WB-B

System Manual

Software Version 6.6
August 2011
P/N 215888

Document Control

Topic	Description	Version/Date issued
BU/RB-B100 Section 1.2, 4.2.2.1, 4.2.6.6.2	New products	SW Version 4.0, July 2006
Change Unit Type Section 4.2.3.13	New feature	SW Version 4.0, July 2006
FIPS 197 Section 4.2.5.8.1.3, 4.2.5.8.2.1, 4.2.6.7	Optional support (under license) of FIPS 197 compliant encryption. BU/RB-B100 only.	SW Version 4.0, July 2006
IDU-ODU Cable Section 2.1.2	Updated maximum length of IDU-ODU cable	SW Version 4.0, July 2006
Frequency configuration Section 4.2.6.2.3.1, 4.2.6.2.5	Improved mechanism for automatic detection of frequency/bandwidth. Removed parameters: Sub Band select (RB), Frequency Subset Definition (RB). New parameters: User Defined Frequency Subsets.	SW Version 4.0, July 2006
Transmit Power, Maximum Transmit Power Section 4.2.6.2.8.1	Simplified configuration mechanism: A single parameter instead of per-modulation level parameters.	SW Version 4.0, July 2006
5.3 FCC limitations Section 4.2.6.2.4.2	Updated Tx Power limitations for compliance with FCC regulations	SW Version 4.0, July 2006
ATPC Delta from Minimum SNR Level Section 4.2.6.2.8.3.3	Default values updated	SW Version 4.0, July 2006
Tx Control Section 4.2.6.2.8.5	Added option: Ethernet Status Control	SW Version 4.0, July 2006
Lost Beacons Transmission Watchdog Threshold Section 4.2.6.2.14	New feature	SW Version 4.0, July 2006
Concatenation Section 4.2.6.2.9	Improved mechanism. New parameter: Maximum Concatenated Frame Size. Removed: Maximum Number of Frames	SW Version 4.0, July 2006
IP Precedence Threshold Section 4.2.6.6.3.2.2	Default value updated	SW Version 4.0, July 2006
DSCP Threshold Section 4.2.6.6.3.2.3	Default value updated	SW Version 4.0, July 2006

Topic	Description	Version/Date issued
Low Priority Traffic Minimum Percent Section 4.2.6.6.3.5	New feature	SW Version 4.0, July 2006
Wireless Link Prioritization Section 4.2.6.6.3.6	New feature (BU-B100 only)	SW Version 4.0, July 2006
Minimum Contention Window Section 4.2.6.5.1	New feature	SW Version 4.0, July 2006
Maximum Contention Window Section 4.2.6.5.2	New feature	SW Version 4.0, July 2006
Fairness Factor Section 4.2.6.2.10.3	New feature	SW Version 4.0, July 2006
FTP Client IP Address Sections 4.2.3.11, 4.2.3.12	Changed functionality (read only, set to unit's IP Address)	SW Version 4.0, July 2006
FTP Server IP Address Sections 4.2.3.11, 4.2.3.12, 4.2.3.9.4	Changed default to 10.0.0.253	SW Version 4.0, July 2006
Number of HW Retries Section 4.2.6.5.7	Maximum value was changed from 15 to 14	SW Version 4.0, July 2006
Ethernet packet length Section 4.2.5.1.1	Updated maximum length for unit with HW revision C and higher	SW Version 4.0, July 2006
Basic Parameters Table Table 3-1	Updated according to applicable changes (new/removed parameters)	SW Version 4.0, July 2006
Parameters that are not reset to default value after Set Complete Factory/Operator Defaults Table 4-2	Updated according to applicable changes (new/removed parameters)	SW Version 4.0, July 2006
Parameters that are not reset to default value after Set Partial Factory/Operator Defaults Table 4-3	Updated according to applicable changes (new/removed parameters)	SW Version 4.0, July 2006
Basic Configuration Menu Section 4.2.4	Updated according to applicable changes (new/removed parameters)	SW Version 4.0, July 2006
Parameters Summary Appendix E	Updated according to applicable changes (new/removed parameters)	SW Version 4.0, July 2006

Topic	Description	Version/Date issued
2.4 GHz Frequency Band Support	New Products	SW Version 4.1 August 2006
IDU PS1036 removed from Manual. Sections 1.4.4.1, 2.4, 3.5 .2	Replaced by PS1073	SW Version 4.0.27 October 2006
Password Recovery Sections 4.1.1	New feature - a procedure for password recovery if password was lost/forgotten.	SW Version 4.0.27 February 2007
AP Client IP Address Sections 4.2.6.3.8, Table 4-3, Parameters Summary Appendix E	New feature	SW Version 4.0.27 February 2007
Noise Immunity Control Section 4.2.6.2.15, Table 4-3, Parameters Summary Appendix E	New feature	SW Version 4.0.27 February 2007
Show Unit Status Section 4.2.2.1	Added Country Code, Serial Number and ATE Test Status	SW Version 4.5 June 2007
Wireless Rx Events Section 4.2.5.1.2	Added Other counter	SW Version 4.5 June 2007
Antenna Compliance Statement (in Legal Rights)	New	SW Version 4.5 June 2007
Transmit Power Compliance With Regulations Section 3.1.3	New	SW Version 4.5 June 2007
Minimum and Maximum Contention Window parameters Run-Time Update definition, Parameters Summary Appendix E	Parameters are not Run-Time Updated (reset required)	SW Version 4.5 June 2007
RB "aging" mechanism (removal from Association Database) Section 4.2.5.4.1	Updated	SW Version 4.5 July 2007
Pulse Detection Sensitivity Section 4.2.6.2.15.5, Parameters Summary Appendix E	Default has been changed to Low	SW Version 4.5 July 2007

Topic	Description	Version/Date issued
Supported range of modulation levels Sections 4.2.6.5.3, 4.2.6.5.4	Updated description	SW Version 4.5 July 2007
Default value of DFS Minimum Pulses to Detect Section 4.2.6.2.4.3.6 Parameters Summary Appendix E	4 for FCC, 8 for other (ETSI)	SW Version 4.5 July 2007
FCC Radiation Hazard Warning (in Legal Rights)	Updated	SW Version 4.5 July 2007
Usable frequencies limitations Section 4.2.6.2.4.2	Updated	SW Version 4.5 July 2007
Re-apply Country Code Values Section 4.2.6.8.2, Appendix E	New feature	SW Version 4.5 July 2007
Basic Parameters Section 4.2.4	Added AP Client IP Address	SW Version 4.5 July 2007
DFS Section 4.2.6.2.4.3.1	Name changed from DFS Option to DFS Required by Regulations (No/Yes)	SW Version 4.5 July 2007
Sub-Band Select in RB Sections 4.2.6.2.5.1, 4.2.6.2.13	Added/updated descriptions	SW Version 4.5 July 2007
Frequency Ranges Sections 1.1, 1.4.1	The 5.8 GHz band is up to 5.875 GHz (actual usable frequencies depend on Country Code)	SW Version 4.5 August 2007
Antenna specifications Section 1.4.1	Updated compliance to ETSI standard (EN 302 326-3 V1.2.1 (2007-01)	SW Version 4.5 August 2007
Limitations on usable frequencies in FCC 5.3 GHz band Sections 3.1.3, 4.2.6.2.4.2	Updated	SW Version 4.5 August 2007
Correct Run-Time update of Unit Control Parameters Appendix E - Parameters Summary Section E.1.1	FTP Server IP Address, FTP Gateway IP Address, FTP User Name, FTP Password are updated in run-time (reset not required)	SW Version 5.0 November 2007

Topic	Description	Version/Date issued
Correct Run-Time update of Air Interface Parameters Appendix E - Parameters Summary Section E.1.3	Preferred BU MAC Address, Wireless Trap Threshold are not updated in run-time (reset is required). DFS Required by Regulations, Frequency Subset Definition, Channel Check Time, Channel Avoidance Period, RB Waiting Option, Minimum Pulses to Detect, Channel Reuse Option, Radar Activity Assessment Period, Maximum Number of Detections in Assessment Period, are updated in run-time (reset is not required). Spectrum Analysis parameters are applicable in run-time (configured per test)	SW Version 5.0 November 2007
Correct Run-Time update of Service Parameters Appendix E - Parameters Summary Section E.1.7	MIR: Downlink, MIR: Uplink are updated in run-time (reset is not required).	SW Version 5.0 November 2007
Send Traps Section 4.2.6.3.7	Traps are generated and sent only by BU (including traps on behalf of associated RB)	SW Version 5.0 November 2007
Unit Control Menu Section 4.2.3	Re-apply Country Codes Values option has been removed (available in Basic and Advanced Configuration, Country Code Parameters.	SW Version 5.0 November 2007
Wi2 IP Address Section 4.2.6.3.8	Updated name (was previously AP Client IP Address)	SW Version 5.0 November 2007
Basic Configuration Menu Section 4.2.4	Added Country Code Parameters	SW Version 5.0 November 2007
Country Code Parameters Sections 4.2.6.8, 3.1.1, 3.1.2	New	SW Version 5.0 November 2007
MAC Address Database in BU Section 4.2.5.4.1	Updated the information displayed in the various options	SW Version 5.0 November 2007
MAC Address Database in RB Section 4.2.5.4.2	Updated the displayed information	SW Version 5.0 November 2007
FIPS-197 Support Sections 1.1, 1.2	Optionally available for all units with HW Revision C or higher	SW Version 5.0 November 2007
Menu header Section 4.1.1	Updated details of Menu header	SW Version 5.0 November 2007
Management Application Section 1.1	BWA Config has been replaced by bwaCRAFT	SW Version 5.0 November 2007

