoining Mask or Filter Range column and enter the required value. Use the scroll bar to move between the 8 available entries.

NOTE

You can only configure either the Mask or Filter Range. If the Range is other than 0, the Mask entry is ignored.

- **DHCP Unicast Override Filter Option**: When user filtering is activated, unicast DHCP messages are filtered out; therefore the unit cannot communicate with the DHCP server. The DHCP Unicast Override Filter Option enables to overcome this problem. When enabled, unicast DHCP messages pass, overriding the user filtering mechanism.
- **Delete Filter:** From the dropdown list, select the entry to be deleted from the ***User Filter Table***. The available options are **None** and **First** to **Eighth**.
- **Delete All Filters:** Mark the check box to delete all entries from the ***User Filter Table.***

2.9.1.2 MIR/CIR Parameters

- **CIR (SU only):** To define the Committed Information Rate in the **Downlink** (AU to SU) and in the **Uplink** (SU to AU). The range depends on unit type. The

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

- **MIR (SU only):** To define the Maximum Information Rate in the **Downlink** (AU to SU) and in the **Uplink** (SU to AU). The range depends on unit type. The actual value will be the entered value rounded to the nearest multiple of 128 (N*128).

- **Maximum Burst Duration:** To define the maximum time during which inactivity bonus time can be accumulated for future burst transmissions. Range: 0 – 2000 (milliseconds).

- **Maximum Delay (SU only):** To define the maximal time packets may be delayed by the MIR\CIR mechanism. Above the configured maximal period the packets are discarded.
  Range: 300 - 10000 (milliseconds).

- **Graceful Degradation Limit (AU only):** To define the maximum limit for activating the graceful degradation algorithm.
  Range: 0 – 70 (%).

- **MIR Only (AU only):** When the MIR Only option is enabled, it overrides the MIR/CIR algorithm for determining actual information rate and forces the algorithm to operate with MIR parameters' settings only. When enabled, the Graceful Degradation algorithm is disabled.

- **MIR Threshold (AU only):** Sets the threshold of wireless link utilization above which the MIR/CIR algorithm is activated.
  The range is from 0 to 100 (%

2.9.2 Traffic Priority Tab

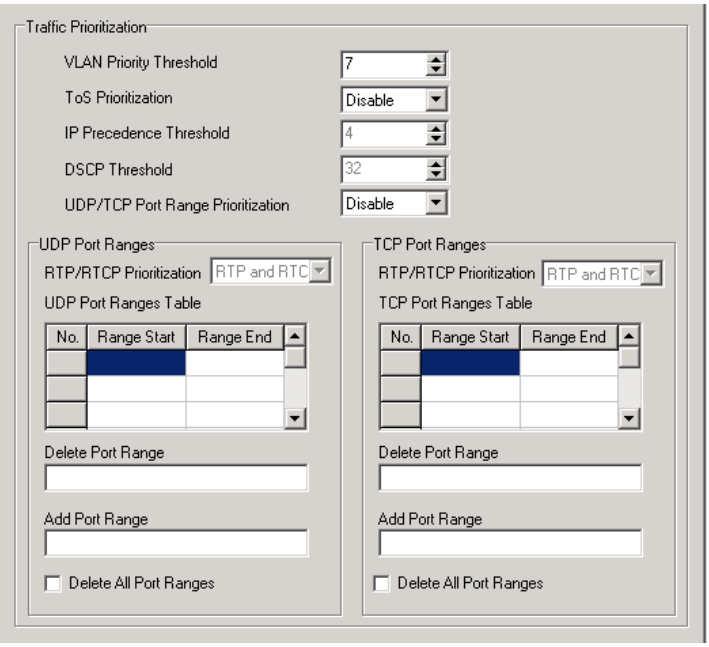


Figure 2-30: Traffic Priority Tab

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

The prioritization of the packets is done using different classifiers:

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

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

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

2.9.2.1 Traffic Prioritization

The Traffic Prioritization parameters include:

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

  Valid values range from 0 to 7. A value of 7 (the default) means that all packets get a low priority (equivalent to disabling the VLAN-based classifier).

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

  - **Disable**

  - **IP Precedence** (RFC791 based prioritization)

  - **DSCP** (RFC2474 based prioritization)

- **IP Precedence Threshold**: The IP Precedence Threshold parameter is applicable when the ToS Prioritization Option is set to IP Precedence. If the value of the 3 IP Precedence bits in the IP header is higher than this threshold, the packet is routed to the High queue. If the value is lower than or equal to this threshold, the packet will be transferred to the Low queue (unless it is assigned a High priority by another classifier).

  Valid values range from 0 to 7. A value of 7 (the default) means that all packets get a low priority (equivalent to disabling the IP Precedence-based classifier).

