Table 3-4: SU-ODU LEDs

Name		Description	Functionality
W-LINK	📡	Wireless Link Indictor	■ Green – Unit is associated with an AU, no wireless link activity ■ Blinking Green – Data received or transmitted on the wireless link. Blinking rate is proportional to wireless traffic rate ■ Off – Wireless link is disabled
Status	⏻	Self-test and power indication	■ Green – Power is available and self-test passed. ■ Blinking Amber – Testing (not ready for operation) ■ Red – Self-test failed – fatal error
ETH	🖧	Ethernet activity/ connectivity indication	■ Green – Ethernet link between the indoor and outdoor units is detected, no activity ■ Blinking Green – Ethernet connectivity is OK, with traffic on the port. Blinking rate proportional to traffic rate. ■ Red – No Ethernet connectivity between the indoor and outdoor units.
SNR BAR (SU-RA)		Received signal strength Indication	■ Red LED: Signal is too low (SNR<4 dB) ■ 8 green LEDs: Quality of the received signal ■ Orange LED: Signal is too high (SNR > 50 dB)

Table 3-5: SU-ODU SNR Bar LED Functionality

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

3.5.2 Indoor Unit Verification

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

Table 3-6 provides information for the BS-AU IDU LEDs. Table 3-7 lists the LEDs of the PS1073 IDU.

Table 3-6: BS-AU LEDs

Name	Description	Functionality
W-LINK	Wireless link activity	■ Green - At least one SU is associated. ■ Blinking Red - No SU is associated. ■ Off - Wireless link is disabled.
ODU CURRENT CONSUMPTION	Current Consumption of the Outdoor Unit	■ Red - over current. ■ Blinking Red - open circuit or below anticipated current consumption. ■ Green - within tolerance.
ODU STATUS	Outdoor Unit Self-test	■ Green - Self test passed and ODU ready for operation. ■ Blinking Amber - Testing (not ready for operation) ■ Red - fatal failure.
IDU PWR	Power indication for the Indoor Unit	■ Green - IDU power is OK. ■ Off - no power is supplied to the IDU.
ALARM	Indoor Unit Alarm Indication	■ Red - a fatal failure indication. ■ Off - IDU is functioning properly.

Table 3-7: PS1073 SU IDU / AU-SA IDU LEDs

Name	Description	Functionality
POWER	Power Indication	■ Green – IDU power is OK ■ Off – No power or power failure
ETH	Self test and end-to-end Ethernet connectivity	■ Off – No Ethernet connectivity has been detected between the outdoor unit and the device connected to the indoor unit.

Table 3-7: PS1073 SU IDU / AU-SA IDU LEDs

Name	Description	Functionality
		■ Green – Self-test passed and Ethernet connection confirmed by the outdoor unit (Ethernet integrity check passed).

3.5.3 SU-I Unit Verification

To verify the correct operation of the SU-I unit, examine the LED indicators located on the front panel of the SU-I unit.

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

Table 3-8: SU-I LEDs

Name		Description	Functionality
⚲	Status	Self-test and power indication	Green: Power is available and self-test passed. Blinking Amber: Testing (not ready for operation) Red: Self-test failed. Fatal error
🖧	Ethernet	Ethernet activity/ connectivity indication	Green: Ethernet link between the SU-I and the data equipment is detected, no activity Blinking Green: Ethernet connectivity is OK, with traffic on the port. Blinking rate proportional to traffic rate. Red: No Ethernet connectivity between the SU-I and the data equipment.
⏻	W-Link	Wireless Link traffic Indication	Green: Unit is associated with an AU, no wireless link activity Blinking Green: Data received or transmitted on the wireless link. Blinking rate is proportional to traffic rate. Off: Wireless link disabled

Table 3-9: SU-I SNR Bar LED Functionality

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

3.5.4 Verifying the Ethernet Connection (Modular Base station)

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

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

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

3.5.6 Verifying Data Connectivity

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

4

Chapter 4 - Operation and Administration

In This Chapter:

4.1 Working with the Monitor Program

4.1.1 Accessing the Monitor Program Using Telnet

1 Connect a PC to the Ethernet port, using a crossed cable.

2 Configure the PC's IP parameters to enable connectivity with the unit. The default IP address is 10.0.0.1.

3 Run the Telnet program. The *Select Access Level* menu is displayed.

4 Select the required access level, depending on your specific access rights. A password entry request is displayed. Table 4-1 lists the default passwords for each of the access levels.

Table 4-1: Default Passwords

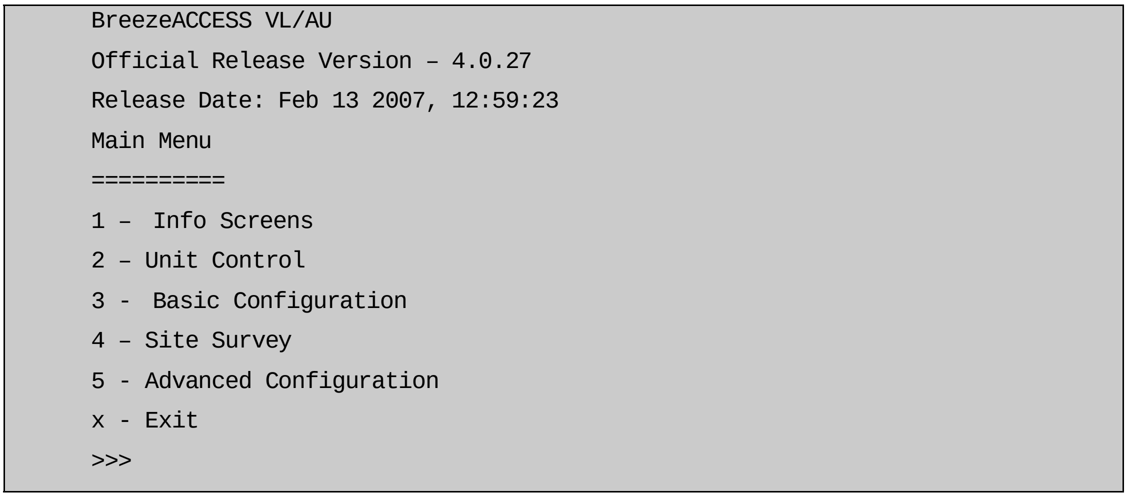
Access Rights	Password
Read-Only	public
Installer	user
Administrator	private

NOTE

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

If you forgot the password, type "h" at the Access Level selection prompt. Type “Recover” at the prompt to get a challenge string consisting of 8 characters. Contact Alvarion's Customer Service and give them the challenge string (after user identification) to receive a one-time password. Aftering entering this password at the prompt, the unit will reboot with the default Administrator password (private). Three consecutive errors in entering the one-time password will invalidate it and block the monitor program. A new challenge string should be used to receive a new one-time password.

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



```
BreezeACCESS VL/AU
Official Release Version – 4.0.27
Release Date: Feb 13 2007, 12:59:23
Main Menu
==========
1 –  Info Screens
2 – Unit Control
3 -  Basic Configuration
4 – Site Survey
5 - Advanced Configuration
x - Exit
>>>
```

Figure 4-1: Main Menu (Administrator Level)

NOTE

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

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

- For users with read only access rights, only the *Info Screens* option is displayed. Users with this access level are not able to access the *Unit Control, Basic Configuration, Site Survey* and *Advanced Configuration* menus.

- For users with Installer access rights, the first four menu items, *Info Screens, Unit Control, Basic Configuration* and *Site Survey*, are displayed. Users with this access level are not able to access the *Advanced Configuration* menu.

- For users with Administrator access rights, the full *Main Menu* is displayed. These users can access all menu items.

4.1.2 Common Operations

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

- Type an option number to open or activate the option. In certain cases you may need to click **Enter**.

- Click Esc to exit a menu or option.

NOTE

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

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

4.2 Menus and Parameters

The following sections describe the menus and parameters provided by the Monitor program.

4.2.1 Main Menu

The *Main Menu* enables to access the following menus, depending on your access level, as described in section 4.1.

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

4.2.2 Info Screens Menu

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

The Info Screens menu includes the following options:

- Show Unit Status
- Show Basic Configuration

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

4.2.2.1 Show Unit Status

The Show Unit Status menu is a read only menu that displays the current values of the following parameters:

- **Unit Name:** As defined in the Unit Control menu.
- **Unit Type:** Identifies the unit's function: AU-BS, AU-SA, AUS-BS, AUS-SA, SU-3-1D, SU-6-1D, SU-6-BD, SU-54-BD, SU-I.
- **Unit MAC Address:** The unit's unique IEEE MAC address.
- **Current Number of Associations (AU only):** The total number of SUs associated with this AU. This number may include units that are not currently active as there is no aging algorithm for associated SUs.

NOTE

An SU is only removed from the list of associated SUs under the following conditions:

- A SNAP frame is received from another AU indicating that the SU is now associated with the other AU.
- The SU failed to respond to a certain number of consecutive frames transmitted by the AU and is considered to have "aged out".

- **Number of Associations Since Last Reset:** For SUs - displays the total number of associations with any AU since the last reset, including duplicate associations with the same AU. For AUs - displays the number of SUs that have associated with the AU since the last reset, including duplicate associations with the same SU.
- **Unit Status (SU only):** The current status of the SU. There are two status options:
  - **SCANNING:** The SU is searching for an AU with which to associate. If the DFS Option is enabled and the SU is currently looking for its previous AU, the AU’s MAC Address will be displayed.
  - **ASSOCIATED:** The SU is associated with an AU.

- **AU MAC Address (SU only):** The MAC address of the AU with which the unit is currently associated. If the unit is not associated with any AU, the address defaults to the IEEE broadcast address, which is FF-FF-FF-FF-FF-FF.

- **Unit Hardware Version:** The version of the outdoor unit hardware.

- **Unit BOOT Version:** The version of the BOOT SW.

- **Time Since Last Reset**

- **Flash Versions:**

  - **Running from:** Shows whether the unit is running from the Main or from the Shadow Version.

  - **Main Version File Name:** The name of the compressed file (with a ".bz" extension) of the version currently defined as the main version.

  - **Main Version Number:** The software version currently defined as the main version.

  - **Shadow Version File Name:** The name of the compressed file (with a ".bz" extension) of the version currently defined as the shadow (backup) version.

  - **Shadow Version Number:** The software version currently defined as the shadow (backup) version.

- **Radio Band:** The radio band of the unit.

- **Log Out Timer:** The value of the Log Out Timer as defined in the Unit Control menu.

- **Ethernet Port Negotiation Mode**: The Ethernet port negotiation mode as defined in the Unit Control menu.

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

- **FTP Parameters**: General FTP parameters (common to SW Version Download, Configuration File Upload/Download and Event File Upload using FTP):
    - FTP Server IP Address
    - FTP Gateway IP Address
    - FTP User Name
    - FTP Password
- **FTP Software Download Parameters:** The parameters for SW download using FTP, as defined in Unit Control menu.
    - FTP Source Directory
    - FTP SW Version File Name
- **Configuration File Download/Upload Parameters:** The parameters for Configuration file upload/download using FTP, as defined in the Unit Control menu.
    - Configuration File Name
    - Configuration File Source Directory
    - Operator Defaults File Name
- **FTP Log File Upload Parameters:** The parameters for Event Log file upload using FTP, as defined in the Unit Control menu.
    - FTP Log File Name
    - FTP Log File Destination Directory
- **Event Log Policy**

4.2.2.2 Show Basic Configuration

The Show Basic Configuration menu is a read only menu that displays the current values of the parameters included in the Basic Configuration menu.

4.2.2.3 Show Advanced Configuration

The Show Advanced Configuration menu enables to access the read only sub menus that display the current values of the parameters included in the applicable sub menus of the Advanced Configuration menu.

4.2.2.4 Show Country Dependent Parameters

Each country has its radio regulation regarding transmissions in the applicable bands that affect parameters such as available frequencies, bandwidth, transmit power, etc. Some other parameters and options may also vary among countries. For each country, one or more sets of parameters are pre-configured in the factory. If more than one set is available, the set to be used can be selected. The Show Country Dependent Parameters displays the available set(s) of these parameters, and includes the following:

- **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).

- **Data Encryption Support**: Indicates whether data encryption is supported for the applicable country.

- **AES Encryption Support**: Indicates whether encryption using AES is supported for the applicable country.

- **Authentication Encryption Support**: Indicates whether authentication encryption is supported for the applicable country.

For each of the available sets (Sub-Bands), the following information is provided:

- **Sub-Band ID and Frequencies**

- **Allowed Bandwidth:** If more than one bandwidth is allowed, then each bandwidth is associated with a different sub-band, as the bandwidth may affect the available frequencies.

- **Regulation Max Tx Power at Antenna Port:** The maximum transmit power allowed at the antenna port of the unit.

- **Regulation Max EIRP:** The maximum allowed EIRP (Effective Isotropic Radiated Power) in dBm, or No Limit.

- **Min Modulation Level:** The lowest allowed modulation level.

- **Max Modulation Level:** The highest allowed modulation level.

- **Burst Mode**: Indicates whether Burst Mode operation is allowed.