Topic	Description	Version/Date issued
Set Complete/Partial Defaults Section 4.2.3.2.1	Selected Country Code does not change after Set Complete/Partial Defaults	SW Version 5.0 November 2007
Feature License Section 4.2.3.10	Added note on potential copy/paste problems	SW Version 5.0 November 2007
10 MHz bandwidth support Sections 1.4.1, 3.1.3, 4.2.2.4, 4.2.6.2.4.2, 4.2.6.5.3, 4.2.6.5.4	New capability in units with HW Revision C	SW Version 5.0 November 2007
Send Broadcasts/Multicasts as Unicasts Section 4.2.6.4.7	New feature	SW Version 5.0 November 2007
Data Encryption Option Section 4.2.6.7.2	BU with Data Encryption Option enabled can accept non-encrypted data frames (previously it was stated that this is applicable only for RB)	SW Version 5.0 December 2007
Low Priority AIFS Section 4.2.6.6.3.6.2	The range has been changed from 3-254 to 3-50.	SW Version 5.0 December 2007
Regulation Max EIRP Table 3-2	Updated (new Country Codes, added support for 10 MHz bandwidth)	SW Version 5.0 December 2007
Scanning Mode Section 4.2.6.2.7	Updated description (set to passive if DFS supported by Country Code)	SW Version 5.0 December 2007
Pulse Detection Sensitivity Section 4.2.6.2.15.5	Updated description.	SW Version 5.0 December 2007
Noise Immunity Control Section 4.2.6.2.15	Updated: Available only in units with HW Revision C and higher, except to Pulse Detection Sensitivity that is available also in units with HW Revision B	SW Version 5.0 December 2007
Antenna Gain Section 4.2.6.2.9	Range updated	SW Version 5.0 December 2007
Maximum Burst Duration Section 4.2.6.6.2	New parameter	SW Version 5.0 December 2007
MAC Address Database in BU Section 4.2.5.4.1	In Display Association Info, RSSI info has been added (per RB)	SW Version 5.2 May 2008
Continuous Noise Floor Display Sections 4.2.5.3.2 (RB), 4.2.5.5 (BU)	New feature	SW Version 5.2 May 2008
Continuous Average SNR/RSSI Display in RB Section 4.2.5.3.1	Average RSSI has been added to the display. Added formula used for calculations.	SW Version 5.2 May 2008

Topic	Description	Version/Date issued
Spectrum Analysis Information Display, Section 4.2.6.2.13.6	Added new parameters (OFDM SNR, OFDM Max SNR, Noise Floor Avg, Noise Floor Max)	SW Version 5.2 May 2008
Show Spectrum Analysis Parameters & Data, Section 4.2.6.2.13.8	Updated manual	SW Version 5.2 May 2008
Show Best BU Parameters and Data, Section 4.2.6.2.6.4	RSSI of the received signal has been added	SW Version 5.2 May 2008
Hidden ESSID Sections 1.4.3, 4.2.2.1, 4.2.6.2.2, 4.2.4.4, 4.2.5.6, 3.1.1, 4.2.3.2.1	New feature	SW Version 5.2 May 2008
DFS in Universal Country Codes in the 5.4 and 5.8 GHz band. Sections 4.2.6.2.4.3, 4.2.6.2.4.3.8, 4.2.4.4, 3.1.1	New feature	SW Version 5.2 May 2008
DFS Required By Regulations Section 4.2.6.2.4.3.1	Updated default: Yes for Country Codes where required by regulations, No for Universal Country Codes in the 5.4 and 5.8 GHz bands	SW Version 5.2 May 2008
Noise Floor Calculation Sections 4.2.6.2.16, 4.2.3.2.1	New feature	SW Version 5.2 May 2008
BU/RB-B10 Sections 1.2, 1.4.1, 1.4.4.1, 1.4.4.2, 2.1.1, 2.3.2, 2.3.5.3, 3.2, 4.2.2.1, 4.2.6.5.10, 4.2.6.6.2.1, 4.2.6.6.2.2	New product	SW Version 5.2 May 2008
Aligning the Antennas Section 3.3	Improved process description	SW Version 5.2 May 2008
Wireless Link Prioritization Sections 1.1, 4.2.3.2.1, 4.2.6.5.1, 4.2.6.6.3, 4.2.6.6.3.6	Starting on this version this feature is available also for BU-B14 and BU-B28	SW Version 5.2 May 2008
Protecting ODU Connections Section 2.3.3	New	SW Version 5.2 May 2008

Topic	Description	Version/Date issued
Calibration of Noise Floor Indication Section 4.2.6.2.17	New feature	SW Version 5.2 May 2008
RTS Threshold Section 4.2.6.5.1	New feature	SW Version 5.2 May 2008
Appendix E - Parameters Summary	Updated to reflect all SW version 5.2 changes	SW Version 5.2 May 2008
RESET Button Functionality Section 2.4.1	Updated	SW Version 5.2 June 2008
Association Database in BU Section 4.2.5.4.1	Updated: Association SNAP from another BU is not used for removal of RB from the database.	SW Version 5.2 June 2008
RB Unit Status Section 4.2.2.1	Updated (added AUTHENTICATING status)	SW Version 5.2 June 2008
File Loading Appendix B	Updated: A known parameter with a value that is invalid or out of range will be ignored	SW Version 5.2 June 2008
Antenna Alignment Section 3.3	Updated and improved	SW Version 5.2 July 2008
Number of entries in Bridging Info (Forwarding Database) Sections 4.2.5.4.1, 4.2.5.4.2	Updated to 4093 in BU, 4092 in RB	SW Version 5.2 July 2008
Equipment Positioning Guidelines Section 2.2	Minimum distance of 10 cm between the ODU and antenna.	SW Version 5.2 July 2008
SNR Bar Table 3-4, Table 3-6	SNR Bar LED functionality for BU updated	SW Version 5.5.20 April 2009
DFS Section 4.2.6.2.3	DFS mechanism updated for ETSI based country codes	SW Version 5.5.20 April 2009
LED Mode Section 4.2.3.14	LEDs behavior can be customized	SW Version 6.0, October 2009
Adaptive Modulation Section 4.2.6.5.10	Updated Adaptive Modulation algorithm	SW Version 6.0, October 2009
Ethernet Frame Size Section 4.2.6.5.11	Added ability to set the maximum ethernet frame size to 2000 bytes.	SW Version 6.0, October 2009
IP Range Prioritization Section 4.2.6.6.3.4	Added IP range prioritization for the priority queue	SW Version 6.0, October 2009

Topic	Description	Version/Date issued
Control Modulation Level Section 4.2.6.5.6	Added control for ACK frames modulation	SW Version 6.0, October 2009
Antenna Compliance Statement	Updated	SW Version 6.6, July 2011

Legal Rights

Electronic Emission Notices

This device complies with Part 15 of the FCC rules.

Operation is subject to the following two conditions:

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

FCC Radio Frequency Interference Statement

The WB-B equipment has been tested and found to comply with the limits for a class B digital device, pursuant to part 15 of the FCC rules and to ETSI EN 301 489-1 rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential environment notwithstanding use in commercial, business and industrial environments. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

FCC Radiation Hazard Warning

To comply with FCC RF exposure requirement in section 1.1307, the antenna used for this transmitter must be fixed-mounted on outdoor permanent structures with a separation distance of at least 2 meter from al persons for antennas with a gain up to 28 dBi.

Antenna Compliance Statement

This device has been tested and certified to operate with the list of antennas detailed in Table 1-2 (based on the local regulations). It is hereby expressly clarified that installation and usage of any other antennas shall be under the sole responsibility and liability of the client. It is the responsibility of the client to assure that such installation and usage is in full compliance with the applicable local laws and regulations, including without limitation with respect to the maximum permitted radiated power. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the Equivalent Isotropically Radiated Power (EIRP) is not more than that permitted for successful communication.

R&TTE Compliance Statement

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

Safety Considerations

For the following safety considerations, "Instrument" means the WB-B system's components and their cables.

Caution

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

Line Voltage

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

Radio

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

Outdoor Unit and Antenna Installation and Grounding

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

Disposal of Electronic and Electrical Waste



Disposal of Electronic and Electrical Waste

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

About this Manual

This manual describes the WB-B Point-to-Point Wireless Bridge and how to install, operate and manage the system components.

This manual is intended for technicians responsible for installing, setting up and operating the WB-B system, and for system administrators responsible for managing the system.

This guide contains the following chapters and appendices:

- **Chapter 1 - System description:** Describes the WB-B system and its components.
- **Chapter 2 - Installation:** Describes how to install the system components.
- **Chapter 3 - Commissioning:** Describes how to configure basic parameters, align the antenna and validate unit operation.
- **Chapter 4 - Operation and Administration:** Describes how to use the WB-B Configuration Utility application for configuring parameters, checking system status and monitoring performance.
- **Appendix A - Software Version Loading Using TFTP:** Describes how to load a new software version using TFTP.
- **Appendix B - File Download and Upload Using TFTP:** Describes how to download and upload configuration files using TFTP. This procedure is also applicable for uploading country code and feature license files.
- **Appendix C - Using the Restore Link Parameters Utility:** Describes how to use the special Restore Link Parameters utility to enable management access to units where wrong or unknown configuration disables regular access to the unit for management purposes.
- **Appendix D - Preparing the indoor to outdoor cable:** Provides details on preparation of the indoor to outdoor Ethernet cable.
- **Appendix E - Parameters Summary:** Provides an at a glance summary of the configuration parameters, value ranges and default values.