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

  Valid values range from 0 to 63. A value of 63 (the default) means that all packets get a low priority (equivalent to disabling the IP Precedence-based classifier).

- **UDP/TCP Port Range Prioritization**: The UDP/TCP Port Range Prioritization parameter defines whether port ranges based prioritization is enabled or disabled. The following options are available:
  - ◇ Disable
  - ◇ UDP Only
  - ◇ TCP Only
  - ◇ UDP and TCP

2.9.2.2 UDP Port Ranges/TCP Port Ranges

The UDP/TCP Port Ranges parameters allow defining port ranges to be used as priority classifiers when the UDP/TCP Port Ranges Prioritization is set to enable the applicable port-based classification. All relevant packets whose destination is included in the list will be routed to the High queue. All other packets will be routed to the Low queue (unless they were assigned a High priority by another classifier).

The UDP/TCP Port Range parameters include:

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

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

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

  The available options are:
  - ◇ RTP and RTCP
  - ◇ RTP Only
- **UDP/TCP Port Ranges Table**: Displays the current prioritized port ranges (up to 64 entries).

- **Add Port Range**: Enter the UDP/TCP port ranges to be added to the UDP/TCP Port Range Table. The list can include up to 64 ranges. It is possible to add discrete port numbers and/or ranges. In ranges, a hyphen is used to separate between start and end port numbers. A comma is used to separate between entries.

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

- **Delete Port Range**: Enter the UDP/TCP port ranges to be deleted from the UDP/TCP Port Range Table. It is possible to delete discrete port numbers and/or ranges. In ranges, a hyphen is used to separate between start and end port numbers. A comma is used to separate between entries.

- **Delete All Port Ranges**: Check this option to delete all UDP/TCP port ranges from the list of priority port numbers.

2.9.3 DRAP Tab (AU Only)

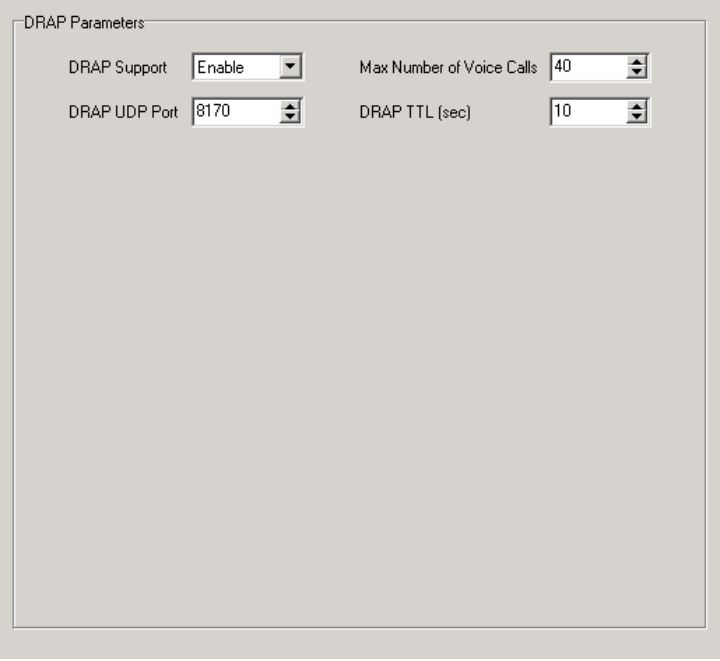


Figure 2-31: DRAP Tab

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

The following DRAP-related options and parameters are available:

- **DRAP Support:** Enables or disables the DRAP feature.

- **DRAP UDP Port:** Defines the UDP port used by the DRAP protocol.

  The range is from 8000 to 8200.

- **Max Number of Voice Calls:** Defines the maximum number of active calls in the cell.

  The range is between 0 and 255.

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

  The range is between 1 and 255 (seconds).