- **Maximum Burst Duration**: If Burst Mode is allowed, this parameter displays the upper limit for the Maximum Burst Duration.

- **DFS Option**: Indicates whether the DFS (Dynamic Frequency Selection) mechanism for identification and avoidance of channels with radar activity is supported.

- **Minimum HW Revision Support**: The minimum HW revision required to support the Sub-Band.

New Country Code files can be uploaded remotely using TFTP (see Appendix B).

4.2.2.5 Show All Parameters

The Show All Parameters menu is a read only menu that displays the current values of all status and configuration parameters.

NOTE

The values of some security related parameters, including the encryption Keys, ESSID and Operator ESSID, are available only with Administrator access rights.

4.2.3 Unit Control Menu

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

- Reset Unit

- Default Settings

- Change Unit Name

- Change Password

- Flash Memory Control

- SW Version Download

- Configuration File Upload/Download

- Log Out Timer

- Ethernet Port Negotiation Mode
- Change System Location
- Event Log Menu
- Feature Upgrade

4.2.3.1 Reset Unit

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

4.2.3.2 Default Settings

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

The Default Setting options are available only to users with Administrator access rights.

The available options are:

- Set Defaults
- Save Current Configuration As Operator Defaults

4.2.3.2.1 Set Defaults

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

A Factory Defaults: This is the standard default configuration.

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

The current configuration file and the Operator Defaults configuration file can be uploaded/downloaded by the unit using FTP. For more information, see section 4.2.3.7 option. These files can also be uploaded/downloaded remotely using TFTP (see Appendix B).

The available options in the Set Defaults submenu are:

- Set Complete Factory Defaults

- Set Partial Factory Defaults
- Set Complete Operator Defaults
- Set Partial Operator Defaults
- Cancel Current Pending Request

4.2.3.2.1.1 Set Complete Factory Defaults

Select this option to reset the unit to the standard Factory Defaults configuration, excluding several parameters that are listed in Table 4-2.

Table 4-2: Parameters not reset after Set Complete Factory/Operator Defaults

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

NOTE

The FTP parameters are not set to their default values after Set Complete Operator Defaults. However, they are set to their default value after Set Complete Factory Defaults. Note that in this case they are set to the default values immediately upon selecting the Set Complete Factory Default option (even before the next reset).

4.2.3.2.1.2 Set Partial Factory Defaults

Select this option to reset the unit to the standard Factory Default configuration, excluding the parameters that are required to maintain connectivity and management access. The parameters that do not change after Set Partial Factory Defaults are listed in Table 4-3.

Table 4-3: Parameters that are not reset after Set Partial Factory/Operator Defaults

Parameters Group	Parameter
Unit Control parameters	Passwords
	Ethernet Port Negotiation Mode
	FTP Server IP address
	FTP Gateway IP Address
	FTP User Name
	FTP Password
IP Parameters	IP Address
	Subnet Mask
	Default Gateway Address
	DHCP Option
	Access to DHCP
Security Parameters	Authentication Algorithm
	Default Key (SU)
	Data Encryption Mode
	Default Multicast Key (AU)
	Security Mode
	Key # 1 to Key # 4

Table 4-3: Parameters that are not reset after Set Partial Factory/Operator Defaults

Parameters Group	Parameter
Air Interface Parameters	ESSID
	Operator ESSID Option (AU)
	Operator ESSID (AU)
	Cell Distance Mode (AU)
	Maximum Cell Distance (AU)
	Per SU Distance Learning Option (AU)
	Selected Sub-Band (AU)
	Frequency (AU)
	DFS Option (AU)
	SU Waiting Option (AU)
	Channel Reuse Option (AU)
	Radar Activity Assessment Period (AU)
	Maximum Number of Detections in Assessment Period (AU)
	Frequency Subset (AU)
	ATPC Option (AU)
	Transmit Power
	Maximum Tx Power (SU)
	Tx Control (AU)
	Best AU Support (SU)
	Preferred AU MAC Address (SU)
	All Noise Immunity Control parameters
Network Management Parameters	AP Client IP Address (SU)
Performance Parameters	Adaptive Modulation Decision Thresholds

Table 4-3: Parameters that are not reset after Set Partial Factory/Operator Defaults

Parameters Group	Parameter
Bridge Parameters	VLAN ID – Management
	Service Provider VLAN ID (SU)
	VLAN QinQ Protocol Ethertype
	MAC Address List (AU)
	MAC Address List Action (AU)
Service Parameters	DRAP Option (AU)
	UDP Port (AU)
	Max Number of Voice Calls (AU)
	DRAP TTL (AU)
	Wireless Link Prioritization Option (AU)
	Low Priority AIFS (AU)
	Number of HW Retries for High Priority Traffic (AU)
	Number of HW Retries for Low Priority Traffic (AU)
	AU Burst Duration for High Priority Traffic (AU)
	AU Burst Duration for Low Priority Traffic (AU)
	SU Burst Duration for High Priority Traffic (AU)
	SU Burst Duration for Low Priority Traffic (AU)
	Low Priority Traffic Minimum Percent

4.2.3.2.1.3 Set Complete Operators Defaults

Select this option to reset the unit to the Operator Defaults configuration, excluding several parameters that are listed in Table 4-2.

4.2.3.2.1.4 Set Partial Operator Defaults

Select this option to reset the unit to the Operator Defaults configuration, excluding the parameters that are required to maintain connectivity and management access. The parameters that do not change after Set Partial Operator Defaults are listed in Table 4-3.

4.2.3.2.1.5 Cancel Current Pending Request

After selecting one of the Set defaults options, it will be executed after the next reset. This option enables to cancel the pending request before execution (provided the unit has not been reset yet).

4.2.3.2.2 Save Current Configuration As Operator Defaults

The Save Current Configuration As Operator Defaults enables defining the current configuration of the unit as the Operator Defaults configuration.

4.2.3.3 Change Unit Name

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

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

The default unit name is an empty string.

4.2.3.4 Change Password

The Change Password submenu enables changing the access password(s). The Change Password submenu is available only to users with Administrator access rights.

Valid values: A string of up to 8 printable ASCII characters.

Refer to section 4.1 for a list of the default passwords for each of the access levels.

4.2.3.5 Flash Memory Control

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

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

The parameters configured in the unit are not changed as a result of loading new software versions unless the new version includes additional parameters or additional changes in the list of parameters. New parameters are loaded with their default values.

Select from the following options:

- **Reset and Boot from Shadow Version:** Activates the shadow (backup) software version. The unit is reset automatically. Following the next reset the unit will switch to the main version.

- **Use Running Version After Reset:** Defines the current running version as the new main version. This version will also be used following the next reset.

4.2.3.6 SW Version Download

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

- **Execute FTP GET SW Version:** The Execute FTP GET SW Version option executes the SW Version FTP download according to the parameters defined below.

- **FTP SW Source Dir:** The FTP SW Source Dir option enables defining the source directory of the SW version file.

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

  The default is an empty string.

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

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

  The default is VxWorks.bz.

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

  The default is: 10.0.0.253.

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

  The default is: 0.0.0.0.

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

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

The default is: vx

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

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

  The default is: vx

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

NOTE

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

4.2.3.7 Configuration File Upload/Download

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

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

  - ◇ Execute FTP Get Configuration File (cfg)
  - ◇ Execute FTP Put Configuration File (cfg)
  - ◇ Execute FTP Get Operator Defaults File (cmr)
  - ◇ Execute FTP Put Operator Defaults File (cmr)

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

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

The default is an empty string.

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

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

  The default is config.cfg.

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

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

  The default is operator.cmr.

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

  The default is: 10.0.0.253

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

  The default is: 0.0.0.0.

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

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

  The default is: vx

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

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

  The default is: vx

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

NOTE

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

4.2.3.8 Log Out Timer

The Log Out Timer parameter determines the amount of inactive time following which the unit automatically exits the Monitor program.

The time out duration can range from 1 to 999 minutes.

The default value is 5 minutes.

4.2.3.9 Ethernet Port Negotiation Mode

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

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

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

4.2.3.10 Change System Location

The Change System Location option enables changing the system location of the unit, which is also the sys location in MIB2. The System Location is also displayed as a part of the Monitor menu's header.

Valid values: A string of up to 35 printable ASCII characters.

The default system location is an empty string.

4.2.3.11 Event Log Menu

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

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

The Event Log Menu includes the following options:

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

4.2.3.11.1 Event Log Policy

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

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

The default selection is Warning Level severity.

4.2.3.11.2 Display Event Log

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

4.2.3.11.3 Erase Event Log

The Erase Event Log option enables clearing the event log.

4.2.3.11.4 Event Log Upload

The Event Log Upload submenu enables the optional uploading of the event log file to a remote FTP server. The Event Log Upload submenu includes the following options:

- **FTP Event Log Upload Execute:** The FTP event Log Upload Execute executes the upload of the Event Log file according to the parameters defined below.

- **Event Log Destination Directory:** The Event Log Destination Directory enables defining the destination directory for the Event Log File.

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

  The default is an empty string.

- **Event Log File Name:** The Event Log File Name option enables defining the name of the event log file to be uploaded.

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

  The default is logfile.log.

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

  The default is: 10.0.0.253

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

  The default is: 0.0.0.0.

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

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

  The default is: vx

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

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

  The default is: vx

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

NOTE

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

4.2.3.12 Feature Upgrade

The Feature Upgrade option enables to enter a license string for upgrading the unit to support new features and/or options. Upon selecting the Manual Feature Upgrade option the user will be requested to enter the license string. Each license string is associated with a unique MAC Address and one feature/option. If the encrypted MAC Address in the license string does not match the unit's MAC Address, the string will be rejected. If there is a match, a message notifying of the new feature/option will be displayed. The unit must be reset for the change to take effect.

The license string should comprise 32 to 64 hexadecimal digits.

New Feature License files can be uploaded remotely using TFTP (see Appendix B).

4.2.4 Basic Configuration Menu

The Basic Configuration menu includes all parameters required for the initial installation and operation of the unit. After the unit is properly installed and operational, additional parameters can be configured either locally or remotely using Telnet or SNMP management.

NOTE

All parameters in the Basic Configuration menu are also available in the relevant sub menus of the Advanced Configuration menu.

The Basic Configuration menu enables to access the following parameter sets:

4.2.4.1.1 IP Parameters

- IP Address
- Subnet Mask
- Default Gateway Address
- DHCP Client

  - DHCP Option
  - Access to DHCP

Refer to section 4.2.6.1 for a description of these parameters.

4.2.4.1.2 Air Interface Parameters

- ESSID
- Operator ESSID Parameters (AU)
  - Operator ESSID Option
  - Operator ESSID
- Frequency Definition
  - Select Sub-Band (AU, if more than one is available)
  - Frequency (AU)
  - User Defined Frequency Subsets (SU)
- Best AU Parameters (SU)
  - Best AU Support
  - Preferred AU MAC Address
- Cell Distance Parameters (AU)
  - Cell Distance Mode
  - Maximum Cell Distance
  - Fairness Factor
  - Per SU Distance Learning
- ATPC Parameters
  - ATPC Option
- Transmit Power

- Maximum Tx Power (SU)
- Tx Control (AU)
- Antenna Gain

Refer to section 4.2.6.2 for a description of these parameters.

4.2.4.1.3 Performance Parameters

- Maximum Modulation Level (SU)

Refer to section 4.2.6.5 for a description of these parameters.

4.2.4.1.4 Bridge Parameters

- VLAN Support
  - ◇ VLAN ID – Management

Refer to section 4.2.6.4 for a description of these parameters.

4.2.4.1.5 Security Parameters

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

Some or all of the security parameters may not be available in units that do not support the applicable features. Refer to section 4.2.6.7 for a description of these parameters.

4.2.5 Site Survey Menu

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

The Site Survey menu includes the following options:

- Traffic Statistics
- Ping Test
- Continuous Link Quality display (SU only)
- MAC Address Database
- Per Modulation Level Counters
- Link Capability

4.2.5.1 Traffic Statistics

The traffic statistics are used to monitor, interpret and analyze the performance of the wired and wireless links. The counters display statistics relating to wireless link and Ethernet frames. The Traffic Statistics menu includes the following options:

- **Display Counters:** Select this option to display the current value of the Ethernet and wireless link (WLAN) counters.
- **Reset Counters:** Select this option to reset the counters.

4.2.5.1.1 Ethernet Counters

The unit receives Ethernet frames from its Ethernet port and forwards the frames to its internal bridge, which determines whether each frame should be transmitted to the wireless medium. Frames discarded by the unit's hardware filter are not counted by the Ethernet counters. For units with HW revision B and lower, the maximum length of a regular IEEE 802.1 Ethernet packet that can be accepted from or transmitted to the Ethernet port is 1514 bytes, excluding CRC and VLAN(s). For units with HW revision C and higher, the maximum length of an Ethernet packet that can be accepted from or transmitted to the Ethernet port (excluding CRC) is 1600 bytes, including VLAN(s) for single or double-tagged packets.

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

The Ethernet Counters include the following statistics:

- **Total received frames via Ethernet:** The total number of frames received from the Ethernet port. This counter includes both invalid frames (with errors) and valid frames (without errors).