Contents

Chapter 1 - System Description 1

1.1 Introducing WB-B 3

1.2 System Components 5

1.3 Management Systems 6

1.3.1 bwaCRAFT 6
1.3.2 bwaNMS 7

1.4 Specifications 8

1.4.1 Radio specifications 8
1.4.2 Data Communication 9
1.4.3 Configuration and Management 10
1.4.4 Physical and Electrical 11
1.4.5 Standards Compliance, General 13

Chapter 2 - Installation 14

2.1 Installation Requirements 16

2.1.1 Packing List (BU, RB) 16
2.1.2 Indoor-to-Outdoor Cables 17

2.2 Equipment Positioning Guidelines 19

2.3 Installing the Outdoor Unit 20

2.3.1 Pole Mounting the Outdoor Unit 20
2.3.2 Pole Mounting the BU/RB-B10 ODU 22
2.3.3 Protecting ODU Connections 26
2.3.4 Connecting the Grounding and Antenna Cables 27
2.3.5 Connecting the Indoor-to-Outdoor Cable 28

2.4 Installing the Universal IDU Indoor Unit 32

2.4.1 RESET Button Functionality 33

Chapter 3 - Commissioning 34

3.1 Configuring Basic Parameters 36

3.1.1 Initial Configuration 36

3.1.2 Country Code Selection 38
3.1.3 Transmit Power Compliance With Regulations 38
3.2 Using the Optional Y-cable (BU/RB-B10 ODU) 41
3.3 Aligning the Antennas 42
3.4 Configuring the Maximum Modulation Level 44
3.5 Operation Verification 46
3.5.1 Outdoor Unit Verification 46
3.5.2 Indoor Unit Verification 48
3.5.3 Verifying Data Connectivity 48
Chapter 4 - Operation 49
4.1 Working with the Monitor Program 51
4.1.1 Accessing the Monitor Program Using Telnet 51
4.1.2 Common Operations 52
4.2 Menus and Parameters 54
4.2.1 Main Menu 54
4.2.2 Info Screens Menu 54
4.2.3 Unit Control Menu 59
4.2.4 Basic Configuration Menu 75
4.2.5 Site Survey Menu 79
4.2.6 Advanced Configuration Menu 95
Appendix A - Software Version Loading Using TFTP 185
Appendix B - File Download and Upload Using TFTP 189
Appendix C - Using the Set Factory Defaults Utility 192
Appendix D - Preparing the Indoor to Outdoor Cable 194
Appendix E - Parameters Summary 197
E.1 Parameters Summary 199
E.1.1 Unit Control Parameters 199
E.1.2 IP Parameters 201
E.1.3 Air Interface Parameters 201
E.1.4 Network Management Parameters 206
E.1.5 Bridge Parameters 207
E.1.6 Performance Parameters 209

E.1.7 Service Parameters.....211
E.1.8 Security Parameters.....213

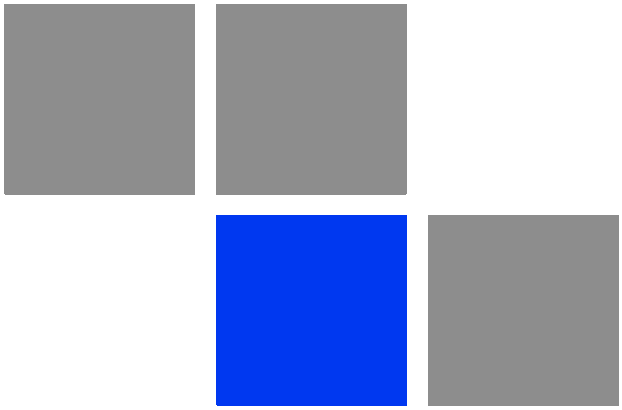
Figures

Figure 2-1: Threaded Holes/Grooves 21
Figure 2-2: 3" Pole Installation Using Special Clamps 21
Figure 2-3: Back View of the ODU of the BU/RB-B10 23
Figure 2-4: BU/RB-B10 ODU Pole Installation Using the Special Clamp, Vertical Polarization .. 24
Figure 2-5: BU/RB-B10 ODU Pole Installation Using the Special Clamp, Horizontal Polarization .. 25
Figure 2-6: BU/RB-B10 ODU Pole Installation Using the Tilt Accessory, Vertical Polarization ... 26
Figure 2-7: Bottom Panel of the Outdoor Unit (excluding B10 ODU), shown without the seal assembly) 28
Figure 2-8: Bottom Panel of the BU/RB-B10 ODU (without IDU COM Sealing Cap) 28
Figure 2-9: The Waterproof Seal 29
Figure 2-10: Inserting the IDU COM Cable into the Sealing Cap 30
Figure 2-11: Connecting the IDU COM connector and inserting the Sealing Cap 31
Figure 2-12: IDU PS 1073 Front Panel 32
Figure 3-1: Connecting the Y-cable 41
Figure 4-1: Main Menu (Administrator Level) 52
Figure D-1: Ethernet Connector Pin Assignments 195

Tables

Table 1-1: Frequency Bands 4
Table 1-2: Detached Antennas 5
Table 1-3: Radio Specifications 8
Table 1-4: Data Communication 9
Table 1-5: Configuration and Management 10
Table 1-6: Mechanical Specifications 11
Table 1-7: Connectors 12
Table 1-8: Ethernet Pin-Out Assignments 12
Table 1-9: Electrical Specifications 12
Table 1-10: Environmental Specifications 12
Table 1-11: Standards Compliance, General 13
Table 2-1: Approved Category 5E Ethernet Cables 17
Table 2-2: Ethernet Pin-Out Assignments 18
Table 3-1: Basic Parameters 36
Table 3-2: Regulation Maximum EIRP 39
Table 3-3: Recommended Maximum Modulation Level 45
Table 3-4: BU-ODU LEDs 46
Table 3-5: RB-ODU LEDs 47
Table 3-6: RB/BU-ODU SNR Bar LED Functionality (In Normal Mode) 47
Table 3-7: PS1073 IDU LEDs 48
Table 4-1: Default Passwords 51
Table 4-2: Parameters not changed after Set Complete Factory/Operator Defaults 62
Table 4-3: Parameters that are not changed after Set Partial Factory/Operator Defaults 63

Table 4-4: Threshold Target Value Ranges 75
Table 4-5: Authentication and Association Process 89
Table 4-6: DFS behavior on RBs using ETSI based country codes 103
Table 4-7: Comparison between DFS implementations for various country codes on the RB 104
Table 4-8: Enhanced ETSI Radar Detection Behavior 109
Table 4-9: VLAN Management Port Functionality 143
Table 4-10: VLAN Data Port Functionality - Access Link 144
Table 4-11: VLAN Data Port Functionality - Trunk Link 144
Table 4-12: VLAN Data Port Functionality - Hybrid Link 145
Table 4-13: VLAN Rule # Parameters 148
Table 4-14: Layer 2 Broadcast/Multicast Frames' Behavior 150
Table 4-15: Recommended Maximum Modulation Level* 158
Table 4-16: Basic Rate Mechanism 160
Table 4-17: Retransmission Percentage Equivalence 163
Table 4-18: Examples of Retransmissions on Different Modulation Levels 164
Table D-1: Cable Color Codes 195



Chapter 1

System Description

In This Chapter:

- "Introducing WB-B" on page 3
- "System Components" on page 5
- "Management Systems" on page 6
- "Specifications" on page 8

1.1 Introducing WB-B

WB-B is a high performance wireless bridge system that provides high-capacity, high-speed point-to-point links. The WB-B system utilizes advanced technologies to support optimal performance in spectrally polluted environments. WB-B products operate in Time Division Duplex (TDD) mode, using Orthogonal Frequency Division Multiplexing (OFDM) modulation with Forward Error Correction (FEC) coding. Using the enhanced multi-path resistance capabilities of OFDM modem technology, WB-B enables operation in near and non-line-of-sight (NLOS) environments. These qualities enable service providers to reach a previously inaccessible and broader segment of the subscriber population. The system also features adaptive modulation for automatic selection of modulation schemes, including BPSK, QPSK, 16 and 64 QAM to maximize data rate and improve spectral efficiency.

Where allowed by applicable radio regulations, WB-B supports the use of 40 MHz frequency channels. When using 40 MHz channels, the WB-B is operating in the "Turbo Mode". The use of this "Turbo Mode" increases the net throughput of the WB-B link, especially for links that suffer from low net throughput due to challenging link budget conditions that result from very long link distances, RF absorbing terrain or non line of sight. Alternatively, the Turbo Mode can extend the range of the WB-B while the capacity is maintained constant.

WB-B supports sensitive applications through optional use of authentication and/or data encryption utilizing WEP or AES algorithm with 128 bit keys. FIPS (Federal Information Processing Standards) 197 certified encryption algorithm is available free of charge for unit with HW Revision C or higher.

The wireless link prioritization feature fully supports delay sensitive applications, enabling Multimedia Application Prioritization (MAP) for high performance voice and video.

The system supports Virtual LANs based on IEEE 802.1Q, enabling secure operation and Virtual Private Network (VPN) services and enabling tele-workers or remote offices to conveniently access their enterprise network. The system supports layer-2 traffic prioritization based on IEEE 802.1p and layer-3 traffic prioritization based on either IP ToS Precedence (RFC791) or DSCP (RFC2474). It also supports traffic prioritization based on UDP and/or TCP port ranges.

WB-B products are currently available in the following frequency bands:

Table 1-1: Frequency Bands

Band	Frequencies (GHz)
5.2	5.150 - 5.350
5.3	5.250 - 5.350
5.4	5.470 - 5.725
5.8	5.725 - 5.875
2.4	2.400 - 2.4835

The available frequencies, as well as other parameters, depend on applicable local regulations. The actual operating frequencies used by the system can be configured according to applicable radio regulations and specific deployment considerations.

WB-B system components can be managed using standard management tools through SNMP agents that implement standard and proprietary MIBs for remote setting of operational modes and parameters. The bwaCRAFT utility is an SNMP-based application designed to manage WB-B system components and upgrade unit software versions. The system administrator can use the management utility to control any number of units from a single location.

1.2 System Components

The WB-B system includes a Base Unit (BU), typically installed at the main site, and a Remote Bridge (RB).

NOTE



To simplify logistic operations, all units are supplied as Base Units. When necessary, the functionality of each unit can be changed from Base Unit to Remote Bridge, and vice versa.

Each unit comprises a desktop or wall-mountable Universal Indoor Unit (IDU) and an outdoor unit (ODU). The IDU provides the interface to the user's equipment and is powered from the 110/220 VAC mains. The customer's data equipment is connected via a standard IEEE 802.3 Ethernet 10/100BaseT (RJ 45) interface. The indoor unit is connected to the outdoor unit via a Category 5E Ethernet cable. This cable carries Ethernet traffic between the indoor and the outdoor units, and also transfers power (54 VDC) and control from the indoor unit to the outdoor unit.

Several system models are available: The basic level WB-B10 system (comprising a BU-B10 Base Unit and an RB-B10 Remote Bridge, currently available only in the 5.4 and 5.8 GHz bands), the entry level, medium throughput WB-B14 system (comprising a BU-B14 Base Unit and an RB B14 Remote Bridge), the high throughput WB-B28 system (comprising a BU-B28 Base Unit and an RB B28 Remote Bridge), and the WB-B100 system (comprising a BU-B100 Base Unit and an RB-B100 Remote Bridge) which can deliver a very high throughput. All WB-B systems also support prioritization in the wireless link to better support delay sensitive applications. In addition, support of FIPS (Federal Information Processing Standards) 197 certified encryption algorithm is available free of charge for units with HW Revision C or higher.