2.9.4 WL Priority Tab (AU only)

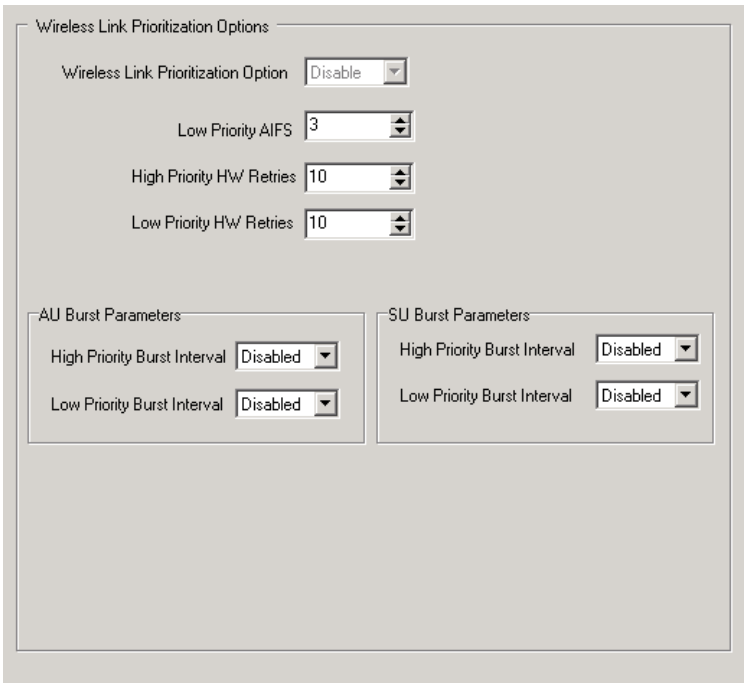


Figure 2-32: WL Priority Tab

The Wireless Link Prioritization parameters enables configuring parameters that affect the processes of gaining access to the wireless media and of transmitting high/low priority packets.

The Wireless Link Prioritization feature is a licensed feature and is available only in units with the suitable Feature License.

The wireless Link Prioritization parameters include:

- **Wireless Link Prioritization Option**: The Wireless Link Prioritization Option enables or disables the Wireless Link Prioritization feature.

- **Low Priority AIFS**: The Low Priority AIFS defines the AIFS number of time slots that will be used by the AU and the SUs served by it for low priority traffic.

  The range is from 3 to 254 (time slots).

- **High Priority HW Retries**: The maximum number of times that an unacknowledged high priority unicast packet can be retransmitted. This is the value that will be used by the AU and by the SUs served with it.

  The range is from 1 to 14 times.

- **Low Priority HW Retries**: The maximum number of times that an unacknowledged low priority unicast packet can be retransmitted. This is the value that will be used by the AU and by the SUs served with it.

  The range is from 1 to 14 times.

- **AU Burst Parameters**

  - **High Priority Burst Interval**: The maximum duration of a burst that can be made by the AU for high priority packets.

    The measurement unit is 250 microseconds and the range is from 1 to 40 (0.25 to 10 milliseconds), or 0 to disable bursts for high priority packets.

  - **Low Priority Burst Interval**: The maximum duration of a burst that can be made by the AU for low priority packets.

    The measurement unit is 250 microseconds and the range is from 1 to 40 (0.25 to 10 milliseconds), or 0 to disable bursts for low priority packets.

- **SU Burst Parameters**

  - **High Priority Burst Interval**: The maximum duration of a burst that can be made by an SU for high priority packets.

The measurement unit is 250 microseconds and the range is from 1 to 40 (0.25 to 10 milliseconds), or 0 to disable bursts for high priority packets.

- **Low Priority Burst Interval**: The maximum duration of a burst that can be made by an SU for low priority packets.

  The measurement unit is 250 microseconds and the range is from 1 to 40 (0.25 to 10 milliseconds), or 0 to disable bursts for low priority packets.

2.10 Security Parameters

The *Security* tab enables you to define security options and parameters. The Security tab differs slightly between Access and Subscriber Units. The applicable parameters are clearly indicated.