- **Transmitted wireless to Ethernet:** The number of frames transmitted by the unit to the Ethernet port. These are generally frames received from the wireless side, but also include frames generated by the unit itself.

4.2.5.1.2 WLAN Counters

The unit submits data frames received from the Ethernet port to the internal bridge, as well as self generated control and wireless management frames. After a unicast data frame is transmitted, the unit waits for an acknowledgement (ACK) message from the receiving unit. Some control and wireless management frames, as well as broadcast and multicast frames sent to more than one unit, are not acknowledged. If an ACK is not received after a predefined time, which is determined by the **Maximum Cell distance** parameter, the unit retransmits the frame until an ACK is received. If an ACK is not received before the number of retransmissions has reached a maximum predefined number, which is determined by the **Number of HW Retries** parameter, the frame is dropped.

Each packet to be transmitted to the wireless link is transferred to one of three queues: Low, Medium and High. Packets in the High queue have the highest priority for transmission, and those in the Low queue have the lowest priority. The packets in the High queue will be transmitted first. When this queue is emptied, the packets in the Medium queue will be sent. Finally, when both the High and Medium queues are empty, the packets in the Low queue will be sent.

Data packets are routed to either the High or Low queue, according to the queue selected for them before the MIR/CIR mechanism (for more information see section 4.2.6.6.3).

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

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

Any frame coming from the Ethernet port, which is meant to reach another BreezeACCESS VL unit via the wireless port (as opposed to messages intended for stations behind other BreezeACCESS VL units), is sent to the High queue, regardless of the priority configuration.

The Wireless Link Counters include the following statistics:

- **Total transmitted frames to wireless:** The number of frames transmitted to the wireless medium. The total includes one count for each successfully transmitted unicast frame (excluding retransmissions), and the number of transmitted multicast and broadcast frames, including control and wireless management frames. In the AU, there are also separate counters for the following:
  - ◇ Beacons (AU only)
  - ◇ Management and Other Data frames, including successfully transmitted unicast frames and multicast/broadcast data frames (excluding retransmissions, excluding Beacons in AU)
- **Total Transmitted Unicasts** (AU only): The number of unicast frames successfully transmitted to the wireless medium, excluding retransmissions. This count is useful for calculating the rates of retransmissions or dropped frames, as only unicast frames are retransmitted if not acknowledged.
- **Total submitted frames (bridge):** The total number of data frames submitted to the internal bridge for transmission to the wireless medium. The count does not include control and wireless management frames, or retransmissions. There are also separate counts for each priority queue through which the frames were routed (High, Mid and Low).
- **Frames dropped (too many retries):** The number of dropped frames, which are unsuccessfully retransmitted without being acknowledged until the maximum permitted number of retransmissions. This count includes dropped data frames as well as dropped control and wireless management frames.
- **Total retransmitted frames:** The total number of retransmissions, including all unsuccessful transmissions and retransmissions.
- **Total transmitted concatenated frames:** The total number of concatenated frames transmitted successfully to the wireless medium, excluding retransmissions. There are also separate counts for concatenated frames that include one frame (Single), two frames (Double) or more than two frames (More). For more details refer to section 4.2.6.5.10.
- **Total Tx events:** The total number of transmit events. Typically, transmission events include cases where transmission of a frame was delayed or was aborted before completion. The following additional counters are displayed to indicate the reason for and the nature of the event:

  - ◇ Dropped: The number of dropped frames, which are unsuccessfully retransmitted without being acknowledged until the maximum permitted number of retransmissions.

  - ◇ Underrun: The number of times that transmission of a frame was aborted because the rate of submitting frames for transmission exceeds the available transmission capability.

  - ◇ Others: The number of frames whose transmission was not completed or delayed due to a problem other than those represented by the other counters.

- **Total received frames from wireless:** The total number of frames received from the wireless medium. The count includes data frames as well as control and wireless management frames. The count does not include bad frames and duplicate frames. For a description of these frames, refer to Bad frames received and Duplicate frames discarded below.

- **Total received data frames:** The total number of data frames received from the wireless medium, including duplicate frames. Refer to Duplicate frames discarded below.

- **Total Rx events:** The total number of frames that were not received properly. The following additional counters are displayed to indicate the reason for the failure:

  - ◇ Phy: The number of Phy errors (unidentified signals).

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

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

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

- **Total received concatenated frames:** The total number of concatenated frames received from the wireless medium, including duplicate frames. There are also separate counts for concatenated frames that include one frame (Single), two frames (Double) or more than two frames (More). For more details refer to section 4.2.6.5.10.

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

- **Duplicate frames discarded:** The number of data frames discarded because multiple copies were received. If an acknowledgement message is not received by the originating unit, the same data frame can be received more than once. Although duplicate frames are included in all counters that include data frames, only the first copy is forwarded to the Ethernet port.

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

4.2.5.2 Ping Test

The *Ping Test* submenu is used to control pinging from the unit and includes the following options:

- **Destination IP Address:** The destination IP address of the device being pinged. The default IP address is 192.0.0.1.

- **Number of Pings to Send:** The number of ping attempts per session. The available range is from 0 to 9999. The default value is **1**. Select 0 for continuous pinging.

- **Ping Frame Length:** The ping packet size. The available range is from 60 to 1472 bytes. The default value is 64 bytes.

- **Ping Frame Timeout:** The ping frame timeout, which is the amount of time (in ms) between ping attempts. The available range is from 100 to 60,000 ms. The default value is 200 ms.

- **Start Sending:** Starts the transmission of ping frames.

- **Stop Sending:** Stops the transmission of ping frames. The test is automatically ended when the number of pings has reached the value specified in the **No. of Pings** parameter, described above. The **Stop Sending** option can be used to end the test before completing the specified number of pings, or if continuous pinging is selected.

- **Show Ping Test Values:** Displays the current values of the ping test parameters, the transmission status, which means whether it is currently sending or not sending pings, the number of pings sent, and the number of pings received, which means the number of acknowledged frames.

4.2.5.3 Link Quality (SU only)

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

4.2.5.3.1 Continuous Average SNR Display

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

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

4.2.5.3.2 Continuous UpLink Quality Indicator Display

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

LQI = (0.9 x ”Previous LQI”) + (0.1 x ”Last Successful Modulation Level”).

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

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

NOTE

If Limited Test is indicated next to the LQI results, it means that the results may not indicate the true quality, as not all modulation levels from 1 to 8 are available. The limitation may be due to the HW of the unit (HW Revision A), or the applicable parameters in the country code, or the configurable Maximum Modulation Level parameter.

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

4.2.5.4 MAC Address Database

4.2.5.4.1 MAC Address Database in AU

The **MAC Address Database** option in the AU displays information regarding the Subscriber Units associated with the AU, as well as bridging (forwarding) information. When DRAP is supported, it enables viewing details on the active Gateways in the sector. The following options are available:

- **Display Bridging and Association Info:** The Display Bridging and Association Info option displays a list of all the Subscriber Units and stations in the AU's Forwarding Database. For stations behind an SU, the SU's MAC address is also displayed (SU Address).

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

  - ◇ **Et (Ethernet):** An address learned from the Ethernet port.

  - ◇ **Vp (Virtual port):** An address of a node behind an associated SU. For these addresses, learned from the wireless port, the address of the applicable SU is also displayed (in parenthesis).

  - ◇ **St (Static):** An associated SU. For these entries, the following details are also displayed: SU Unit Name, SU SW version, SU Unit Type and SU’s Distance from the AU.

  - ◇ **X:** An SU that is included in the Deny List.

  - ◇ **Sp (Special):** 7 addresses that are always present, including:

    - ➢ The MAC address of the AU, which appears twice as it is learned from both the Ethernet and wireless ports.

    - ➢ The MAC address of the internal Operating System stack, which also appears twice.

    - ➢ Alvarion's Multicast address (01-20-D6-00-00-01, which also appears twice. The system treats this address as a Broadcast address.

    - ➢ The Ethernet Broadcast address (FF-FF-FF-FF-FF-FF).

  In addition, a summary table displays information about the Forwarding Database (Bridging Info) and the Associated Subscriber Units Database (Association Info). Each database includes the following information:

  - ◇ The current number of entries. For Bridging Info this includes the **Et** (Ethernet) and the **Vp** (Virtual ports) entries. For Association Info this is the number of the currently associated SUs.

NOTE

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

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

- The SU failed to respond to 50 consecutive frames transmitted by the AU and is considered to have "aged out".

  ◇ The aging time specified for entries in these tables. The aging time for Bridging Info is as specified by the **Bridge Aging Time** parameter. The default is 300 seconds. There is no aging time for Association Info entries.

  ◇ The maximum number of entries permitted for these tables, which are 1017 (1024 minus the number of special Sp addresses as defined above) for Bridging Info and as specified by the **Maximum Number of Associations** parameter for Association Info. The default value of the Maximum Number of Associations parameter is 512.

NOTE

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

- **Display Association Info:** Displays information regarding the Subscriber Units associated with the AU. Each list entry includes the following information:

  ◇ The MAC Address of the associated Subscriber Unit

  ◇ Age in seconds, indicating the elapsed time since receiving the last packet from the Subscriber Unit.

  ◇ The value configured for the Maximum Modulation Level parameter of the Subscriber Unit

  ◇ The Status of the Subscriber Unit. There are three options:

  1 Associated

  2 Authenticated

  3 Not Authenticated (a temporary status)

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

Table 4-4: Authentication and Association Process

Message	Direction	Status in AU

Table 4-4: Authentication and Association Process

Message	Direction	Status in AU
SU Status: Scanning		
A Beacon with correct ESSID	AU → SU	-
SU Status: Synchronized		
Authentication Request	SU → AU	Not authenticated
Authentication Successful	AU → SU	Authenticated
SU Status: Authenticated		
Association Request	SU → AU	Authenticated
Association Successful	AU → SU	Associated
SU Status: Associated		
ACK	SU → AU	Associated
Data Traffic	SU ↔ AU	Associated

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

In addition, a summary table displays information about the Forwarding Database (Bridging Info). The database includes the following information:

- The current number of entries. This is the number of currently associated SUs.

NOTE

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

- A SNAP frame is received from another AU indicating that the SU is now associated with the other AU.
- The SU failed to respond to 50 consecutive frames transmitted by the AU and is considered to

have "aged out".

- ◇ The aging time specified for entries in these table. There is no aging time for Association Info entries.
- ◇ The maximum number of entries permitted for this table, which is specified by the **Maximum Number of Associations** parameter. The default value of the **Maximum Number of Associations** parameter is 512.

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

  Each entry includes the following information:

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

- **Display MAC Pinpoint Table**: The MAC Pinpoint table provides for each of the Ethernet stations (identified by the MAC Address) connected to either the AU or to any of the SUs served by it, the identity (MAC Address) of the wireless device to which they are connected.

- **Gateways Table**: When the DRAP option is supported, the Gateways Table provides details on the active Gateways connected to any of the SUs served by the AU. For each Gateway, the displayed information includes:

  - ◇ Gateway Type (VG-1D1V, VG-1D2V, NG-4D1W)
  - ◇ IP Address
  - ◇ Number of Voice Calls (applicable only to Voice Gateways)

4.2.5.4.2 MAC Address Database in SU

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

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

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

  - **Et (Ethernet):** An address learned from the Ethernet port.

  - **Wl (Wireless):** An address of a node behind the associated AU, learned via the wireless port.

  - **Sp (Special):** 8 addresses that are always present, including:

    - The MAC address of the SU, which appears twice as it is learned from both the Ethernet and wireless ports.

    - The MAC address if the internal Operating System’s stack, which also appears twice.

    - Alvarion's Multicast address (01-20-D6-00-00-01), which also appears twice. The system treats this address as a Broadcast address.

    - Alvarion's special Multicast address (01-20-D6-00-00-05), reserved for future use.

    - The Ethernet Broadcast address (FF-FF-FF-FF-FF-FF).

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

4.2.5.5 Per Modulation Level Counters

The Per Modulation Level Counters display statistics relating to wireless link performance at different radio modulation levels. The Per Modulation Level Counters menu includes the following options:

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

- **Reset Counters:** Select this option to reset the Per Modulation Level Counters.

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

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

- **SUCCESS:** The total number of successfully transmitted unicasts at the applicable modulation level.

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

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

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

4.2.5.6 Link Capability

The Link Capability option provides information on HW and SW capabilities of relevant units. In an AU, the information provided in the Link Capability reports is for all associated SUs. In an SU, the Link Capability reports include information on all AUs in the neighboring AUs table (all AUs with whom the SU can communicate).

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

The Link Capability submenu includes the following options:

4.2.5.6.1 Show Link Capability-General

Select this option to view information on general parameters of relevant units. For each relevant unit, identified by its MAC address, the following details are displayed:

- **HwVer**: the hardware version of the unit.

- **CpldVer**: The version of the Complex Programmable Logic Device (CPLD) used in the unit. This parameter is available only in AUs, displaying the CPLD version in the relevant SU.

- **Country**: The 3 or 4 digits country code supported by the unit.

- **SwVer**: The SW version used by the unit. This parameter is available only in SUs, displaying the SW version in the relevant AU.