The ODU contains the processing and radio modules and are available either with an integral flat antenna or with a connection to a detached antenna (D models). Availability of detached antenna in certain regions many depend on the relevant radio regulations. Currently available detached antennas include the following:

Table 1-2: Detached Antennas

Antenna	Band (GHz)	Horizontal Beam Width	Gain
UNI-23-9	5.150 - 5.875	9°	23 dBi
UNI-28-4	5.150 - 5.875	4.5°	28 dBi
UNI-24-SC	2.400 - 2.500	6°	24 dBi

1.3 Management Systems

The end-to-end IP-based architecture of the system enables full management of all components, from any point in the system. The devices can be managed using standard management tools through SNMP agents that implement standard and proprietary MIBs for remote setting of operational modes and parameters. The same SNMP management tools can also be used to manage other system components including switches, routers and transmission equipment. Security features incorporated in the units restrict access for management purposes to specific IP addresses and/or directions, that is, from the Ethernet and/or wireless link.

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

1.3.1 bwaCRAFT

bwaCRAFT is an SNMP (Simple Network Management Protocol) application designed for on-line management of system components. This utility simplifies the installation and maintenance of small size installations by easily enabling the change of settings or firmware upgrade for one unit or an entire sector at a time.

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

- Device Manager for the selected Unit
- Selected unit or a complete sector configuration modification
- Firmware upgrade for a single unit or an entire sector
- On-line performance data monitoring
- Export of configuration details to a CSV file
- Support for Telnet cut-through to the managed devices and http cut-through to Gateways or Wi^2 APs behind connected SUs.

1.3.2 bwaNMS

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

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

bwaNMS provides the following BWA network management functionality:

- Device Discovery
- Device Inventory
- Topology
- Fault Management
- Configuration Management
- Data Collection
- Performance Monitoring
- Device embedded Software Upgrade
- Security Management
- Northbound interface to other Network Management Systems.

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

1.4 Specifications

1.4.1 Radio specifications

Table 1-3: Radio Specifications

Item	Description
Frequency[1]	5.2 GHz Family: 5.150 - 5.350 GHz 5.3 GHz Family: 5.250 - 5.350 GHz 5.4 GHz Family: 5.470 - 5.725 GHz 5.8 GHz Family: 5.725 - 5.875 GHz 2.4 GHz Family: 2400 - 2.483.5GHz
Operation Mode	Time Division Duplex (TDD)
Channel Bandwidth[1]	10, 20, 40 (Turbo Mode) MHz
Central Frequency Resolution	10 MHz, 5 MHz in units with HW Revision C and higher when using a 10 MHz bandwidth.
5 GHz ODU Integral Antenna excluding BU/RB-B10)	21 dBi in the 5.150 5.875 GHz band. 10.5° horizontal x 10.5° vertical, vertical polarization, compliant with ETSI EN 302 326-3 V1.2.1 (2007-01)
BU/RB-B10 ODU Integral Antenna (5.4/5.8 GHz)	20 +/- 1 dBi typical in the 5.250 5.875 GHz band, 14° AZ x 14° EL, vertical/horizontal polarization, compliant with ETSI EN 302 326-3 V1.2.1 (2007-01), RoHS
2.4 GHz ODU Integral Antenna	16 dBi in the 2.400 2.700 GHz band. 20° horizontal x 20° vertical, vertical polarization, compliant with ETSI EN 302 326-3 V1.2.1 (2007-01)
5 GHz Detached Antennas[2]	■ UNI-23-9: 23 dBi, 5.150-5.875 GHz, 9° horizontal x 9° vertical, vertical polarization, compliant with ETSI EN 302 326-3 V1.2.1 (2007-01) ■ UNI-28-4: 28 dBi, 5.150-5.875 GHz, 4.5° horizontal x 4.5° vertical, vertical polarization, compliant with ETSI EN 302 326-3 V1.2.1 (2007-01)
2.4 GHz Detached Antenna	UNI-24-SC: 24 dBi, 2.400-2.500 GHz, 6° horizontal x 10° vertical, vertical polarization
Antenna Port (D-model ODU)	N-Type, 50 Ohm
Max. Input Power (at antenna port)	-30 dBm typical

Table 1-3: Radio Specifications

Item	Description		
Maximum Output Power[3]	21 dBm.		
Sensitivity, Minimum (dBm at antenna port, PER<10%, 20 MHz bandwidth[4])	Modulation Level[5]	Sensitivity	Minimum SNR
	1	-89 dBm	6 dB
	2	-88 dBm	7 dB
	3	-86 dBm	9 dB
	4	-84 dBm	11 dB
	5	-81 dBm	14 dB
	6	-77 dBm	18 dB
	7	-73 dBm	22 dB
	8	-71 dBm	23 dB
Modulation	OFDM modulation, 64 FFT points; BPSK, QPSK, QAM16, QAM64		

[1] The actual available frequency channels and bandwidth are defined by the selected Sub-Band, which reflects the applicable regulatory constraints. For more details refer to Section 4.2.2.4 .

[2] In 5.4 GHz units with a detached antenna, if the gain of the antenna (as inserted into Antenna gain field) is higher than 30 dBm, then the Maximum EIRP can vary by more than +/-3 dB. As regulations in most countries limit the EIRP of units operating in the 5.4 GHz band, it is recommended to use detached antennas up to and including 28 dBi.

[3] The actual available maximum output power for each modulation level is defined by the selected Sub-Band, which reflects the applicable regulatory constraints. For some countries the power may also be limited by limitations on the maximum EIRP (also included in the Sub-Band parameters) and the Antenna Gain parameter. For more details refer to Section 4.2.2.4 and to Section 4.2.6.2.8.1.

[4] The sensitivity values are for a bandwidth of 20 MHz. When using a 40 MHz bandwidth ("Turbo mode"), the Sensitivity for each modulation level is higher by 3 dB higher. For 10 MHz bandwidth the sensitivity is lower by 3 dB.

[5] Modulation Level indicates the radio transmission rate and the modulation scheme. Modulation Level 1 is for the lowest radio rate and modulation scheme.

1.4.2 Data Communication

Table 1-4: Data Communication

Item	Descriptions
Standard compliance	IEEE 802.3 CSMA/CD
VLAN Support	Based on IEEE 802.1Q
Layer 2 Traffic Prioritization	Based on IEEE 802.1p

Table 1-4: Data Communication

Item	Descriptions
Layer 3 Traffic Prioritization	■ IP Precedence ToS (RFC791) ■ DSCP (RFC2474) ■ Source/destination IP address
Layer 4 Traffic Prioritization	UDP/TCP destination ports

1.4.3 Configuration and Management

Table 1-5: Configuration and Management

Item	Description
Management	■ Via Telnet ■ SNMP based Configuration Utility ■ Configuration upload/download
Management Access	From Wired LAN, Wireless Link
Management access protection	■ Multilevel password ■ Configuration of remote access direction (from Ethernet only, from wireless link only or from both) ■ Configuration of IP addresses of authorized stations
Security	■ Authentication messages encryption option ■ Data encryption option ■ WEP or AES OCB 128-bit encryption algorithms ■ FIPS 197 certified encryption (for units with HW revision C or higher) ■ ESSID and Hidden ESSID
SNMP Agents	SNMP ver 1 client, MIB II, Bridge MIB, Private MIB
Allocation of IP parameters	Configurable or automatic (DHCP client)
Software upgrade	■ FTP ■ TFTP

Table 1-5: Configuration and Management

Item	Description
Configuration upload/download	■ FTP ■ TFTP

1.4.4 Physical and Electrical

1.4.4.1 Mechanical

Table 1-6: Mechanical Specifications

Unit	Structure	Dimensions (cm)	Weight (kg)
General	An IDU indoor unit and an ODU outdoor unit		
IDU PS1073	Plastic box (black), desktop or wall mountable	14 x 6.6 x 3.5	0.3
5 GHz ODU with Integral Antenna	Metal box plus an integral antenna in a cut diamond shape in a plastic enclosure, poll or wall mountable	43.2 x 30.2 x 5.9	2.9
BU/RB-B10 ODU (5.4/5.8 GHz)	Diamond shaped metal box plus an integral antenna in a plastic enclosure, pole or wall mountable	22 x 22 x 7	1.3
2.4 GHz ODU with Integral Antenna	Metal box plus an integral antenna in a plastic enclosure, poll or wall mountable	30.5 x 30.5 x 6.2	3.3
ODU with a Connection to a Detached Antenna	Metal box, pole or wall mountable	30.6 x 12.0 x 4.7	1.85
UNI-23-9	A pole mountable antenna includes a mounting bracket supporting +/- 22.5° tilt and a 1.5m LMR 400 cable.	30.5 x 30.5 x 2.5	1.5
UNI-28-4	A pole mountable antenna includes a mounting bracket supporting +/- 22.5 tilt and a 1.5m LMR 400 cable.	60 x 60 x 5.5	5
UNI-24-SC	A 1"-2" pole mountable parabolic antenna includes a mounting bracket supporting +/- 30 tilt in 10 increments and a 0.6m cable.	61 x 99 x 38	2.45

1.4.4.2 Connectors

Table 1-7: Connectors

Unit	Connector	Description
IDU	ETHERNET	10/100BaseT Ethernet (RJ-45) with 2 embedded LEDs. Cable connection to a PC: crossed Cable connection to a hub: straight
	RADIO	10/100BaseT Ethernet (RJ-45): Ethernet + power for outdoor connection over a CAT-5 shielded cable
	AC IN	3 pin AC power plug
ODU (excluding BU/RB-B10)	INDOOR	10/100BaseT Ethernet (RJ-45), protected by a waterproof sealing assembly
	ANT (D models)	N-Type jack, 50 ohm, lightning protected
BU/RB-B10 ODU (5.4/5.8 GHz)	IDU COM	10/100BaseT Ethernet (RJ-45), protected by a sealing cap

Table 1-8: Ethernet Pin-Out Assignments

Radio	Power
Pins: 4 & 7 Power (+) 5 & 8 Power (-)	56V

1.4.4.3 Electrical

Table 1-9: Electrical Specifications

Unit	Details
General	Power consumption: 25W
IDU	AC power input: 85-265 VAC, 50-60 Hz
ODU	54VDC from the IDU over the indoor-outdoor Cat-5 shielded Ethernet cable