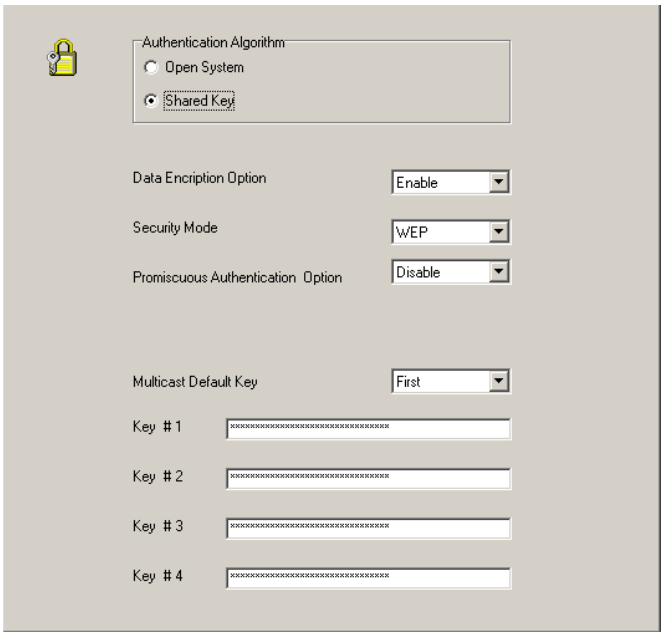


Figure 2-33: Security Tab – Access Unit

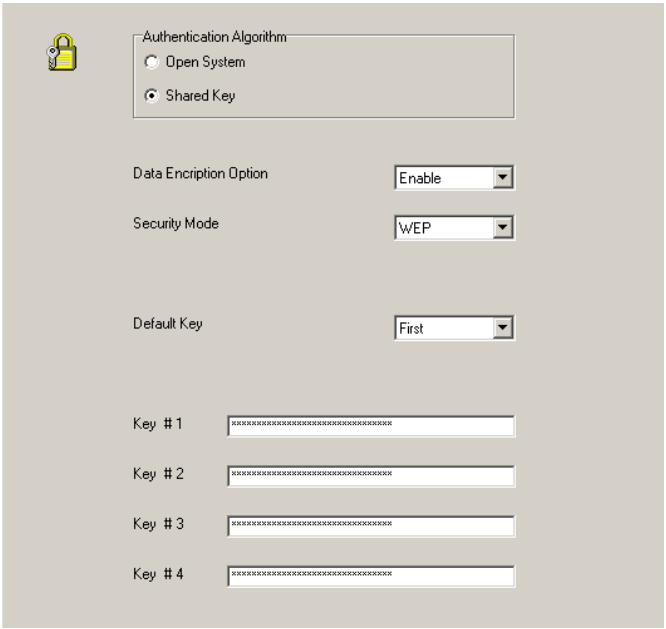


Figure 2-34: Security Tab – Subscriber Unit

The *Security* tab is comprised of the following components:

- **Authentication Algorithm:** Enables selection between **Open System** (no encryption) and **Shared Key** (encryption) authentication modes.

NOTE

The AU and all the SUs it serves must use the same Authentication Algorithm option.

- **Data Encryption Option:** From the dropdown menu, select whether to Enable or Disable the data encryption option.

NOTE

The AU and all the SUs it serves must use the same Data Encryption mode.

- **Security Mode**: From the dropdown menu, select whether to use WEP, AES OCB or FIPS-197 encryption standard.

NOTE

The FIPS 197 encryption algorithm is a licensed feature, and is available only in units with the required license. FIPS 197 can be supported only in units with HW revision C or higher.

- **Default Key** (SU only): From the dropdown menu, select which of the 4 keys should be used for authentication privacy and/or data encryption.
- **Default Multicast Key** (AU only): From the dropdown menu, select which of the 4 keys should be used for encrypting multicasts.
- **Promiscuous Authentication Mode** (AU only): From the dropdown menu, select whether to enable the Promiscuous Authentication mode, allowing any SU to be authenticated by and communicate with the AU regardless of its security settings.

NOTE

Do not leave the AU in the mode of Promiscuous Authentication enabled for prolonged periods. Use it only when absolutely necessary, perform the required actions (SW upgrade and or setting Security parameters in a new SU) as quickly as possible and disable it. The unit will return automatically to Promiscuous Authentication disabled mode after reset.

- **Key # 1** through **Key # 4**: Enter the required key. Each key comprises 32 hexadecimal digits. For security reasons these are write-only fields.

2.11 Site Survey

The *Site Survey* tab displays read-only results of various tests and counters for verifying the quality of the wireless link. This information can be used to help determining where to position the units for optimal coverage, antenna alignment and to assist in troubleshooting.

The *Site Survey* tab is comprised of 4 secondary tabs: *Traffic*, *Tx Counters*, *Rx Counters* and *Per Modulation Level Counters* (SU) or *Per SU Counters* (AU).

2.11.1 Site Survey Traffic Tab

The *Traffic* tab displays general Ethernet traffic statistics for the selected unit.

Figure 2-35: Site Survey Traffic Tab

2.11.1.1 Ethernet Counters

- **Tx Packets:** Displays the total number of packets received from the Ethernet port.
- **Rx Packets:** Displays the number of packets transmitted by the unit to the Ethernet port. These include packets received from the wireless medium and packets generated by the unit itself.

To reset the Ethernet counters to zero:

Click Reset Counters to reset the Ethernet counters to zero. This reverts to 0 also the Tx and Rx counters.

To view a real-time graph of a counter:

Double-click on the value of a counter to view a real-time graph of the selected counters. For more details refer to section 2.11.6.

2.11.2 Site Survey Tx Counters Tab

The *Tx Counters* tab displays information regarding data transmitted from the selected unit.