- **BootVer**: The Boot Version of the unit. This parameter is available only in AUs, displaying the Boot version in the relevant SU.

4.2.5.6.2 Show Link Capability-Wireless Link Configuration

Select this option to view information on current wireless link parameters of relevant units. For each relevant unit, identified by its MAC address, the following details are displayed:

- **ATPC Option**: Enable or Disable.

- **Adaptive Modulation Option**: Enable or Disable.

- **Burst Mode Option**: Enable or Disable.

- **DFS Option**: Enable or Disable. This parameter is available only in SUs, displaying the current option in the relevant AU.

- **Concatenation Option**: Enable or Disable.

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

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

4.2.5.6.3 Show Link Capability-Security Configuration

Select this option to view information on current security related parameters of relevant units. For each relevant unit, identified by its MAC address, the following details are displayed:

- **Security Mode**: WEP, AES OCB or FIPS 197.

- **Authentication Algorithm**: Shared Key or Open System.

- **Data Encryption Option**: Enable or Disable.

4.2.5.6.4 Show Link Capability by AU (SU only)

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

4.2.5.6.5 Show Link Capability by SU (AU only)

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

4.2.6 Advanced Configuration Menu

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

The Advanced Configuration menu enables accessing the following menus:

- IP Parameters
- Air Interface Parameters
- Network Management Parameters
- Bridge Parameters
- Performance Parameters
- Service Parameters
- Security Parameters

4.2.6.1 IP Parameters

The IP Parameters menu enables defining IP parameters for the selected unit and determining its method of IP parameter acquisition.

The IP Parameters menu includes the following options:

- IP Address
- Subnet Mask
- Default Gateway Address
- DHCP Client

4.2.6.1.1 IP Address

The IP Address parameter defines the IP address of the unit.

The default IP address is 10.0.0.1.

4.2.6.1.2 Subnet Mask

The Subnet Mask parameter defines the subnet mask for the IP address of the unit.

The default mask is 255.0.0.0.

4.2.6.1.3 Default Gateway Address

The Default Gateway Address parameter defines the IP address of the unit's default gateway.

The default value for the default gateway address is 0.0.0.0.

4.2.6.1.4 DHCP Client

The DHCP Client submenu includes parameters that define the method of IP parameters acquisition.

The DHCP Client submenu includes the following options:

- DHCP Option
- Access to DHCP

4.2.6.1.4.1 DHCP Option

The DHCP Option displays the current status of the DHCP support, and allows selecting a new operation mode. Select from the following options:

- Select **Disable** to configure the IP parameters manually. If this option is selected, configure the static IP parameters as described above.
- Select **DHCP Only** to cause the unit to search for and acquire its IP parameters, including the IP address, subnet mask and default gateway, from a DHCP (Dynamic Host Configuration Protocol) server only. If this option is selected, you must select the port(s) through which the unit searches for and communicates with the DHCP server, as described in section 4.2.6.1.4.2. You do not have to configure static IP parameters for the unit. DHCP messages are handled by the units as management frames.
- Select **Automatic** to cause the unit to search for a DHCP server and acquire its IP parameters from the server. If a DCHP server is not located within approximately 40 seconds, the currently configured parameters are used. If this option is selected, you must configure the static IP parameters as described above. In addition, you must select the port(s) through which the unit searches for and communicates with the DHCP server, as described in section 4.2.6.1.4.2.

  The default is Disable.

4.2.6.1.4.2 Access to DHCP

The Access to DHCP option enables defining the port through which the unit searches for and communicates with a DHCP server. Select from the following options:

- From Wireless Link Only
- From Ethernet Only
- From Both Ethernet and Wireless Link

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

4.2.6.1.5 Show IP Parameters

The Show IP Parameters option displays the current values of the IP parameters, including the **Run Time IP Address, Run Time Subnet Mask** and **Run Time Default Gateway Address**.

4.2.6.2 Air Interface Parameters

The Air Interface Parameters menu enables viewing the current Air Interface parameters defined for the unit and configuring new values for each of the relevant parameters.

4.2.6.2.1 Country Code and Sub-Bands

Each country has its own regulations regarding operation modes and parameters such as allowable frequencies and bandwidth, the need to employ an automatic mechanism for detection and avoidance of frequencies used by radar systems, maximum transmit power at each of the supported modulation levels and the ability to use burst transmissions. To efficiently manage these country dependent parameters, each unit has a ‘Country Code’ parameter and a set of accompanying parameters, which depend on this country code. Where more than one set of parameters can be used, the available sets are defined as Sub-Bands, selectable through the Frequency configuration menu.

4.2.6.2.2 ESSID Parameters

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

4.2.6.2.2.1 ESSID

The ESSID parameter defines the ESSID of the unit.

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

The default value is ESSID1.

NOTE

The ESSID string is case sensitive.

4.2.6.2.2.2 Operator ESSID Parameters (AU only)

The Operator ESSID Parameters submenu includes the following parameters:

4.2.6.2.2.2.1 Operator ESSID Option

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

The default is Enable.

4.2.6.2.2.2.2 Operator ESSID

The Operator ESSID parameter defines the Operator ESSID.

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

The default value is ESSID1.

NOTE

The Operator ESSID string is case sensitive.

4.2.6.2.3 Frequency Definition Parameters

4.2.6.2.3.1 Sub-Bands and Frequency Selection

Each unit is delivered with one or more pre-configured Sub-Bands, according to the country code. These sets of parameters include also the frequencies that can be used and the bandwidth.

The parameters that determine the frequency to be used are set in the AU. If more than one Sub-Band is available, the sub-band to be used can be selected. If only one Sub-Band is supported, then the sub-band selection option is not available. The SU should be configured with a minimal set of parameters to ensure that it will be able to automatically detect and use the frequency/bandwidth used by the AU, including possible changes in this frequency (Automatic Sub Band Select feature).

To simplify the installation process the SU scans a definable frequencies subset after power-up. The defined frequencies subsets may include frequencies from more than one Sub-Band, enabling automatic detection of both frequency and bandwidth. If the Best AU feature is enabled, the SU will scan the defined subset and the operating frequency/bandwidth will be determined by the Best AU mechanism (including the optional use of the Preferred AU feature). Otherwise the SU will try to associate with the first AU it finds. If no AU is found, the SU will start another scanning cycle.

4.2.6.2.3.2 Avoiding Frequencies with Radar Activity

In some regions, it is important to ensure that wireless access equipment does not interfere with certain radar systems in the 5 GHz band. If radar is being detected, the wireless access network should move automatically to a frequency that does not interfere with the radar system.

The country dependent set of parameters includes also an indication whether DFS (Dynamic Frequency Selection) should be used. The DFS algorithm is designed to detect and avoid operation in channels with radar activity. If the current sub-band does not support DFS, then the DFS parameters configuration submenu is not available.

When the DFS Option is enabled, the AU monitors the spectrum continuously, searching for signals with a specific pattern indication radar activity. Upon detecting radar activity, the AU immediately stops transmitting on this frequency and starts looking for another radar-free frequency. The subset of viable frequencies is configurable.

The AU maintains a continuously updated database of all applicable frequencies, where each frequency is marked as Radar Free, Radar Detected or Adjacent to Radar. The AU attempts to check a new frequency only if it is marked as Radar Free. If a radar activity was detected on a certain frequency, it will be marked in the database as a Radar Detected frequency. The AU will not attempt to check for radar activity in frequencies marked as Radar Detected. A certain time after detecting radar activity on a frequency, it will be removed from the list of Radar Detected frequencies and will be marked as Radar Free. If radar activity was detected on a certain frequency, adjacent channels should not be used as well, according to the bandwidth. For instance, if the bandwidth is 20 MHz, then if radar activity was detected in 5800 MHz, frequencies 5790 MHz and 5810 MHz should not be used as well. These frequencies are marked in the database as Adjacent to Radar, and will be treated the same as Radar Detected frequencies.

Before ceasing transmission on the frequency where radar signals had been detected, the AU sends a special disassociation message to its associated SUs. This message includes an indication whether the SUs should wait for this AU. If the SUs should wait, the message includes also the waiting time. During this time each SU searches for the AU in the defined frequencies subset. If the AU was not found within the waiting time, or if a waiting request was not included in the message, the SU starts searching for any AU, using the Best AU mechanism if applicable.

Typically, operators prefer to preserve the original frequency planning and to avoid moving to a new channel unless they are sure that there is a continuous radar activity in the original channel. It should be noted that detection of radar activity does not necessarily indicate a continuous radar activity in the channel. A channel reuse algorithm enables returning to the original channel under certain conditions that indicates low radar activity on the channel.

4.2.6.2.4 Frequency Definition Submenu in AU

The Frequency Definition submenu in AU includes the following parameters:

4.2.6.2.4.1 Sub-Band Select

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

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

The default selection is Sub-Band 1.

4.2.6.2.4.2 Frequency

The Frequency parameter defines the transmit/receive frequency when the DFS Option is not enabled. If the DFS Option is enabled, it sets the initial operational frequency upon starting the DFS mechanism for the first time.

The range depends on the selected Sub-Band.

The default is the lowest frequency in the Sub-Band.

CAUTION

a. In units using Country Code 1023 (FCC 5.3 GHz), for full compliance with FCC regulations the Transmit Power parameter in the AU when operating at 5270 MHz with a 20 MHz bandwidth, and the Maximum Tx Power parameter in the SUs connected to this AU, should not be set to a value above “17-Antenna Gain” (The maximum allowed EIRP for 5270 MHz is 17 dBm).

b. In units using Country Code 392 (4.9 GHz Japan, regular - not B&B point-to-point) with a 10 MHz bandwidth, the following rules must be met for full compliance with regulations:

- When operating at 4945 MHz, the Transmit Power parameter in the AU should not be set to a value above 11 dBm. The Maximum Transmit Power of the SU should not be set to a value above 10 dBm.
- When operating at 5055 MHz, the Transmit Power parameter in the AU should not be set to a value above 13 dBm. The Maximum Transmit power of the SU should not be set to a value

above 10 dBm.

This requirement, although not indicated in the certification document, is needed following the tests performed in the certification lab.

4.2.6.2.4.3 DFS Parameters

The DFS Parameters submenu is available only if DFS is supported by the current Sub-Band. The DFS Parameters submenu includes the following parameters:

4.2.6.2.4.3.1 DFS Option

The DFS Option enables or disables the radar detection and dynamic frequency selection mechanism.

The default is Enable.

4.2.6.2.4.3.2 Frequency Subset Definition

The Frequency Subset Definition parameter defines the frequencies that will be used in the DFS mechanism. The available frequencies according to the Sub-Band are displayed, and each of the frequencies in the list is associated with an index. The frequencies subset can be defined by entering the indexes of the required frequencies, or “A” to select all available frequencies.

The default is the complete list of frequencies available in the Sub-Band.

4.2.6.2.4.3.3 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 attempting 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.

The default is 60 seconds.

4.2.6.2.4.3.4 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. When this time has elapsed, the unit frequency’s marking will change to Radar Free.

The range is 1 to 60 minutes.

The default is 30 minutes.

4.2.6.2.4.3.5 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 the 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.

The default is Enable.

4.2.6.2.4.3.6 Minimum Pulses to Detect

The Minimum Pulses to Detect parameter defines the minimum number of radar pulses that should be detected before reaching a decision that radar is active on the channel.

The range is from 1 to 100 pulses.

The default is 6 pulses.

4.2.6.2.4.3.7 Clear Radar Detected Channels After Reset

When the Clear Radar Detected Channels After Reset is enabled, 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.

The default is Disable.

4.2.6.2.4.4 Channel Reuse Parameters (DFS+)

The Channel Reuse algorithm enables returning to the original channel under certain conditions that indicate low radar activity on the original channel. The conditions are that radar was detected in this channel not more than N times (Maximum Number of Detections in Assessment Period) during the last T hours (Radar Activity Assessment Period). When the Channel Reuse Option is enabled, then by the end of the Channel Avoidance Period the unit will attempt returning to the original frequency, provided these conditions are met.

The Channel Reuse Parameters submenu includes the following options:

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

  The default is Disable.

- **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.

  The default is 5 hours.

- **Maximum Number of Detections in Assessment Period**: The maximum number of radar detections 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.

  The default is 5 radar detections.

4.2.6.2.4.4.1 Show DFS Settings And Data

Upon selecting the Show DFS Settings and Data, the values of all DFS parameters and the current operating frequency will be displayed. The current defined frequency subset as well as the defined subset (to be used after the next reset) are also displayed. In addition, all the applicable frequencies will be displayed together with their status in the database (Radar Free, Radar Detected or Adjacent to Radar).

4.2.6.2.4.5 Country Code Learning by SU

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

The AU advertises its country code in every beacon and association response message. Upon synchronization the SU will check if its country code and the country code received from the AU are the same. If they are not the same and the Country Code Learning by SU is enabled, the SU will use the AU’s country code: the country code derived limitations will be forced and the following parameters will be set according to new country definitions:

- Maximum TX Power will be set to the maximum defined by the country code.

- TX Power will be set to the maximum defined by the country code.