1.4.4.4 Environmental

Table 1-10: Environmental Specifications

Type	Unit	Details
Operating temperature	Outdoor units	-40° C to 55° C
	Indoor equipment	0° C to 40° C

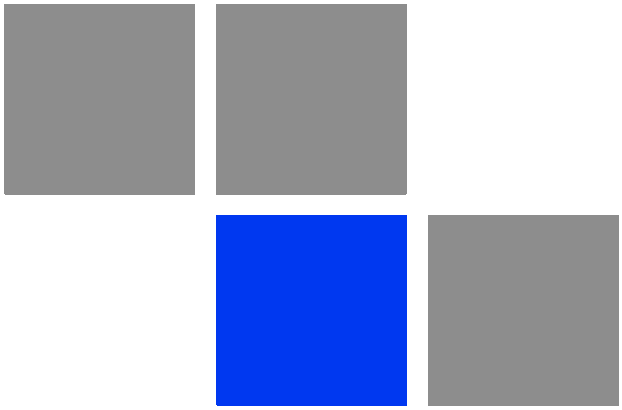
Table 1-10: Environmental Specifications

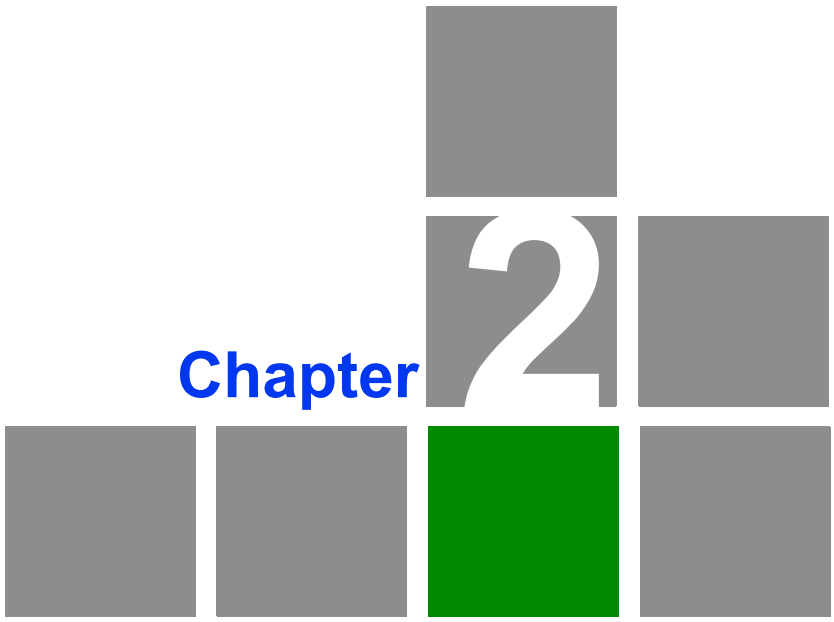
Type	Unit	Details
Operating humidity	Outdoor units	5%-95% non condensing, Weather protected
	Indoor equipment	5%-95% non condensing

1.4.5 Standards Compliance, General

Table 1-11: Standards Compliance, General

Type	Standard	
EMC	■ FCC Part 15 class B ■ ETSI EN 300 489-1	
Safety	■ UL 60950 ■ EN 60950	
Environmental	Operation	■ ETS 300 019 part 2-3 class 3.2E for indoor units ■ ETS 300 019 part 2-4 class 4.1E for outdoor units
	Storage	ETS 300 019-2-1 class 1.2E
	Transportation	ETS 300 019-2-2 class 2.3
Lightning protection	EN 61000-4-5, Class 3 (2kV)	
Radio	■ FCC Part 15.247 ■ ETSI EN 300 328 ■ ETSI EN 301 893 (2003-04)	





Chapter 2

Installation

In This Chapter:

- "Installation Requirements" on page 16
- "Equipment Positioning Guidelines" on page 19
- "Installing the Outdoor Unit" on page 20
- "Installing the Universal IDU Indoor Unit" on page 32

2.1 Installation Requirements

This section describes all the supplies required to install the WB-B system components and the items included in each installation package.

2.1.1 Packing List (BU, RB)

- IDU indoor unit with a wall mounting kit
- Mains power cord
- ODU outdoor unit with an integrated antenna
  Or
  ODU outdoor unit with a connection to a detached antenna (not included)
- Pole mounting kit for the ODU
- An IDU to ODU cable kit, including 20m Category 5E Ethernet cable with a shielded RJ-45 connector crimped on one end, a waterproof sealing assembly and two shielded RJ-45 connectors (not applicable for BU/RB-B10).

2.1.1.1 Additional Installation Requirements

The following items are also required to install the WB-B system:

- Detached Antenna* (for D model units), including a pole mounting kit and an RF cable
- Ethernet cable (straight for connecting to a hub/switch etc., crossed for connecting directly to a PC's NIC)
- For BU/RB-B10 (or for other units if the Indoor-to-Outdoor cable supplied with the equipment is not long enough) - Category 5 Ethernet cable with shielded RJ-45 connectors * (available in different lengths. For more details refer to Section 2.1.2)
- Crimping tool for RJ-45 connectors
- Ground cables with an appropriate termination

- Mains plug adapter or termination plug (if the power plug on the supplied AC power cord does not fit local power outlets)
- Portable PC with Ethernet card and bwaCRAFT * application and a crossed Ethernet cable
- Installation tools and materials, including appropriate means (e.g. a pole) for installing the outdoor equipment.

2.1.1.2 Optional Items*

- Tilt Pole Mounting kit for the smaller size ODU of BU/RB-B10 units
- A Y-cable for connecting directly to the IDU COM of the BU/RB-B10 ODU for configuration/performance monitoring using a portable PC.

NOTE



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

2.1.2 Indoor-to-Outdoor Cables

NOTE



The length of the Indoor-to-Outdoor Ethernet cable should not exceed 90 meters. The length of the Ethernet cable connecting the indoor unit to the user's equipment, together with the length of the Indoor-to-Outdoor cable, should not exceed 100 meters.

Use only Category 5E Ethernet cables from approved manufacturers, listed in Table 2-1. Consult with the Supplier's specialists on the suitability of other cables.

Table 2-1: Approved Category 5E Ethernet Cables

Manufacturer	Part Number
HES Cabling Systems www.hescs.com	H5E-00481

Table 2-1: Approved Category 5E Ethernet Cables

Manufacturer	Part Number
Southbay Holdings Limited 11th Fl., 15, Lane 347, Jong Jeng Rd. Shin Juang City, Taipei County Taiwan, R.O.C Attn: Eva Lin Tel. 886-2-2832 3339 Fax. 886-2-2206 0081 E-mail: eva@south-bay.com.tw	TSM2404A0D

Table 2-2: Ethernet Pin-Out Assignments

Radio	Power
Pins: 4 & 7 Power (+) 5 & 8 Power (-)	56V

NOTE



In case of missing information (product specifications, ordering information, etc.) regarding these products on the manufacturer's web site, it is highly recommended to contact the manufacturer's sales representative directly.

2.2 Equipment Positioning Guidelines

This section provides key guidelines for selecting the optimal installation locations for the various WB-B system components.

CAUTION



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

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

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

- The outdoor unit can be either pole or wall mounted. Its location should enable easy access to the unit for installation and testing.
- The higher the placement of the antenna, the better the achievable link quality.
- ODU units with a detached antenna (D model) should be installed as close as possible to the antenna (to ensure that the antenna's characteristics are not affected by the ODU the distance must be higher than 10 cm).
- The ODU with its integrated antenna (or the detached antenna) should be installed to provide a direct, or near line of sight with the antenna of the other side.
- The indoor equipment should be installed as close as possible to the location where the indoor-to-outdoor cable enters the building. The location of the indoor equipment should take into account its connection to a power outlet and the CPE.

2.3 Installing the Outdoor Unit

The following sections describe how to install the outdoor units, including pole mounting the ODU, and connecting the indoor-to-outdoor, grounding and RF cables.

NOTE

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

2.3.1 Pole Mounting the Outdoor Unit

NOTE

This section is not applicable for the smaller size ODU of BU/RB-B10 units. For details on pole mounting the BU/RB-B10 ODU refer to Section 2.3.2.

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

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

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

NOTE

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

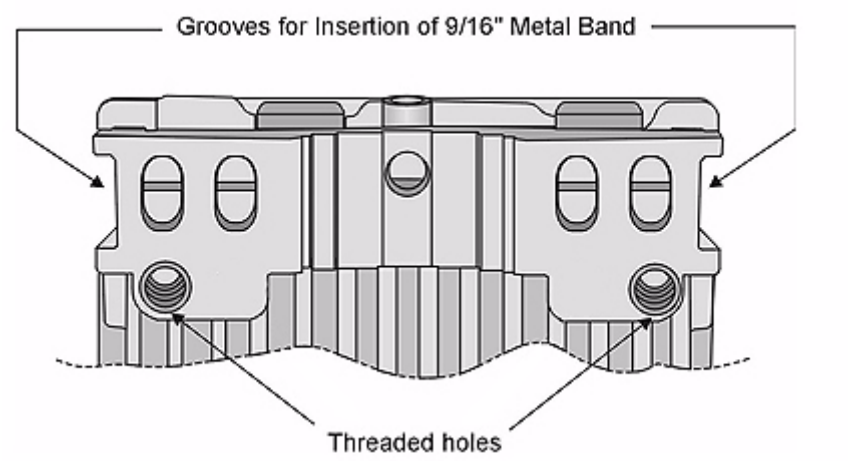


Figure 2-1: Threaded Holes/Grooves

Figure 2-2 illustrates the method of mounting an outdoor unit on a pole, using the clamps and threaded rods.