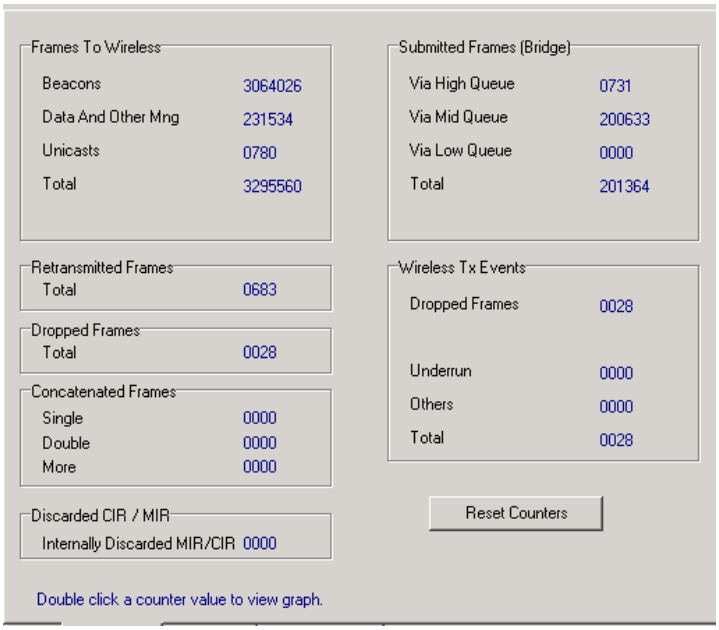


Figure 2-36: Site Survey Tx Counters Tab (AU)

The *Tx Counters* tab is comprised of the following components:

2.11.2.1 Frames to Wireless

- **Beacons (AU only):** The number of Beacon frames transmitted to the wireless medium.
- **Data and Other Mng (AU only):** The number of data and other management frames (excluding beacons) transmitted to the wireless medium. The count includes multicasts/broadcasts, and one count for each unicast frame transmitted successfully (excluding retransmissions).
- **Unicasts (AU only):** The number of unicast frames successfully transmitted to the wireless medium, excluding retransmissions.
- **Total:** The number of frames transmitted to the wireless medium. The count includes one count for each data frame transmitted successfully (excluding

retransmissions), and the number of transmitted control and wireless management frames.

2.11.2.2 Submitted Frames (Bridge)

- **Via High Queue:** Displays the number of frames sent to the bridge and routed to the highest priority queue for transmission to the wireless medium.
- **Via Mid Queue:** Displays the number of frames sent to the bridge and routed to the medium priority queue for transmission to the wireless medium.
- **Via Low Queue:** Displays the number of frames sent to the bridge and routed to the lowest priority queue for transmission to the wireless medium.
- **Total:** Displays the total number of data frames submitted to the bridge for transmission to the wireless medium. This statistic does not include internally generated control or wireless management frames or retransmissions.

2.11.2.3 Retransmitted Frames

- **Total:** The total number of retransmissions of data frames (counts all unsuccessful transmissions/retransmissions).

2.11.2.4 Dropped Frames

- **Total:** Displays the total number of frames that were dropped after being retransmitted to the extent of the maximum permitted number of retransmissions.

2.11.2.5 Concatenated Frames

- **Single**: The total number of concatenated data frames with a single data packet transmitted to the wireless medium.
- **Double**: The total number of concatenated data frames with two data packets transmitted to the wireless medium.
- **More**: The total number of concatenated data frames with more than two data packets transmitted to the wireless medium.

2.11.2.6 Discarded CIR/MIR

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

2.11.2.7 Wireless Tx Events

- **Dropped Frames:** The number of frames that were dropped because they were retransmitted to the maximum allowed number of retransmissions without being acknowledged.
- **Underrun:** The number of times that a transmission was aborted because the rate of submitting frames for transmission exceeds the available transmission capability.
- **Others:** The number of Tx events due to reasons other than those represented by the other Tx Events counters.
- **Total:** The total number of Tx events.

To reset Tx counters to zero:

Click Reset Counters to revert the Tx counters to zero. This reverts to 0 also the Traffic (Ethernet) and Rx counters.

To view a real-time graph of a counter:

Double-click on the value of a counter to view a real-time graph of the selected counters. For more details refer to section 2.11.6.

2.11.3 Site Survey Rx Counters Tab

The Rx Counters tab displays statistics regarding the traffic received by the selected unit.