- The Modulation Level will be set to the maximum modulation level defined by the country code.

- The Multicast Modulation Level will be set to the minimum modulation level defined by the country code.

- The Burst Mode will be set to enable if the country code supports burst mode, and the burst duration will be set to default.

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

The default is Enable.

NOTE

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

4.2.6.2.4.6 Show Frequency definitions

Upon selecting Show Frequency Definitions, the selected Sub-Band and Frequency are displayed. In addition, all the parameters displayed upon selecting Show DFS Settings and Data are also displayed.

4.2.6.2.5 Frequency Definition Submenu in SU

4.2.6.2.5.1 User Defined Frequency Subsets

The User Defined Frequency Subsets menu 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, and an index is associated with each frequency. Enter either the desired frequency indexes, ‘A’ (All) for using all frequencies in the subset or ‘N’ (None) for not scanning that sub-band.

The default is all frequencies in all available sub-bands.

4.2.6.2.5.2 Show Frequency Definitions

Upon selecting the Show Frequency Definitions, the selected frequencies in the available Sub-Bands and the current operating frequency are displayed.

4.2.6.2.6 Best AU Parameters (SU)

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

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

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

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

NOTE

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

The Best AU Parameters menu includes the following options:

4.2.6.2.6.1 Best AU Support

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

The default is Disable.

NOTE

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

4.2.6.2.6.2 Number Of Scanning Attempts

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

Valid values: 1 - 255.

Default value: 4.

4.2.6.2.6.3 Preferred AU MAC Address

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

Valid values: A MAC address string.

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

4.2.6.2.6.4 Show Best AU Parameters and Data

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

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

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

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

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

4.2.6.2.7 Scanning Mode (SU only)

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

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

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

When DFS Option is enabled, Scanning Mode is forced to Passive.

The default selection is Passive.

4.2.6.2.8 Power Control Parameters

The Automatic Transmit Power Control (ATPC) algorithm simplifies the installation process and ensures optimal performance while minimizing interference to other units. This is achieved by automatically adjusting the power level transmitted by each SU according to the actual level at which it is received by the AU. To support proper operation of the system with optimal performance and minimum interference between neighboring sectors, the ATPC algorithm should be enabled in all units.

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

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

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

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

Different power levels may be used for different modulation levels by taking into account possible HW limitations or regulatory restrictions.

4.2.6.2.8.1 Transmit Power

The Transmit Power submenu includes the following options:

- Transmit Power
- Show Transmit Power Parameters

4.2.6.2.8.1.1 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.
- The Maximum EIRP as defined for the applicable Sub-Band, together with the value of the Antenna Gain. In certain countries the Maximum EIRP of some equipment types cannot exceed a certain value. In these cases the Transmit Power cannot exceed the value of (Maximum EIRP – Antenna Gain).
- Maximum Tx Power parameter (in SU only)

For information on how to view the Sub-Bands supported by the unit and the supported parameters' values and options, refer to section 4.2.2.4.

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

For each modulation level, the unit will use as transmit power the minimum between this parameter and the maximum Tx power allowed by the HW and the Country Code for the specific modulation level.

The default Transmit Power is the highest allowed value.

4.2.6.2.8.1.2 Show Transmit Power Parameters

This option displays the Transmit Power parameter and the current transmit power for the different modulation levels.

4.2.6.2.8.2 Maximum Transmit Power (SU only)

The Maximum Transmit Power submenu includes the following options:

- Maximum Tx Power
- Show Maximum Tx Power Parameters

4.2.6.2.8.2.1 Maximum Tx Power

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.
- The Maximum EIRP as defined for the applicable Sub-Band, together with the value of the Antenna Gain. In certain countries the Maximum EIRP of some equipment types cannot exceed a certain value. In these cases the Transmit Power cannot exceed the value of (Maximum EIRP – Antenna Gain).

For information on how to view the Sub-Bands supported by the unit and the supported parameters’ values and options, refer to section 4.2.2.4.

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

For each modulation level, the unit will use as maximum transmit power the minimum between this parameter and the maximum Tx power allowed by the HW and the Country Code for the specific modulation level.

The default Maximum Tx Power is the highest allowed value.

4.2.6.2.8.2.2 Show Maximum Tx Power Parameters

This option displays the Maximum Tx Power parameter and the current maximum Tx power for the different modulation levels.

4.2.6.2.8.3 ATPC Parameters in AU

4.2.6.2.8.3.1 ATPC Option

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

The default is Enable.

4.2.6.2.8.3.2 ATPC Minimum SNR Level

The Minimum SNR Level defines the lowest SNR at which you want each SU to be received at the AU (the lower limit of the optimal reception level range).

Available values: 4 to 60 (dB).

Default value: 28 (dB).

4.2.6.2.8.3.3 ATPC Delta from Minimum SNR Level

The Delta from Minimum SNR Level is used to define the highest SNR at which you want each SU to be received at the AU (the higher limit of the optimal reception level range):

Max. Level=Minimum SNR Level + Delta from Minimum SNR Level.

Available values: 4 to 20 (dB).

Default value: 5 (dB) for units operating in the 5.4 and 5.8 GHz bands. 8 (dB) for units operating in the 4.9, 5.2 and 5.3 GHz bands.

4.2.6.2.8.3.4 Minimum Interval Between ATPC Messages

The Minimum Interval Between ATPC Messages parameter sets the minimal time between consecutive power-up/power-down messages to a specific SU. Setting a low value for this parameter may lead to higher overhead and to an excessive rate of power level changes at the SUs. High values for this parameter increase the time it will take the SUs to reach optimal transmit power level.

Available values: 1 to 3600 seconds.

Default value: 30 seconds.

4.2.6.2.8.3.5 ATPC Power Level Step

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

Valid range: 1-20 (dB)

Default value: 5 (dB)

4.2.6.2.8.4 ATPC Parameters in SU

4.2.6.2.8.4.1 ATPC Option

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

The default is Enable.

NOTE

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

4.2.6.2.8.5 Tx Control (AU only)

The Tx Control option enables turning Off/On the AU’s transmitter, or having the AU 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 transmitter will be switched to Off
- If the Ethernet link is up, the AU transmitter will be switched to On.

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

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

The default is On.

4.2.6.2.9 Antenna Gain

The Antenna Gain parameter enables to define the net gain of a detached antenna. The configured gain should take into account the attenuation of the cable connecting the antenna to the unit. The Antenna Gain is important especially in countries where there is a limit on the EIRP allowed for the unit; the maximum allowed value for the Transmit Power parameters cannot exceed the value of (EIRP - Antenna Gain), where the EIRP is defined in the selected Sub-Band.

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

The range is 0 – 50 (dB). A value of “Don’t Care” means that the actual value is not important. A value of “Not Set Yet” means that the unit will not transmit until the actual value (in the range 0 to 50) is configured. The unit can be configured to “Don’t Care” or “Not Set Yet” only in factory (when upgraded to SW version 2.0 from a lower version it will be set automatically to one of these options). Once a value is configured, it is not possible to reconfigure the unit to either “Don’t Care” or “Not Set Yet”.

The default value depends on unit type. In SUs with integral antenna it is set to 21 (read only). The default value for AUs that are supplied with a detached antenna is in accordance with the antenna’s gain. In units supplied without an antenna the default is typically “Not Set Yet”.

4.2.6.2.10 Cell Distance Parameters (AU only)

The higher the distance of an SU from the AU that is serving it, the higher the time it takes for messages sent by one of them to reach the other. To ensure appropriate services to all SUs regardless of their distance from the AU while maintaining a high overall performance level, two parameters should be adapted to the distances of SUs from the serving AU:

- The time that a unit waits for a response message before retransmission (ACK timeout) should take into account the round trip propagation delay between the AU and the SU (The one-way propagation delay at 5 GHz is 3.3 microseconds per km/5 microseconds per mile.). The higher the distance from the AU of the SU served by it, the higher the ACK timeout should be.
  The ACK timeout in microseconds is: 20+Distance (km)*2*3.3 or 20+Distance (miles)*2*5.

- To ensure fairness in the contention back-off algorithm between SUs located at different distances from the AU, the size of the time slot should also take into account the one-way propagation delay. The size of the time slot of all units in the cell should be proportional to the distance from the AU of the farthest SU served by it.

The Cell Distance Mode parameter in the AU defines the method of computing distances. When set to Manual, the Maximum Cell Distance parameter should be configured with the estimated distance of the farthest SU served by the AU. When set to Automatic, the AU uses a special algorithm to estimate its distance from each of the SUs it serves, determine which SU is located the farthest and use the estimated distance of the farthest SU as the maximum cell distance. The value of the maximum cell distance parameter (either computed or configured manually) is transmitted in the beacon messages to all SUs served by the AU, and is used by all units to calculate the size of the time slot, that must be the same for all units in the same sector. When the Per SU Distance Learning option is enabled, the AU uses the re-association message to send to each SU its estimated distance from the AU. The per-SU distance is used to calculate the ACK timeout to be used by the SU. When the Per SU Distance Learning option is disabled (or if it cannot be used because the SU uses a previous SW version that does not support this feature), the SU will use the maximum cell distance to calculate the ACK timeout. The AU always uses the maximum cell distance to calculate the ACK timeout.

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

The Cell Distance Parameters menu includes the following parameters:

4.2.6.2.10.1 Cell Distance Mode

The Cell Distance Mode option defines whether the maximum distance of the AU from any of the SUs it serves will be determined manually (using the Maximum Cell Distance parameter) or automatically. In addition, the Per SU Distance Learning feature is supported only when the Cell Distance Mode is set to Automatic.

The Options are Automatic or Manual.

The default is Automatic.

4.2.6.2.10.2 Maximum Cell Distance

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

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

The default is 0 (No Compensation).

4.2.6.2.10.3 Fairness Factor

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

The range is 0 to 100 (%)

The default is 100 (%).

4.2.6.2.10.4 Per SU Distance Learning

The Per SU Distance Learning option defines the mode in which SUs calculate the 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 for the calculation of the ACK timeout the maximum cell distance; when enabled, each SU uses instead its actual distance from the AU.

The options are Disable or Enable.

The default is Disable.

4.2.6.2.10.5 Show Cell Distance Parameters

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

4.2.6.2.11 Arbitration Inter-Frame Spacing (AIFS)

The time interval between two consecutive transmissions of frames is called Inter-Frame Spacing (IFS). This is the time during which the unit determines whether the medium is idle using the carrier sense mechanism. The IFS depends on the type of the next frame to be transmitted, as follows:

- SIFS (Short Inter-Frame Spacing) is used for certain frames that should be transmitted immediately, such as ACK and CTS frames. The value of SIFS is 16 microseconds.

- DIFS (Distributed coordination function Inter-Frame Spacing) is typically used for other frame types when the medium is free. If the unit decides that the medium is not free, it will defer transmission by DIFS plus a number of time slots as determined by the Contention Window back-off algorithm (see section 4.2.6.5.2) after reaching a decision that the medium has become free.

DIFS equal SIFS plus AIFS, where AIFS can be configured to one or two time slots. Typically, AIFS should be configured to two time slots. A value of 1 should only be used in one of the two units in a point-to-point link, where in the other unit the AIFS remains configured to two time slots. This ensures that the unit with AIFS configured to one has an advantage over the other unit, provided that the Minimum Contention Window (section 4.2.6.5.2) parameter in both units is configured to 0 to disable the contention window back-off algorithm.

NOTE

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

The available options are 1 or 2 (time slots).

The default is 2 time slots.

CAUTION

An AIFS value of 1 should only be used in point-to-point applications (when the Wireless Link Prioritization Option is enabled). Otherwise the default value of 2 must always be used. In a point-to-point link, only one unit should be configured to an AIFS value of 1. When both units need to transmit, the unit with an AIFS value of 1 will have an advantage over the unit with AIFS of 2. In this case, the Minimum Contention Window parameter in both units must be configured to 0 to disable the contention window back-off algorithm.

4.2.6.2.12 Maximum Number of Associations (AU only)

The Maximum Number of Associations parameter defines the maximum number of Subscriber Units that can be associated with the selected AU, while still guaranteeing the required quality of service to customers.

Available values for AU-BS and AU-SA range from 0 to 512. For AUS-BS and AUS-SA the range is from 0 to 8.

Default value for AU-BS and AU-SA is 512. For AUS-BS and AUS-SA the default is 8.

NOTE

When the Data Encryption Option is enabled, the actual maximum number of SUs that can associate with the AU-BS or AU-SA is limited to 124. The number displayed for the Maximum Number of Associations is the value configured for this parameter, which might be higher than the actual limit. The Maximum Number of Associations Limit (512 when Data Encryption is disabled, 124 when Data Encryption is enabled) is indicated in the Show Air Interface Parameters display.

NOTE

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

- A SNAP frame is received from another AU indicating that the SU is now associated with the other AU.
- The SU failed to respond to a certain number of consecutive frames transmitted by the AU and is considered to have "aged out".

Therefore, the database of associated SUs may include units no longer associated with the AU. If the number of associated SUs has reached the value of the Maximum Number of Associations parameter, the selected AU cannot serve additional SUs. To view the current number of associated SUs, use the Display Association Info option in the MAC Address Database menu. To delete inactive SUs from the database you must reset the AU.