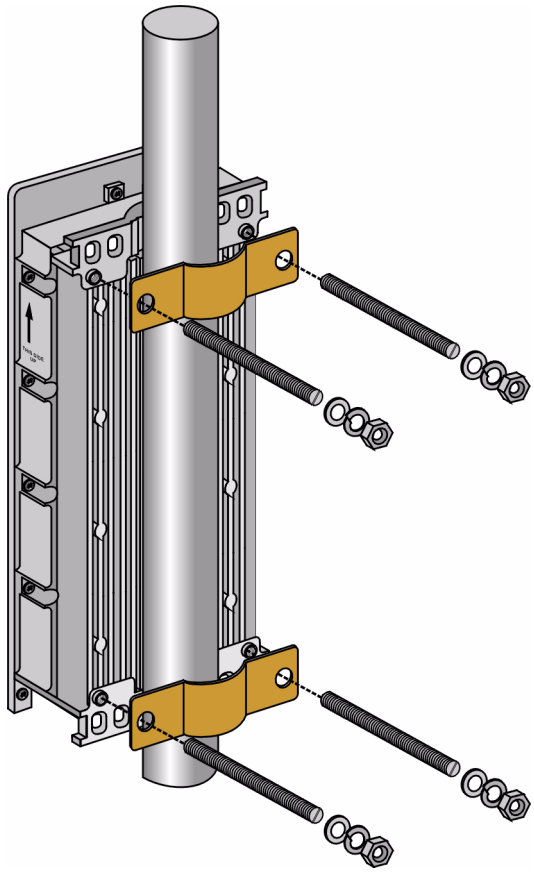


Figure 2-2: 3" Pole Installation Using Special Clamps

NOTE



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

2.3.2 Pole Mounting the BU/RB-B10 ODU

The ODU of the BU/RB-B10 can be mounted on a 1" to 4" pole using one of the following options:

- A pole mounting kit is supplied with each unit. The kit includes a special clamp and a pair of threaded rods, flat washers, spring washers and nuts. There are two pairs of threaded holes on the back of the unit, enabling to use the mounting kit for installing the unit using either vertical or horizontal polarization. The clamp enables installing the unit on diverse pole diameters from 1" to 4".

- A Tilt Pole Mounting kit, providing a tilt range of +/-15° is available from the Supplier. The Tilt kit can be attached to the ODU and be mounted on a 1" to 4" pole using two 9/16" wide metal bands.

2.3.2.1 Polarization

The ODU of the BU/RB-B10 can be pole mounted to provide either vertical or horizontal polarization.

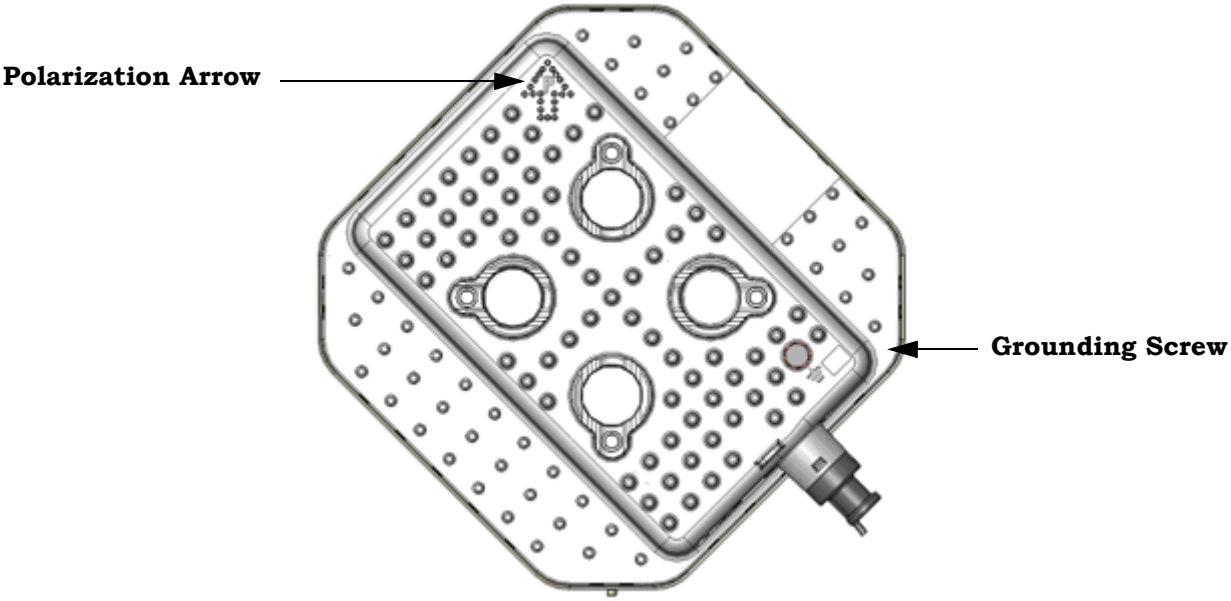


Figure 2-3: Back View of the ODU of the BU/RB-B10

The Polarization Arrow on the back of the unit indicates the type of polarization.

- For vertical polarization install the unit with the Polarization Arrow pointing upward (as in the figure above).
- For horizontal polarization install the unit with the Polarization Arrow pointing sideward and the connectors facing downward.

2.3.2.2 Pole Mounting the ODU Using the Clamp

Figure 2-4 and Figure 2-5 illustrate how to mount an ODU on a pole, using the clamp and threaded rods.

NOTE

There is a groove on one end of the threaded rod. Be sure to insert the threaded rods with the grooves pointing outward, and fasten them to the unit using a screwdriver. Install the unit with the bottom panel, which includes the connectors, facing downward.

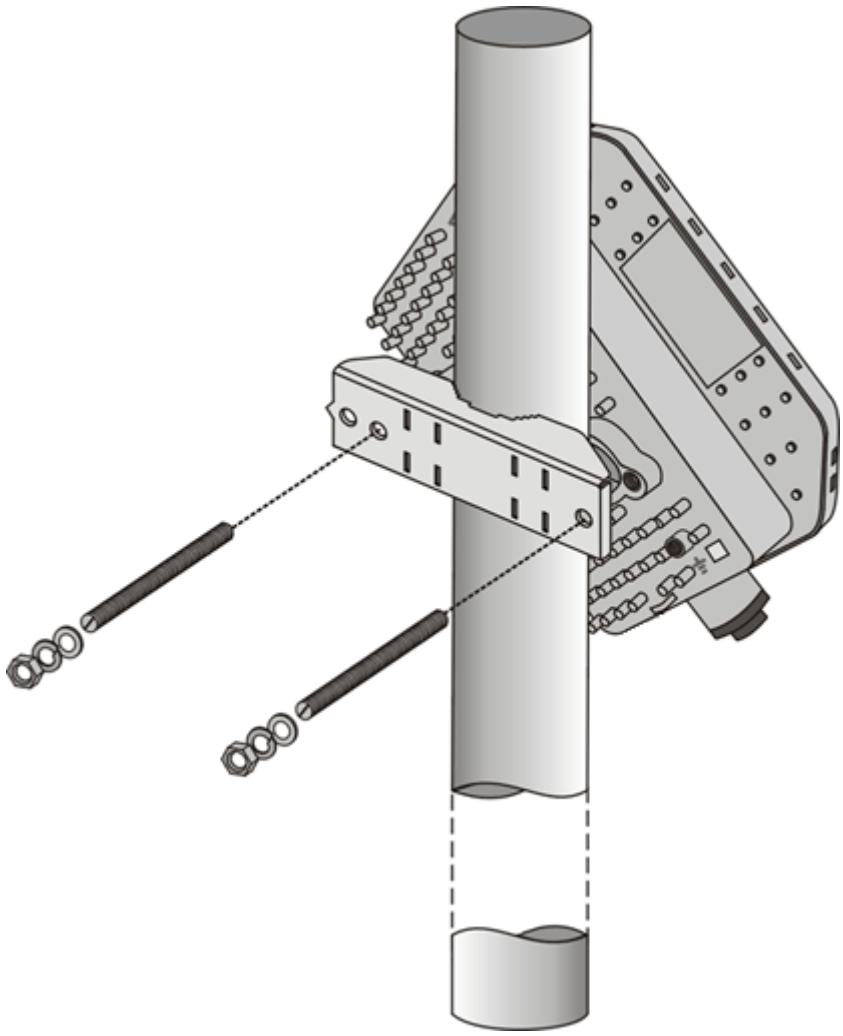


Figure 2-4: BU/RB-B10 ODU Pole Installation Using the Special Clamp, Vertical Polarization

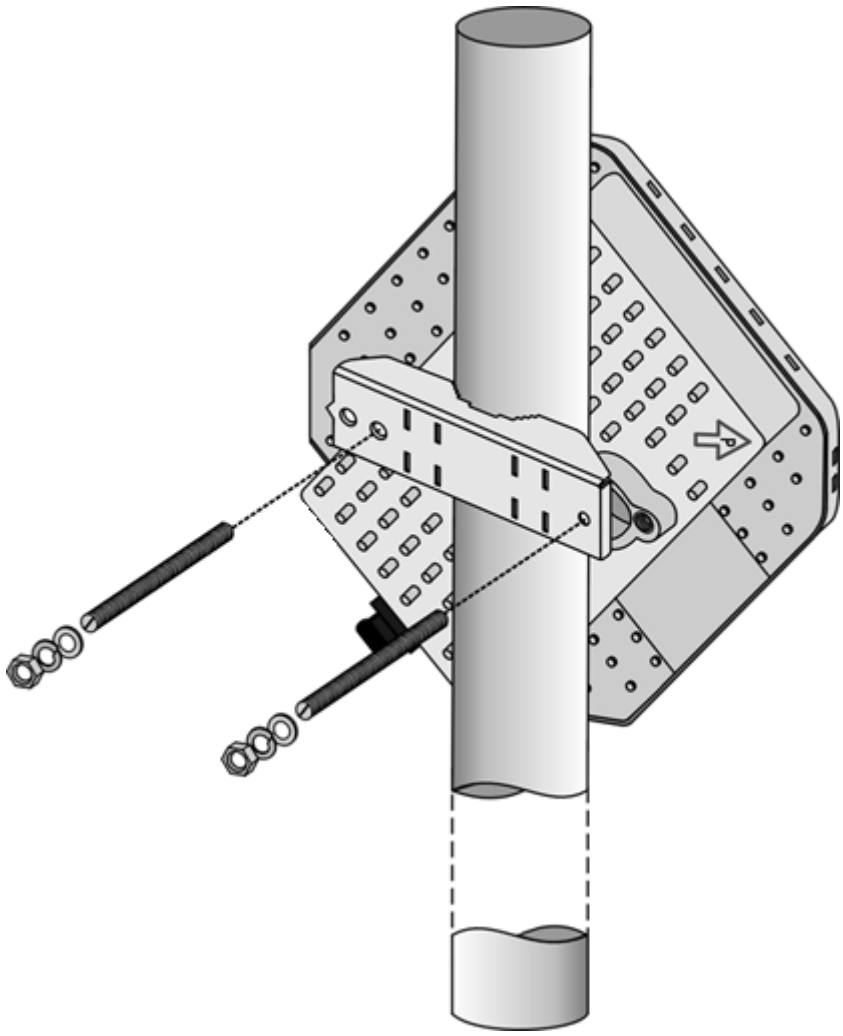


Figure 2-5: BU/RB-B10 ODU Pole Installation Using the Special Clamp, Horizontal Polarization