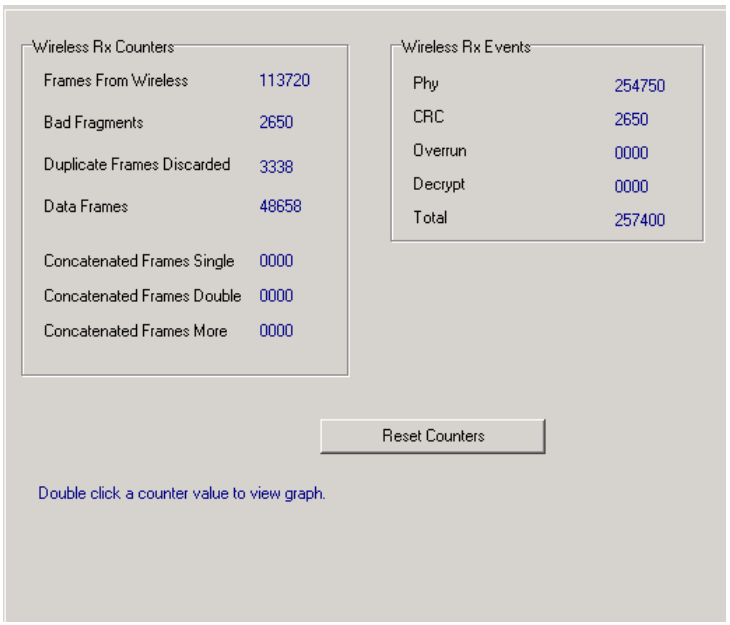


Figure 2-37: Site Survey Rx Counters Tab

The *Rx Counters* tab is comprised of the following components:

2.11.3.1 Wireless Rx Counters

- **Frames from Wireless:** Displays the total number of frames received from the wireless medium, including data, control and wireless management frames and beacons received from the AU. The count does not include frames discarded internally, bad frames and duplicate frames.

- **Bad Fragments:** Displays the total number of frames received from the wireless medium that contain CRC errors.

- **Duplicate Frames Discarded:** Displays the number of frames discarded because multiple copies are received.

- **Data Frames:** The total number of data frames received from the wireless medium, including duplicate frames.

- **Concatenated Frames Single**: The total number of concatenated data frames with a single data packet received from the wireless medium.

- **Concatenated Frames Double**: The total number of concatenated data frames with two data packets received from the wireless medium.

- **Concatenated Frames More**: The total number of concatenated data frames with more than two data packets received from the wireless medium.

2.11.3.2 Wireless Rx Events

- **Hardware:** The number of frames that were not received properly due to a hardware problem.

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

- **Overrun:** The number of frames that were discarded because the receive rate exceeded the processing capability or the capacity of the Ethernet port.

- **Decrypt:** The number of frames that were not received properly due to a problem in the data decryption mechanism.

- **Total:** The total number of Rx events.

To reset Rx counters to zero:

Click Reset Counters to revert the Rx counters to zero. This reverts to 0 also the Tx and Traffic (Ethernet) counters.

To view a real-time graph of a counter:

Double-click on the value of a counter to view a real-time graph of the selected counters. For more details refer to section 2.11.6.

2.11.4 Site Survey Per Modulation Level Counters Tab (SU)

The *Per Modulation Level Counters* tab displays information related to each modulation level supported by the selected unit.

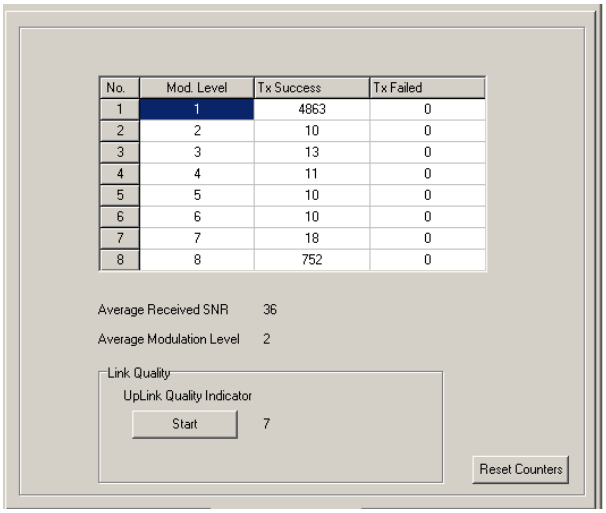


Figure 2-38: Per Modulation Level Counters Tab – Subscriber Unit

The *Per Modulation Level Counters* tab is comprised of a table with the following components:

- **Mod. Level:** The applicable modulation level.
- **Tx Success:** The total number of unicast frames successfully transmitted by the selected unit at the applicable modulation level (excluding retransmissions).
- **Tx Failed:** The total number of failures to successfully transmit unicast frames at the applicable modulation level.
- **Average Received SNR:** The average Signal to Noise Ratio of the received frames.
- **Average Modulation Level** (AML): The average modulation level (rounded to the nearest integer) since the last time the Per Modulation Level counters were reset. The average is calculated using the SUCCESS count at each modulation level as weights.
- **Link quality Indicator (LQI):** Click on the Start button to gather information on the average quality of the wireless link to the AU, using the dynamically updated average modulation level measurements. After a short period the Link Quality Indicator will be displayed.