4.2.6.2.13 Wireless Link Trap Threshold (AU only)

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

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

The default is 30 (%).

4.2.6.2.14 Country Code Learning by SU (AU only)

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

The AU advertises its country code in every beacon and association response message. Upon synchronization the SU shall check if its country code and the country code received from the AU are the same. If they are not the same and the Country Code Learning by the SU is enabled, the SU will use the AU’s country code: the country code derived limitations will be forced and the following parameters will be set according to the new country definitions:

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

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

The default is Enable.

4.2.6.2.15 Spectrum Analysis

Gaining knowledge of the noise characteristics per channel enables construction of a relatively noise free working environment. In order to gain information regarding noise characteristics in the location of the unit, the unit will enter passive scanning mode for a definite period, during which information will be gathered. The scanned channels will be the channels comprising the selected sub set.

Upon activating the spectrum analysis the unit will automatically reset. During the information-gathering period the unit will not receive nor transmit data. It also will not be able to synchronize/associate, meaning that it cannot be managed via the wireless link. During the spectrum analysis period the unit security mode is changed to promiscuous to enable gathering information regarding all legal frames received by the unit. At the end of the period the unit will reset automatically regaining normal operability upon start up.

The Spectrum Analysis submenu includes the following options:

4.2.6.2.15.1 Spectrum Analysis Channel Scan Period

The Spectrum Analysis Channel Scan Period is the period of staying on each channel during each cycle for information gathering when performing spectrum analysis.

Range: 2-30 seconds.

Default value: 5 seconds.

4.2.6.2.15.2 Spectrum Analysis Scan Cycles

The Spectrum Analysis Scan Cycle is the number of scanning cycles when performing Spectrum Analysis.

Range: 1-100 cycles.

Default value: 2 cycles.

4.2.6.2.15.3 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: when the analysis is completed it will be disabled automatically.

The default is Disable.

4.2.6.2.15.4 Spectrum Analysis Activation

The Spectrum analysis Activation option enables activation of the spectrum analysis process. Upon activation, the unit will reset automatically and start-up in spectrum analysis mode.

4.2.6.2.15.5 Reset Spectrum Analysis Information

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

4.2.6.2.15.6 Spectrum Analysis Information Display

The Spectrum Analysis Information Display option enables viewing the results of the last analysis process. The displayed information includes the following details for each channel:

- **Frequency in MHz**
- **Signal Count:** The number of signals (excluding OFDM frames with the correct bandwidth) in the channel.
- **Signal SNR:** The approximate SNR of signals (excluding OFDM frames with the correct bandwidth) in the channel.
- **Signal Width:** The average width in microseconds of signals (excluding OFDM frames with the correct bandwidth) in the channel.
- **OFDM Frames:** The number of OFDM frames with the correct bandwidth detected in the channel.

4.2.6.2.15.7 Spectrum Analysis Information Display - Continuous

The Spectrum Analysis Information Display - Continuous option is available only when the analysis process is active. It enables viewing the continuously updated results of the current analysis process. The displayed information includes the same details available for a regular Spectrum Analysis Information Display option.

4.2.6.2.16 Lost Beacons Transmission Watchdog Threshold

When it is unable to send beacon frames for a predetermined period of time, such as in the case of interferences, the AU resets itself. The Lost Beacons Transmission Threshold parameter represents the number of consecutive lost beacons after which the unit will reset itself.

The range for this parameter is 100 – 1000 or 0. When the parameter is set to 0, this feature is disabled, i.e. internal refresh will never be performed.

The default value is 218.

4.2.6.2.17 Disassociate (AU only)

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

The Disassociate submenu includes two options:

- **Disassociate All SUs**
- **Disassociate SU By MAC Address**: to disassociate a selected SU

4.2.6.2.18 Noise Immunity Control

The Adaptive Noise Immunity (ANI) mechanism is designed to reduce the wireless physical layer errors and by that enhance the AU processing power of the unit, delivering higher packet processing efficiency.

This ANI mechanism is triggered by the rate of detected Physical Errors and it is modifying different thresholds affecting the immunity to specific interference types.

This feature, active by default, exists in all units with HW revision C and higher running SW version 3.0 and higher. Starting in SW version 4.0, the processing power of the system has been increased dramatically. When using version 4.0 the units are capable to process more packets per seconds, including physical error packets. As a result, the ANI mechanism (triggered by the number of received error packets) may not function properly in certain scenarios, resulting in link performances that are far below the expectations. The option of manually controlling the various parameters used by the ANI mechanism enables to achieve optimal performance in certain deployments where the automatic ANI mechanism may not function properly.

It is strongly recommended to consult with Alvarion experts before switching to manual mode and modifying any of the parameters.

The general rules for using the Noise Immunity Control parameters are:

In the SU, if performance (Modulation Level) is lower than expected based on the SNR, try switching to Manual mode without changing any of the parameters.

CAUTION

Do not change any of the SU’s Noise Immunity Control parameters (except the Noise Immunity State Control) from remote, as it may result in loss of connectivity to the unit.

In the AU, try switching to Manual mode if overall throughput is too low or if SUs are lost although communication conditions are sufficient for good connectivity.

In many deployments the transition to Manual mode is sufficient. If not, you may try changing the Noise Immunity Level and/or Spur Immunity Level parameters. The target is to reduce the amount of Phy Error rate reported by the unit (see

Total Rx events on page 109). To ensure that sensitivity is not reduced too much and SUs are not lost, verify that the Age (see **Display Association Info** on page 113) of all SUs is below 20 seconds.

Do not activate the OFDM Weak Signal parameter if the SNR is below 36 dBm. Under normal conditions, the OFDM Weak Signal should never be activated in the AU, since the SNR of all SUs will be below 36 dBm when ATPC is enabled.

The Noise Immunity Control submenu includes the following options:

4.2.6.2.18.1 Noise Immunity State Control

The Noise Immunity State Control defines the activation mode of the Adaptive Noise Immunity mechanism: Automatic or Manual. The following parameters of the Noise Immunity Control mechanism are applicable only for Manual mode.

The default is Automatic.

4.2.6.2.18.2 Noise Immunity Level

The Noise Immunity Level parameter sets the threshold for immunity against broadband interfering signals. A higher value may reduce the number of errors at the expense of reduced sensitivity.

The range is from 0 to 4. In the current version only 0 and 4 should be used.

The default is 0.

4.2.6.2.18.3 Spur Immunity Level

The Spur Immunity Level parameter sets the threshold for immunity against narrow band interfering signals such as spurious from signals at other frequencies. A higher value may reduce the number of errors at the expense of reduced sensitivity.

The range is from 0 to 7.

The default is 0.

4.2.6.2.18.4 OFDM Weak Signal

The OFDM Week Signal parameter sets the threshold for immunity against interfering OFDM signals.

The available options are 0 or 1. A value of 1 means that the unit will immediately reject OFDM packets with a relatively SNR.

The default is 0.

4.2.6.2.18.5 Pulse Detection Sensitivity

The Pulse Detection Sensitivity parameter affects the Phy error count: If it is set to Low, than all Phy errors will be reported as regular Phy errors, regardless of the signal level. If it is set to High, all Phy errors with levels bellow a certain threshold (not accessible to the user) will be reported as regular Phy errors, while those with levels higher than the threshold will be reported as detected radar pulses.

When DFS (radar detection) is used, the Pulse Detection Sensitivity cannot be set to Low (forced to high). When Spectrum Analyzer is running, the Pulse Detection Sensitivity is automatically forced to high for the duration of the test.

The default is High.

4.2.6.2.18.6 Show Noise Immunity

Select this option to view the current values of the Noise Immunity Control parameters, and some additional parameters of the ANI mechanism.

4.2.6.3 Network Management Parameters

The Network Management Parameters menu enables protecting the Unit from unauthorized access by defining a set of discrete IP addresses as well as IP address ranges from which the unit can be managed using protocols such as Telnet, FTP, TFTP, SNMP, DHCP and ICMP. This excludes management messages generated in the unit, such as Traps or Ping Test frames, which are not filtered. The direction from which management access is permitted can also be configured, which means that management access may be permitted from the wireless medium only, from the wired Ethernet only, or from both.

The Network Management Menu also enables managing transmission of traps, including definition of up to 10 traps destination IP addresses and the associated community strings. In addition, the menu enables specifying the IP address of a connected AP client device to facilitate remote management of a BreezeACCESS WI^2 system.

The Network Management Parameters menu includes the following options:

- Access to Network Management
- Network Management Filtering
- Set Network Management IP address
- Delete a Network Management IP Address
- Delete All Network Management IP Addresses
- Set/Change Network Management IP Address Ranges
- SNMP Traps
- AP Client IP Address (SU only)

4.2.6.3.1 Access to Network Management

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

- From Wireless Link Only
- From Ethernet Only
- From Both Ethernet and Wireless Link

The default selection is From Both Ethernet and Wireless Link.

CAUTION

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

4.2.6.3.2 Network Management Filtering

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

- **Disable:** No IP address based filtering is configured.

- **Activate IP Filter on Ethernet Port:** Applicable only if the Access to Network Management parameter is configured to either From Ethernet Only or From Both Ethernet and Wireless Link. The unit can be managed from the Ethernet port only by stations with IP addresses matching one of the entries in the Set Network Management IP Addresses parameter. If the Access to Network Management parameter is configured to From Both Ethernet and Wireless Link then no IP address based filtering is configured for the wireless port.

- **Activate IP Filter on Wireless Link Port:** Applicable only if the Access to Network Management parameter is configured to either From Wireless Link Only or From Both Ethernet and Wireless Link. The unit can be managed from the wireless port only by stations with IP addresses matching one of the entries in the Set Network Management IP Addresses parameter. If the Access to Network Management parameter is configured to From Both Ethernet and Wireless Link then no IP address based filtering is configured for the Ethernet port.

- **Activate IP filter on Both Ethernet and Wireless Link Ports:** Applicable to all options of the Access to Network Management parameter. The unit can be managed from the port(s) defined by the Access to Network Management parameter only by stations with IP addresses matching one of the entries in the Set Network Management IP Addresses parameter.

The default selection is Disable.

4.2.6.3.3 Set Network Management IP Address

The Set Network Management IP Address option enables defining up to 10 IP addresses of devices that can manage the unit if the Network Management Filtering option is enabled.

The default Network Management IP Address is 0.0.0.0 (all 10 addresses).

4.2.6.3.4 Delete a Network Management IP Address

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

4.2.6.3.5 Delete All Network Management IP Addresses

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

4.2.6.3.6 Set/Change Network Management IP Address Ranges

The Set/Change Network Management IP address Ranges menu enables defining, updating or deleting IP address ranges from which the unit can be managed if the Network Management Filtering option is enabled. This is in addition to the previous options in the Network Management menu that enable defining, updating and deleting discrete IP addresses.

The menu includes the following options:

4.2.6.3.6.1 Set/Change Network Management IP Address Ranges

The Set/Change Network Management IP Address Ranges option enables defining/updating up to 10 IP address ranges from which the unit can be managed if the Network Management Filtering option is enabled.

The default Network Management IP Address Range is 0.0.0.0 TO 0.0.0.0 (all 10 ranges).

A range can be defined using a string that includes either a start and end address, in the format “<start address> to <end address>” (example: 192.168.1.1 to 192.168.1.255), or a base address and a mask, in the format “<base address> mask <mask>” (example: 192.168.1.1 mask 255.255.255.0).

4.2.6.3.6.2 Delete Network Management IP Address Range

The Delete Network Management IP Address Range option enables deleting IP address range entries from the Network Management IP Address Ranges list.

4.2.6.3.6.3 Delete All Network Management IP Address Ranges

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

4.2.6.3.7 SNMP Traps

The SNMP submenu enables or disables the transmission of SNMP Traps. If this option is enabled, up to 10 IP addresses of stations to which SNMP traps are sent can be defined.

4.2.6.3.7.1 Send SNMP Traps

The Send SNMP Traps option enables or disables the sending of SNMP traps.

The default selection is Disable.

4.2.6.3.7.2 SNMP Traps Destination IP Addresses

The SNMP Traps Destination IP Addresses submenu enables defining up to 10 IP addresses of devices to which the SNMP Traps are to be sent.

The default of all 10 SNMP Traps IP destinations is 0.0.0.0.

4.2.6.3.7.3 SNMP Traps Community

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

Valid strings: Up to 8 ASCII characters.

The default for all 10 addresses is “public”, which is the default Read community.

4.2.6.3.7.4 Delete One Trap Address

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

4.2.6.3.7.5 Delete All Trap Addresses

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

4.2.6.3.8 AP Client IP Address (SU Only)

The BreezeACCESS WI^2 system comprises a self-contained combination of an advanced WiFi Access Point and a BreezeACCESS SU-ODU that provides backhaul connectivity. The AP Client IP Address parameter enables the installer to configure in the SU the IP address of the WiFi AP connected to it, providing availability of the IP address information for remote management of the AP.

The default AP Client IP Address is 0.0.0.0 (meaning none).