2.3.2.3 Pole Mounting the ODU with the Tilt Accessory

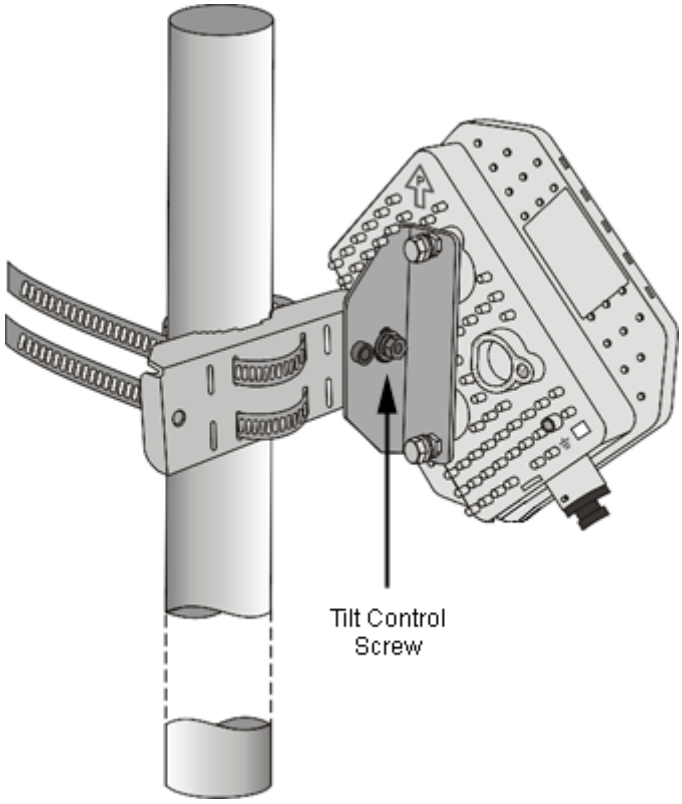


Figure 2-6: BU/RB-B10 ODU Pole Installation Using the Tilt Accessory, Vertical Polarization

To mount the ODU on a pole using the Tilt accessory:

1. Attach the Tilt accessory to the ODU using the two pairs of flat washers, spring washers and nuts supplied in the Tilt kit.
2. Mount the Tilt accessory on a 1" to 4" pole using two 9/16" metal bands.
3. Release slightly the Tilt Control Screw, tilt the ODU downward/upward as required, and re-tighten the screw.

2.3.3 Protecting ODU Connections

4Use appropriate sealing material to protect the connection against moisture and humidity. Use removable sealing material, such as a tar seal, to enable future access to the connector.

NOTE

Use high quality sealing material such as Scotch 130C Linerless Rubber Splicing Tape from 3M to ensure protection against dust and water.

Loop & tie the cable near the unit for strain relief and for routing water away from the unit: use additional cable strips to route the cable such that water can accumulate on the cable bends, away from the unit.

2.3.4 Connecting the Grounding and Antenna Cables

The Grounding screw (marked ⏚) is located on the bottom panel of the outdoor unit. The Antenna RF connector (marked Y) is located on the top panel of the D-model ODU.

To prepare the grounding cable:

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

To connect the RF cable (D model):

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

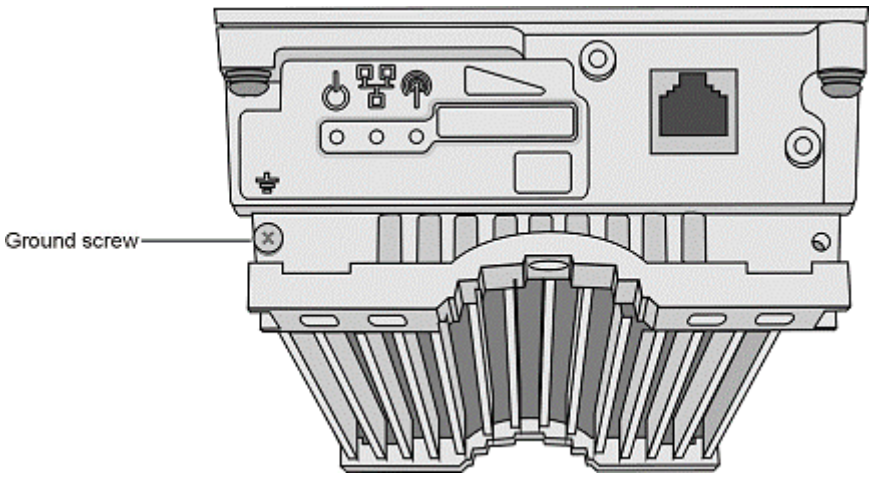


Figure 2-7: Bottom Panel of the Outdoor Unit (excluding B10 ODU), shown without the seal assembly)

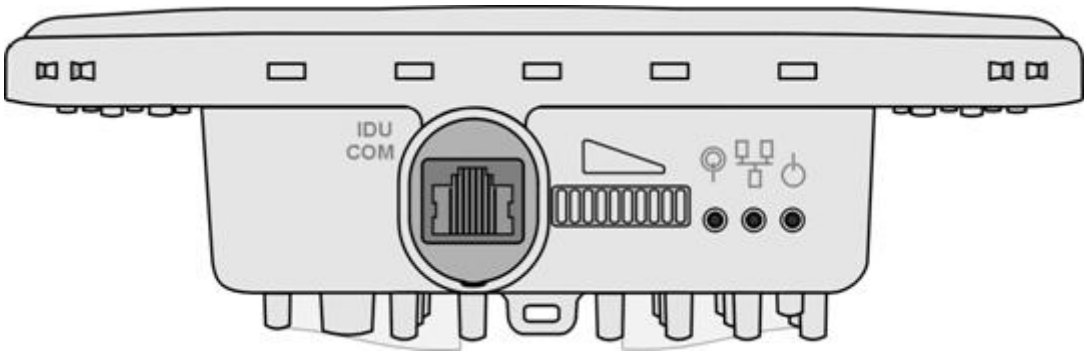


Figure 2-8: Bottom Panel of the BU/RB-B10 ODU (without IDU COM Sealing Cap)

NOTE

The MAC Address of the unit is marked on both the ODU and the IDU (on the bottom side of the unit). If for any reason the ODU is not used with the IDU with which it was shipped, the MAC Address of the system is in accordance with the marking on the ODU.

2.3.5 Connecting the Indoor-to-Outdoor Cable

2.3.5.1 Units with an Installed Waterproof Seal (not applicable for BU/RB-B10)

To connect the indoor-to-outdoor cable:

1 Remove the two screws holding the waterproof seal to the outdoor unit and remove the waterproof seal.

2 Unscrew the top nut from the waterproof seal.

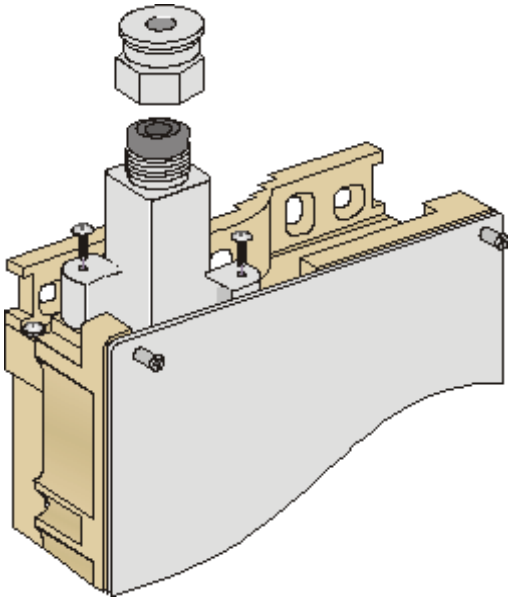


Figure 2-9: The Waterproof Seal

3 Route a straight Category 5E Ethernet cable (8-wire, 24 AWG) through both the top nut and the waterproof seal

NOTE

Use only Category 5E 4x2x24# FTP outdoor cables from an approved manufacturer. See list of approved cables and length limitations in Section 2.1.2.

4 Insert and crimp the RJ-45 connector. Refer to Appendix C for instructions on preparing the cable.

5 Connect the Ethernet cable to the outdoor unit RJ-45 connector.

6 Replace the waterproof seal and then the top nut. Make sure that the external jack of the cable is well inside the waterproof seal to guarantee a good seal.

7 Route the cable to the location selected for the indoor equipment.

8 Assemble an RJ-45 connector with a protective cover on the indoor end of the indoor-to-outdoor cable.

2.3.5.2 Units with a Waterproof Seal Supplied with the Ethernet Cable (not applicable for BU/RB-B10)

To connect the indoor-to-outdoor cable:

1. Verify that the o-ring supplied with the cable kit is in place.
2. Connect the RJ-45 connector of the Ethernet cable to the outdoor unit.
3. Attach the waterproof seal to the unit. Tighten the top nut.
4. Route the cable to the location selected for the indoor equipment.
5. Assemble an RJ-45 connector with a protective cover on the indoor end of the indoor-to-outdoor cable.
   See Appendix C for instructions on preparing the cable.

2.3.5.3 BU/RB-B10 ODU

1. The sealing cap has a special groove allowing to insert an ethernet cable with an already assembled RJ-45 connector through the cap. To expose the groove, lightly squeeze the cap. Carefully insert the cable with the assembled connector through the groove.

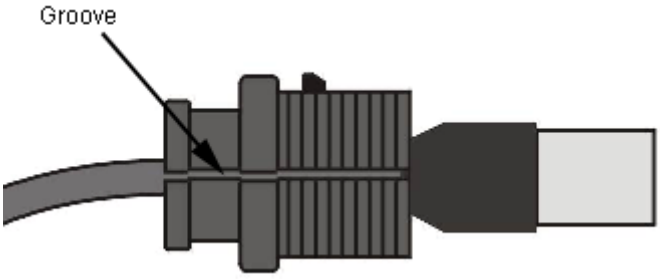


Figure 2-10: Inserting the IDU COM Cable into the Sealing Cap

2. Connect the Ethernet cable to the IDU COM RJ-45 connector.
3. Put the sealing cap back in its place. Make sure that the small protrusion on the side of the cap fits inside the hole on the connector's protective body.