In order to get quick and reliable LQI measurements, there should be sufficient traffic between the SU and the AU. It is recommended to have traffic of at least 100 packets per second.

If Limited Test is indicated next to the LQI results, it means that the results may not indicate the true quality since not all modulation levels from1 to 8 are available. The limitation may be due to the HW of the unit (HW Revision A), or the applicable parameters in the country code, or the configurable Maximum Modulation Level parameter.

To reset all Per Modulation Level Counters to zero:

Click Reset Counters to revert all Per Modulation Level Counters to zero.

To refresh the display:

Click Refresh to refresh the display.

2.11.5 Site Survey Per SU Counters Tab (AU)

The Per SU Counters tab displays information related to each of the associated SUs.

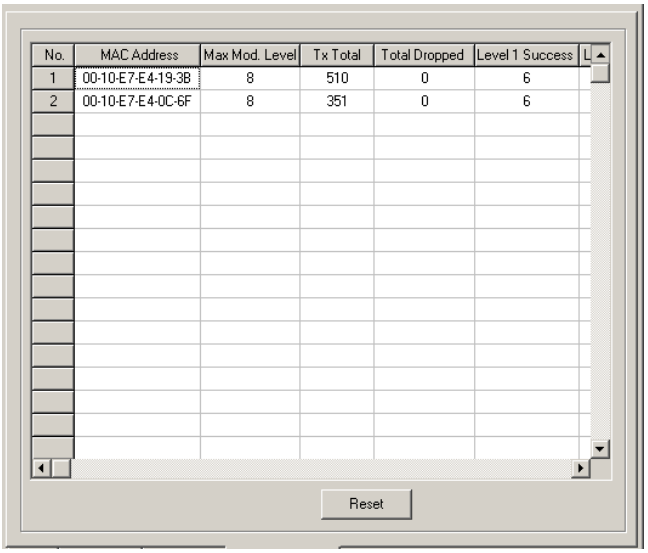


Figure 2-39: Per SU Counters Tab - Access Unit

The *Per SU Counters* tab is comprised of a table that includes the following information for each associated Subscriber Unit:

- **MAC Address:** The MAC address of the SU.
- **Max Mod. Level:** The value configured in the SU for the ***Maximum Modulation Level*** parameter.

- **Tx Total:** The total number of unicast frames (excluding retransmissions) that were successfully transmitted to the SU

- **Dropped Total:** The total number of frames intended to the SU that were dropped because they were retransmitted to the extent of the maximum allowed number of retransmissions without being acknowledged.

- **Level N Success:** The number of unicast frames (excluding retransmissions) that were successfully transmitted to the SU at each of the applicable modulation levels.

- **Level N Failed:** The number of failures to successfully transmit unicast frames intended to the SU at each of the applicable modulation levels.

Use the vertical scroll bar to review additional units. Use the horizontal scroll bar to review additional parameters.

To reset all statistics to zero:

Click Reset to revert all statistics to zero.

To refresh the display:

Given the time required to acquire updated information from the selected units, the display is not continuously updated.
Click Refresh to update the display with information gathered from the selected unit.

2.11.6 The Graph Option

In the Traffic, Tx Counters and Rx Counters tabs you can double-click on the value displayed for a counter to view the real-time graph of the selected counter.

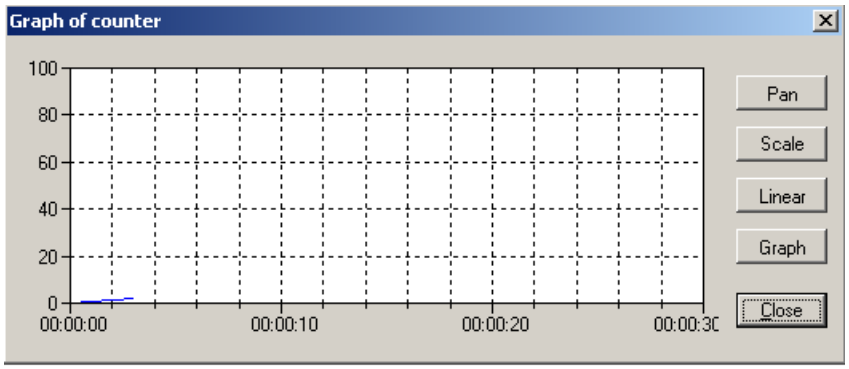


Figure 2-40: Graph

You can modify the display using the buttons on the right side of the window:

- **Pan/Zoom** toggle button: In Pan mode, click the mouse on the graph area and move left/right to shift the time axis, or up/down to shift the value axis. In Zoom mode, click the mouse on the graph area and move left/right to change the resolution the time axis, or up/down to change the resolution of the value axis.