4.2.6.4 Bridge Parameters

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

The Bridge Parameters menu includes the following options:

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

4.2.6.4.1 VLAN Support

The VLAN Support menu enables defining the parameters related to the IEEE 802.1Q compliant VLAN aware (Virtual LAN aware) feature of the units. Each VLAN includes stations that can communicate with each other, but cannot communicate with stations belonging to different VLANs. The VLAN feature also provides the ability to set traffic priorities for transmission of certain frames. The information related to the VLAN is included in the VLAN Tag Header, which is inserted in each frame between the MAC header and the data. VLAN implementation in BreezeACCESS VL units supports frame routing by port information, whereby each port is connected to only one VLAN.

The system also supports the 802.1 QinQ standard, which defines the way to have 2 VLAN tags (double-tagged frames). This procedure allows an additional VLAN tag, called Service Provider VLAN tag, to be inserted into an existing IEEE 802.1Q tagged Ethernet frame. This is a solution to transport multiple customers' VLANs across the service provider's network without interfering with each other.

The VLAN Support menu includes the following parameters:

- VLAN Link Type

- VLAN ID – Data (SU only)
- VLAN ID – Management
- Service Provider VLAN ID (SU only)
- VLAN Forwarding
- VLAN Relaying (AU only)
- VLAN Traffic Priority
- VLAN QinQ Protocol Ethertype

4.2.6.4.1.1 VLAN ID-Data (SU only)

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

Valid values range from 1 to 4094.

Default value: 1.

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

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

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

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

4.2.6.4.1.2 VLAN ID-Management

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

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

The default value is 65535.

If the VLAN ID-Management is other than 65535:

- Only single-tagged management frames with a matching VLAN ID, or double-tagged management frames with a matching Service Provider VLAN ID received on either the Ethernet or wireless link ports are forwarded to the unit.

- A VLAN Management Tag is inserted in all management frames generated by the unit before transmission on either the Ethernet or wireless link port. The tag includes the values of the **VLAN ID-Management** and the **VLAN Priority-Management** parameters.

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

- For Access, Trunk and Hybrid links: Only untagged management frames received on either the Ethernet or wireless link ports are forwarded to the unit.

- An AU operating in Service Provider link mode with VLAN ID – Management = 65535 cannot be managed from either the Ethernet or wireless ports.

- An SU operating in Service Provider link mode with VLAN ID – Management = 65535 will accept untagged management frames from the Ethernet port. From the wireless port it will accept only tagged frames with a VLAN ID tag that matches the defined Service Provider VLAN ID.

- Management frames generated by the unit are not tagged.

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

Table 4-5: VLAN Management Port Functionality	
Action	**Management Port - Internal**
Receive from Ethernet when Link Type is Access, Trunk or Hybrid	Tagged frames, matching VID-M Untagged frames when VID-M=65535
Receive from Ethernet when Link Type is Service Provider	Tagged frames, matching VID-M
Receive from Wireless when Link Type is Access, Trunk or Hybrid	Tagged frames, matching VID-M Untagged frames when VID-M=65535
Receive from wireless when Link Type is Service Provider	Tagged frames, matching VID-M
Transmit	Insert VID-M, PID-M

Table Legend:

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

4.2.6.4.1.3 VLAN Link Type

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

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

The default selection is Hybrid Link.

4.2.6.4.1.3.1 Access Link (SU only)

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

Table 4-6 summarizes the functionality of the data port for an Access link.

Table 4-6: VLAN Data Port Functionality - Access Link

Action	Data Port - SU
Receive from Ethernet	Untagged frames
Accept from Wireless	Tagged frames, matching VID-D
Tag Insert	VID-D, PID-D (to wireless)
Tag Remove	Yes (to Ethernet)

Table Legend:

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

4.2.6.4.1.3.2 Trunk Link

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

CAUTION

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

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

NOTE

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

If the VLAN Relaying option is enabled in an AU, a data frame relayed with a VLAN ID that is not a member of the unit's VLAN Relaying List is discarded.

NOTE

If the **VLAN Relaying** option is enabled and you manage your devices from behind an SU unit, be sure to include the **VLAN ID-Management** value of all units to be managed when relaying via the wireless port of the AU unit, in the Relaying List. If the VLAN Forwarding option is also enabled in the AU, these VLAN IDs should also be included in the Forwarding List.

Table 4-7 summarizes the functionality of the data port for a Trunk link.

Table 4-7: VLAN Data Port Functionality - Trunk Link

Action	Data Port – AU and SU
Accept from Ethernet	Tagged frames. If Forwarding is enabled, only frames with VLAN ID values which are included in the Forwarding list
Accept from Wireless	Tagged frames If Forwarding is enabled, only frames with VLAN ID values which are included in the Forwarding list
Tag Insert	No
Tag Remove	No

4.2.6.4.1.3.3 Hybrid Link

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

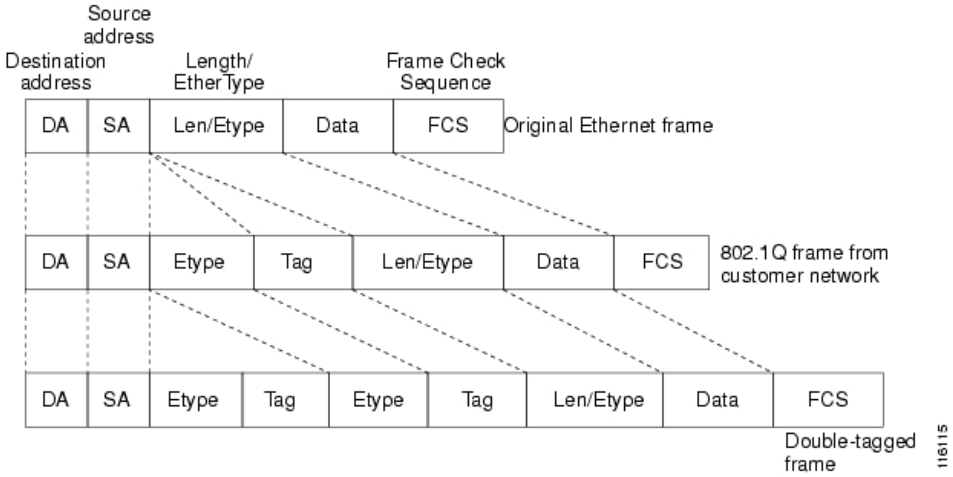
Table 4-8 summarizes the functionality of the data port for a Hybrid link.

Table 4-8: VLAN Data Port Functionality - Hybrid Link

Action	Data Port – AU and SU
Accept from Ethernet	All
Accept from Wireless	All
Tag Insert	No
Tag Remove	No

4.2.6.4.1.3.4 Service Provider Link

A Service Provider Link transfers both single tagged frames (Service Provider tag) and double-tagged frames (Service Provider tag + Customer tag). The Service Provider tag includes the Service Provider VLAN ID and the VLAN QinQ Ethertype.



The following tables summarize the functionality of the SU/AU data port for a Service Provider Link.

Table 4-9: VLAN Data Port Functionality for SU - Service Provider Link

Action	Data Port –SU
Accept from Ethernet	Untagged frames Single tagged frames: ■ If Forwarding is disabled ■ If Forwarding is enabled, only frames with VLAN ID values which are included in the Forwarding List
Accept from Wireless	Single tagged frames: only frames with a Service Provider tag whose parameters match the Service Provider parameters defined in the unit (Service Provider VLAN ID and VLAN QinQ Ethertype) Double tagged frames: only frames with a Service Provider tag whose parameters match the Service Provider parameters defined in the unit (Service Provider VLAN ID and VLAN QinQ Ethertype). If Forwarding is enabled, only frames with Customer VLAN ID values that are included in the Forwarding List
Tag Insert	Service Provider (SP) tag (to wireless)
Tag Remove	Yes (to Ethernet)

Table 4-10: VLAN Data Port Functionality for AU - Service Provider Link

Action	Data Port –AU
Accept from Ethernet	Single tagged frames: ■ If Forwarding is disabled ■ If Forwarding is enabled, only frames with VLAN ID values which are included in the Forwarding List Double tagged frames: ■ If Forwarding is disabled ■ If Forwarding is enabled, only frames with Service Provider VLAN ID values which are included in the Forwarding List
Accept from Wireless	Single tagged frames: ■ If Forwarding is disabled ■ If Forwarding is enabled, only frames with VLAN ID values which are included in the Forwarding List Double tagged frames: ■ If Forwarding is disabled ■ If Forwarding is enabled, only frames with Service Provider VLAN ID values which are included in the Forwarding List
Tag Insert	No
Tag Remove	No

NOTE

The following units management limitations apply when using a Service Provider Link:

- The unit can be managed only with tagged frames: VLAN ID – Management must be other than 65535.
- To enable proper management, all units in a cell (the AU and all SUs served by it) must use the VLAN ID - Management.
- The VLAN ID – Management must differ from the Customer's VLAN ID - Data.

4.2.6.4.1.4 VLAN Forwarding (AU and SU)

The VLAN Forwarding feature is applicable only for Trunk Links and Service Provider Links. It enables defining the VLAN ID values to be included in the VLAN Forwarding List. If the Link Type is defined as either a Trunk Link or a Service Provider Link and the VLAN Forwarding option is enabled, a 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 is discarded.

The VLAN Forwarding submenu provides the following options:

4.2.6.4.1.4.1 VLAN Forwarding Support

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

Available selections are Disable and Enable.

The default selection is Disable.

4.2.6.4.1.4.2 Add Forwarding VLAN ID

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

Valid values are 1 to 4094.

4.2.6.4.1.4.3 Remove Forwarding VLAN ID

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

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

4.2.6.4.1.4.4 Show VLAN ID Forwarding List

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

NOTE

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

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

4.2.6.4.1.5 VLAN Relaying (AU only)

The VLAN Relaying feature is applicable only for Trunk Links and Service Provider Links. It enables defining the VLAN ID values to be included in the VLAN Relaying List.

If the Link Type is defined as either a Trunk Link or a Service Provider Link and the VLAN Relaying Support option is enabled, a frame relayed from the wireless link, which is a frame received from the wireless link that should be transmitted back through the wireless link, with a VLAN ID (or a Service Provider VLAN ID) that is not a member of the unit's VLAN Relaying List, is discarded. If VLAN Forwarding Support is also enabled, it is necessary to configure all the VLAN IDs in the Relaying List also in the Forwarding List to enable the relaying operation.

The VLAN Relaying menu provides the following options:

4.2.6.4.1.5.1 VLAN Relaying Support

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

Available selections are Disable and Enable.

The default selection is Disable.

4.2.6.4.1.5.2 Add Relaying VLAN ID

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

Valid values are 1 to 4094.

4.2.6.4.1.5.3 Remove Relaying VLAN ID

The Remove Relaying VLAN ID option enables removing a VLAN ID from the VLAN ID Relaying List. Valid values are VID values (from 1 to 4094)) that are included in the VLAN Relaying List.

4.2.6.4.1.5.4 Show VLAN ID Relaying List

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

NOTE

If the VLAN ID Relaying List is empty and the VLAN Relaying Support is Enabled, then all data frames relayed from the wireless link are discarded.

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

4.2.6.4.1.6 Service Provider VLAN ID (SU only)

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

The range is 1 to 4094.

The default value is 1.

The Service provider VLAN ID affects frames received from the wireless link port, as follows:

- Both single-tagged frames (having Service Provider VLAN ID tag) and double-tagged frames (having Service Provider VLAN ID and customer VLAN ID tags) with matching VLAN ID are forwarded to the Ethernet Port (provided the Ethertype of the tag matches the configured VLAN QinQ Ethertype).

- Before transmitting the frames to the Ethernet port, the Service Provider VLAN ID tag is removed.

The Service Provider VLAN ID affects frames received from the Ethernet link port, as follows: A Service Provider tag, that includes the configured Service Provider VLAN ID (and the VLAN QinQ Ethertype) is inserted in all frames, both tagged and untagged, before transmission to the wireless link.

4.2.6.4.1.7 VLAN Traffic Priority

The VLAN Traffic Priority menu enables configuring the VLAN Priority field in applicable frames. These parameters only impact the way in which other VLAN aware devices in the network will handle the packet. All parameters that affect prioritization within the BreezeACCES VL system, including VLAN-based prioritization, are located in the Traffic Prioritization menu.

The VLAN Traffic Priority menu includes the following parameters:

- VLAN Priority – Data (SU only)

- VLAN Priority – Management

4.2.6.4.1.7.1 VLAN Priority - Data (SU only)

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

Valid values range from 0 to 7.

The default value is 0.

4.2.6.4.1.7.2 VLAN Priority - Management

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

Valid values range from 0 to 7.

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

4.2.6.4.1.8 VLAN QinQ Protocol Ethertype

The VLAN QinQ Proptocol Ethertype parameter sets the Ethertype of the Service Provider tag, and is applicable only for Service Provider Links.

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

The default value is 8100 (Hex).

4.2.6.4.1.9 Show VLAN Parameters

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

4.2.6.4.2 Ethernet Broadcast Filtering (SU only)

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

The Ethernet Broadcast Filtering menu includes the following parameters:

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

4.2.6.4.2.1 Filter Options

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

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

The default selection is Disable.