- **Scale:** If you lost track of the where about of the graph (due to shifting it in Pan mode), click on the Scale button to correct the scale.

- **Linear/Log** toggle button: Enables selection of either linear or logarithmic scale for the value axis.

- **Graph/Bar** toggle button: Enables selection of the graph type: Graph (line) or bar.

2.12 Trap Monitor

The *Trap Monitor* tab enables viewing details of traps received from all units that send traps to the BreezeCONFIG management station.

To enable sending of traps in managed units:

In the Network Management Send Traps tab of each relevant unit, configure the **Traps Sending** to Enable and add the IP Address of the BreezeCONFIG station to the **Send Traps To** table.

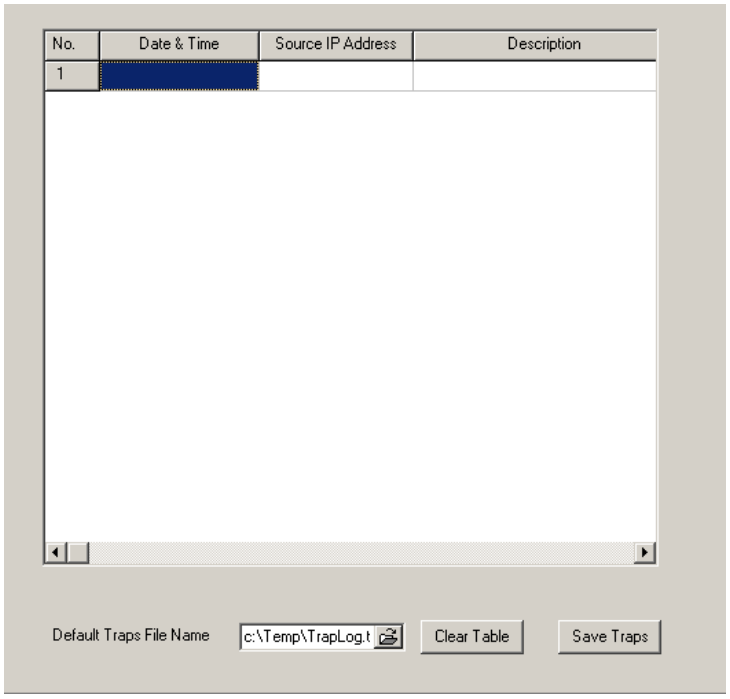


Figure 2-41: Trap Monitor Tab

The *Trap Monitor* tab is comprised of the following columns:

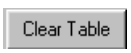
- **Date & Time:** Displays the date and time that the SNMP trap is received.
- **Source IP Address:** Displays the IP address of the unit that sent the SNMP trap.
- **Description:** Displays a description of the SNMP trap message. The trap variables are displayed in the relevant following columns.
- **Device MAC Address:** Displays the MAC address of the unit from which the SNMP trap originated.

- **Associated SU MAC Address:** Applicable only to AU traps where an associated SU is involved. The MAC address of the associated SU.
- **Associated AU MAC Address:** Applicable only to SU traps where an associated AU is involved. For example, association traps. The MAC address of the associated AU.
- **Parameter Changed:** Displays the type of parameter modified during a configuration change. This can include IP Filter or VLAN.
- **IP Address of Telnet User:** Displays the IP address of a management station logged in to the relevant unit for management purposes via Telnet.
- **Access Rights:** Displays the access level of the user logged via the monitor port or Telnet, if applicable.
- **Toggle:** On or off, if applicable.
- **RTx (%):** Applicable to AU only when the number of retransmissions as a percentage of total transmissions has changed below or above the threshold defined by the ***Wireless Trap Threshold*** parameter. Indicates the most recently measured number of retransmissions as a percentage of total transmissions.
- **Login/Logout:** Displays each time a user logs in or out of the monitor application via Telnet.
- **FTP/TFTP Session Status:** The status of the last FTP/TFTP loading process.
- **DFS New Frequency**: Applicable only to AU with the DFS Option enabled. The new frequency in MHz after detecting radar on a previous channel.
- **SW Version:** Applicable to a trap indicating that an SU with SW version below 4.0 tries to associate with an AU using SW version 4.0 or higher, with the Wireless Link Prioritization Option enabled. This is the SW Version of the SU.

To define the Default Traps File Name:

If the number of entries reaches 5000, the current contents are saved to a log file and the Trap Monitor is cleared. Click the  icon to open a dialog box for defining the name and location of the Default Traps File Name.

To clear the display:

Click 

to clear the display.

To save the traps into a log file:

Click 

to save the current contents into a log file.