4.2.6.4.2.2 DHCP Broadcast Override Filter

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

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

The default selection is Disable.

4.2.6.4.2.3 PPPoE Broadcast Override Filter

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

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

The default selection is Disable.

4.2.6.4.2.4 ARP Broadcast Override Filter

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

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

The default selection is Enable.

4.2.6.4.3 Ethernet Broadcast/Multicast Limiter

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

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

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

The Ethernet Broadcast/Multicast Limiter menu allows viewing and setting the following parameters:

4.2.6.4.3.1 Ethernet Broadcast/Multicast Limiter Option

The Ethernet Broadcast/Multicast Limiter Option defines the limiter's functionality. The available options are:

- Disable: No limiter
- Limit only Broadcast Packets
- Limit Multicast Packets that are not Broadcasts
- Limit All Multicast Packets (including broadcast)

The default selection is Disable.

4.2.6.4.3.2 Ethernet Broadcast/Multicast Limiter Threshold

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

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

The default is 50 packets.

4.2.6.4.3.3 Ethernet Broadcast/Multicast Limiter Send Trap Interval

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

The range is from 1 to 60 minutes.

The default is 5 minutes.

4.2.6.4.4 Bridge Aging Time

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

The available range is 20 to 2000 seconds.

The default value is 300 seconds.

4.2.6.4.5 Broadcast Relaying (AU only)

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

The default selection is Enable.

4.2.6.4.6 Unicast Relaying (AU only)

The Unicast Relaying option enables selecting whether the unit performs unicast relaying. When the Unicast Relaying parameter is enabled, unicast packets originating from devices on the wireless link can be transmitted back to the wireless link devices. If disabled, these packets are not sent to the wireless link even if they are intended for devices on the wireless link. Disable the Unicast Relaying parameter only if all unicast messages from the wireless link are certain to be directed to the local wired LAN.

The default selection is Enable.

4.2.6.4.7 MAC Address List (AU only)

The MAC Address List submenu enables to define a list of up to 100 MAC addresses as belonging to devices that are either granted or denied service. 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.

The MAC Address List submenu includes the following:

4.2.6.4.7.1 Add MAC Address to List

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

4.2.6.4.7.2 Remove MAC Address from List

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

4.2.6.4.7.3 MAC Address List Action

This parameter 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.

Possible options for this parameter are Deny and Allow.

The default is Deny.

4.2.6.4.7.4 Show MAC Address List

Select Show MAC Address List to display the current list of MAC Addresses included in the List and the selected List Action.

4.2.6.4.8 Roaming Option (SU only)

The Roaming Option defines the roaming support of the unit. When roaming is not expected, it is preferable to set this parameter to Disable. This will cause the unit to start scanning for another AU after losing connectivity with the current AU only after 7 seconds during which no beacons were received from the current AU. This will prevent scanning for another AU in cases where no beacons were received due to a short temporary problem.
When set to Enable, the SU will wait only one second before it starts scanning for another AU. In addition, when the Roaming Option is enabled, the SU will send Roaming SNAP messages upon associating with a new AU. This enables fast distribution of the new location for all clients that are behind the SU. In this case, the SU will send multicast SNAP messages via the wireless link each time it associates with a new AU, except for the first association after reset. The SU will send one SNAP message for each client learned on its Ethernet port, based on its bridging table. In the SNAP message the clients’ MAC address is used as the source address. The AU that receives this SNAP message learns from it the new location of the clients. It forwards the SNAP to other AUs and Layer-2 networking equipment via its Ethernet port, to facilitate uninterrupted connectivity and

correct routing of transmissions to these clients. The new AU as well as the previous AU with which the SU was associated, will forward the SNAP messages to all other SUs associated with them.

The default is Disable.

4.2.6.4.9 Ports Control (SU only)

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

4.2.6.4.9.1 Ethernet Port Control

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

The default selection is Enable.

4.2.6.4.10 Show Bridge Parameters

The Show Bridge Parameters option displays the current values of the Bridge parameters.

4.2.6.5 Performance Parameters

The Performance Parameters menu enables defining a series of parameters that control the method by which traffic is transmitted through the wireless access network.

The Performance Parameters menu includes the following parameters:

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

4.2.6.5.1 RTS Threshold

The RTS Threshold parameter defines the minimum frame size that requires an RTS/CTS (Request To Send/Clear To Send) handshake. Frames whose size is smaller than the RTS Threshold value are transmitted directly to the wireless link without being preceded with RTS frames. Setting this parameter to a value larger than the maximum frame size eliminates the RTS/CTS handshake for frames transmitted by this unit.

The available values range from 20 to 4032 bytes for units with HW revision C, and 20 to 2200 for units with HW revision A or B.

The default value is 60 bytes for SUs. For AUs with HW revision C the default is 4032, and for AUs with HW revision A or B the default is 2200. It is recommended that these values be used to ensure that RTS/CTS is never used in the AU.

4.2.6.5.2 Minimum Contention Window

The Minimum Contention Window parameter determines the time that a unit waits from the time it has concluded that there are no detectable transmissions by other units until it attempts to transmit. The BreezeACCESS VL system uses a special mechanism based on detecting the presence of a carrier signal and analyzing the information contained in the transmissions of the AU to estimate the activity of other SUs served by the AU. The target is to minimize collisions in the wireless medium resulting from attempts of more than one unit to transmit at the same time.

The system uses an exponential Back-off algorithm to resolve contention between several units that want to access the wireless medium. The method requires each station to choose a random number N between 0 and a given number C each time it wants to access the medium. The unit will attempt to access the medium only after a time equal to DIFS (for more details refer to section 4.2.6.2.11) plus N time slots, always checking if a different unit has accessed the medium before. Each time the unit tries to transmit and a collision occurs; the maximum number C used for the random number selection will be increased to the next available value. The available values are 7, 15, 31, 63, 127, 255, 511 and 1023.

The Minimum Contention Window parameter is the first maximum number C used in the back-off algorithm. The higher the number of SUs served by the same AU, the higher the Minimum Contention Window for each SU should be. In addition, when the Wireless Link Prioritization Option is enabled, the Minimum and Maximum Contention Window parameters can be configured to provide certain units with an advantage over other units.

The available values are 0, 7, 15, 31, 63, 127, 255, 511 and 1023. A value of 0 means that the contention window algorithm is not used and that the unit will attempt to access the medium immediately after a time equal to DIFS.

The default value is 15.

CAUTION

A value of 0 disables the contention window back-off algorithm. It should only be used in point-to-point applications. For more details on configuring units in a point-to-point link refer to section 4.2.6.2.11.

4.2.6.5.3 Maximum Contention Window

The Maximum Contention Window parameter defines the upper limit for the maximum number C used in the back-off algorithm as described in Minimum Contention Window above.

The available values are 7, 15, 31, 63, 127, 255, 511 and 1023.

The default value is 1023.

4.2.6.5.4 Multicast Modulation Level (AU only)

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

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

The minimum value for the Multicast Modulation Level is defined by the Sub-Band in use.

The maximum value for the Multicast Modulation Level is defined by the Sub-Band in use and the HW revision of the unit. Units with HW revision A support a maximum value of 7, while units with HW revision B and higher support a maximum value of 8.

For information on how to view the Sub-Bands supported by the unit and the supported parameters' values and options, refer to section 4.2.2.4.

The default value is the lowest supported modulation level.

4.2.6.5.5 Maximum Modulation Level

When the Adaptive Modulation Algorithm (see section 4.2.6.5.9) is enabled, it changes the modulation level dynamically according to link conditions. The purpose is to increase the probability of using the maximum possible modulation level at any given moment. Although the algorithm will avoid using modulation levels that are too high for the prevailing link conditions, it might be better under certain conditions to limit the use of higher modulation levels. If the link quality is not sufficient, it is recommended that the maximum modulation level be decreased, as higher modulation levels increase the error rate. In such conditions, a higher Maximum Modulation Level increases the number or retransmissions before the modulation level is being reduced by the Adaptive Modulation Algorithm. A high number of retransmissions reduces the overall throughput of the applicable SU as well as all other SUs associated with the same AU.

The link quality can be estimated based on the SNR measurement of the SU at the AU, which can be viewed in the MAC Address Database option in the Site Survey menu. If the measured SNR is less than a certain threshold, it is recommended that the maximum modulation level of the SU be decreased in accordance with Table 4-11, using the values of typical sensitivity. It is recommended to add a 2 dB safety margin to compensate for possible measurement inaccuracy or variance in the link quality.

NOTE

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

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

The minimum value for the Maximum Modulation Level is defined by the Sub-Band in use.

The maximum value for the Maximum Modulation Level is defined by the Sub-Band in use and the HW revision of the unit. Units with HW revision A support a maximum value of 7, while units with HW revision B and higher support a maximum value of 8.

For information on how to view the Sub-Bands supported by the unit and the supported parameters' values and options, refer to section 4.2.2.4.

The default is the highest supported Modulation Level.

Table 4-11: Recommended Maximum Modulation Level*

SNR	Maximum Modulation Level
SNR > 23 dB	8
21 dB < SNR < 23 dB	7
16 dB < SNR < 21 dB	6
13 dB < SNR < 16 dB	5
10 dB < SNR < 13 dB	4
8 dB < SNR < 10 dB	3
7 dB < SNR < 8 dB	2
6 dB < SNR < 7 dB	1

* The maximum supported value depends on the unit's HW revision and on the Max Modulation Level according to the Sub-Band.

4.2.6.5.6 Average SNR Memory Factor

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

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

Default value: 5

4.2.6.5.7 Number of HW Retries

The Number of HW Retries parameter defines the maximum number of times that an unacknowledged packet is retransmitted. When the Adaptive Modulation Algorithm is disabled, a frame will be dropped when the number of unsuccessful retransmissions reaches this value. For details on the effect of this parameter when the Adaptive Modulation Algorithm is enabled, refer to section 4.2.6.5.9.

NOTE

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

The available values range is from 1 to 14.

The default value is 10.

4.2.6.5.8 Burst Mode

Burst mode provides an increased throughput by reducing the overhead associated with transmissions in the wireless medium. In a burst transmission the inter-frame spacing is reduced and unicast data frames are transmitted without any contention period (burst mode is not activated on broadcasts/multicasts).

The Burst Mode is available only if Burst Mode is supported by the Sub-Band in use. For information on how to view the Sub-Bands supported by the unit and the supported parameters' values and options, refer to section 4.2.2.4.

In AUs with HW Revision B or lower, Burst Mode cannot be activated when the DFS option is used. In AUs with HW Revision B or lower, the Burst Mode option will be "blocked" upon trying to enable Burst Mode when the DFS Option is enabled. This limitation does not apply to AUs with HW Revision C.

In SUs and AUs with HW Revision B or lower, Burst Mode cannot be activated when using WEP for data encryption. In units with HW Revision B or lower, the Burst Mode option will be "blocked" upon trying to enable it when using WEP for data encryption. This limitation does not apply to units with HW Revision C.

NOTE

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

4.2.6.5.8.1 Burst Mode Option

The Burst Mode Option enables or disables the Burst Mode operation.

The default is Enable.

4.2.6.5.8.2 Burst Mode Time Interval

The Burst Mode Time Interval defines the burst size, which is the time in which data frames are sent immediately without contending for the wireless medium.

The range is 1 to the value of the Maximum Burst Duration defined for the Sub-Band.

The default is 5 milliseconds or the value of Maximum Burst Duration defined for the Sub-Band (the lower of the two values).

4.2.6.5.9 Adaptive Modulation Algorithm (Multi Rate)

The Adaptive Modulation Algorithm enables adapting the modulation level of transmitted data to the prevailing conditions of the applicable radio link. The algorithm provides Access Units with simultaneous, adaptive support for multiple Subscriber Units at different modulation levels, as transmission’s modulation level decisions are made separately for each associated SU.

Link quality fluctuates due to various environmental conditions. Dynamically switching between the possible modulation levels increases the probability of using the maximum modulation level suitable for the current radio link quality at any given moment.

The decisions made by the Adaptive Modulation Algorithm for the modulation level to be used are based on multiple parameters, including information on received signal quality (SNR) that is received periodically from the destination unit, the time that has passed since last transmission to the relevant unit, and the recent history of successful and unsuccessful transmissions/retransmissions. In the AU the decision algorithm is performed separately for each SU.

The transmission/retransmission mechanism operates as follows:

1. Each new frame (first transmission attempt) will be transmitted at a modulation level selected by the Adaptive Modulation algorithm.

2. If first transmission trial has failed, the frame will be retransmitted at the same modulation level up to the maximum number of retransmission attempts defined by the Number of HW Retries parameter.

The Adaptive Modulation Parameters menu includes the following parameters:

4.2.6.5.9.1 Adaptive Modulation Option

The Adaptive Modulation Option enables or disables the Adaptive Modulation decision algorithm. When enabled, the algorithm supports decrease/increase of transmission’s modulation levels between the lowest possible level to the value configured for the Maximum Modulation Level parameter. If the Maximum Modulation Level is set at the lowest possible level, the Adaptive Modulation algorithm has no effect.