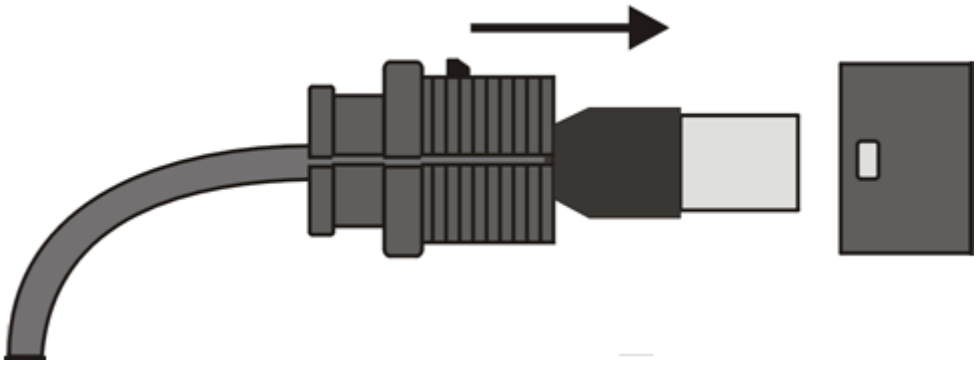


Figure 2-11: Connecting the IDU COM connector and inserting the Sealing Cap

4 Use appropriate sealing material to protect the connection against moisture and humidity. Use removable sealing material, such as a tar seal, to enable future access to the connector.

NOTE

Use high quality sealing material such as Scotch® 130C Linerless Rubber Splicing Tape from 3M to ensure protection against dust and water.

5 Loop & tie the cable near the unit for strain relief and for routing water away from the unit: use additional cable strips to route the cable such that water can accumulate on the cable bends, away from the unit.

6 Route the cable to the location selected for the indoor equipment.

7 Assemble a shielded RJ-45 connector with a protective cover on the indoor end of the IDU-ODU cable. See Appendix D for instructions on preparing the cable.

2.4 Installing the Universal IDU Indoor Unit

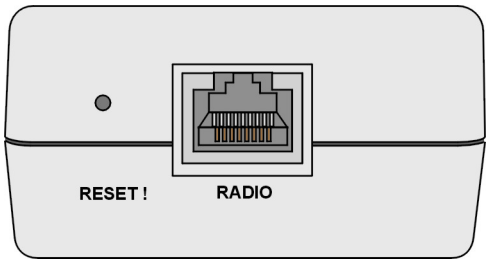


Figure 2-12: IDU PS 1073 Front Panel

The RADIO connector and RESET button are located on the front panel, the ETHERNET connector is located on the side panel and LEDs are located on the top panel.

CAUTION

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

To install the IDU:

1 Connect the Indoor-to-Outdoor cable to the RADIO connector, located on the front panel of the indoor unit.

2 Connect the power cord to the unit's AC socket, located on the rear panel. Connect the other end of the power cord to the AC mains. The unit can operate with AC mains of 100-240 VAC, 50-60 Hz.

NOTE

The color codes of the power cable are as follows:

Brown	Phase	~
Blue	Neutral	0
Yellow/Green	Ground	⏚

3 Verify that the POWER LED (located on the top panel of the PS1073 IDU) is lit, indicating that power is supplied to the unit.

4 Configure the basic parameters as described in Section 3.1.

5 Connect the 10/100 BaseT ETHERNET connector (located on the side panel of the PS1073 IDU) to the network. The cable connection should be a straight Ethernet if connecting the indoor unit to a hub/switch and a crossed cable if connecting it directly to a PC Network Interface Card (NIC).

NOTE



The length of the Ethernet cable connecting the indoor unit to the user's equipment, together with the length of the Indoor-to-Outdoor cable, should not exceed 100 meters.

2.4.1 RESET Button Functionality

Using a sharp object, press the recessed RESET push button for a short time to reset the unit and reboot from the Main version.

In units with ODU HW revision C or higher, the RESET button can be used for setting the unit to its factory defaults. Press the button for at least 5 seconds (until the ETH LED of the IDU stops blinking): the unit will reboot with the factory default configuration.

Chapter 3

Commissioning

In This Chapter:

- "Configuring Basic Parameters" on page 36
- "Using the Optional Y-cable (BU/RB-B10 ODU)" on page 41
- "Aligning the Antennas" on page 42
- "Configuring the Maximum Modulation Level" on page 44
- "Operation Verification" on page 46

3.1 Configuring Basic Parameters

3.1.1 Initial Configuration

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

Refer to Section 4.1 for information on how to access the Monitor program using Telnet.

The Basic Configuration menu in the Monitor program includes all the parameters necessary for the initial installation and operation of WB-B units. In many installations, most of these parameters should not be changed from their default values. The basic parameters and their default values are listed in Table 3-1.

Refer to Section 4.2 for detailed information on the applicable parameters.

NOTE



For compliance with ETSI regulations, the bandwidth used in the default Sub Band for units in the 5.4 GHz band is 20 MHz. The use of a Sub Band with a 40 MHz bandwidth (Turbo Mode) in the 5.4 GHz band is allowed only if approved by the applicable local regulatory administration.

Table 3-1: Basic Parameters

Parameter	Default Value	Comment
Change Unit Type to RB (in Unit Control Menu)		If necessary. Reset before continuing with configuration.
Ethernet Port Negotiation Mode (in Unit Control Parameters)	Auto Negotiation	
IP Address	10.0.0.1	
Subnet Mask	255.0.0.0	
Default Gateway Address	0.0.0.0	
DHCP Options	Disable	
Access to DHCP	BU: From Ethernet Only RB: From Wireless Only	
ESSID	ESSID1	

Table 3-1: Basic Parameters

Parameter	Default Value	Comment
Hidden ESSID Option (BU)	Disable	
Hidden ESSID Support (RB)	Disable	
Operator ESSID Option (BU)	Enable	
Operator ESSID (BU)	ESSID1	Applicable only if Operator ESSID Option is set to Enable.
Country Code Select	Depends on factory configuration	Applicable only for 5.4 and 5.8 GHz units. See Section 3.1.2 below.
Sub Band Select (BU)	1	Applicable only if more than one Sub Band is available.
Frequency (BU)	The lowest frequency in the selected Sub Band	
User Defined Frequency Subsets (RB)	A (All)	The list of frequencies is in accordance with the Sub Band.
DFS Required By Regulation (if DFS is supported by Country Code)	Depends on Country Code	
Frequency Subset Definition (BU, if DFS is supported)	All frequencies	Applicable only if DFS is enabled
DFS Detection Algorithm (for Universal Country Code in 5.4 or 5.8 GHz band)	ETSI	Applicable only if DFS is enabled
Transmit Power	Dependent on unit type and Sub Band	Transmit Power in RB cannot be higher than the Maximum Tx Power parameter
Maximum Tx Power (RB)	Dependent on Sub Band	Maximum Tx Power cannot be higher than the upper limit according to the Sub Band in use.
Tx Control (BU)	On	
Antenna Gain	Depends on unit type and Sub Band	If set to "Not Set Yet", must be configured according to actual value, taking into account cable's attenuation.
ATPC Option	Enable	
Best BU Support (RB)	Disable	
Preferred BU MAC Address (RB)	00-00-00-00-00-00 (none)	Applicable only when Best BU Support is enabled
Link Distance Mode (BU)	Automatic	

Table 3-1: Basic Parameters

Parameter	Default Value	Comment
Maximum Link Distance (BU)	0 (No Compensation)	
Maximum Modulation Level	8 (or the highest value supported according to the country code).	Refer to Section 3.4
Wi2 IP Address (RB)	0.0.0.0 (none)	
VLAN ID-Management	65535	
Authentication Algorithm	Open System	Availability of security parameters depends on support according to the Country Code.
Data Encryption Option	Disable	
Security Mode	WEP	
Default Key (RB)	Key 1	
Key 1 to Key 4	00……0 (32 zeros, meaning no key)	

NOTE

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

3.1.2 Country Code Selection

CAUTION

The selected Country Code must comply with applicable local radio regulations.

3.1.3 Transmit Power Compliance With Regulations

CAUTION

In regions where local radio regulations limit the maximum transmit power of the unit the installer is responsible to properly set the Antenna Gain parameter (if configurable) according to the actual antenna being used. This will limit the upper limits of the Tx Power parameter in the BU and the Maximum Tx Power in the RB (where applicable) to the value of "Permitted EIRP-Antenna Gain".

The Tx Power parameter in the BU and the Maximum Tx Power in the RB (where applicable) should not exceed the Permitted EIRP-Antenna Gain, according to the following table:

Table 3-2: Regulation Maximum EIRP

Country Code	Maximum EIRP (dBm)
FCC 5.3 GHz	30 for 20 and 40 MHz bandwidth, 27 for 10 MHz bandwidth (NOTES 1, 2, 3)
FCC 5.4 GHz	30 for 20 and 40 MHz bandwidth, 27 for 10 MHz bandwidth
ETSI 5.4 GHz	30 for 20 and 40 MHz bandwidth, 27 for 10 MHz bandwidth
ETSI-F 5.4 GHz	30 for 20 and 40 MHz bandwidth, 27 for 10 MHz bandwidth
Australia 5.4 GHz	30 for 20 and 40 MHz bandwidth, 27 for 10 MHz bandwidth
Universal 5.4 GHz	49
UK 5.8 GHz	36 for 20 and 40 MHz bandwidth, 33 for 10 MHz bandwidth
Australia 5.8 GHz	36
India 5.8 GHz	36
Germany 5.8 GHz	36 for 20 and 40 MHz bandwidth, 33 for 10 MHz bandwidth
ETSI 2.4 GHz	20 for 20 and 40 MHz bandwidth, 17 for 10 MHz bandwidth

NOTE 1 (FCC 5.3 GHZ, 20 MHz Bandwidth):

For full compliance with FCC regulations, the following requirements should be followed in units using a 20 MHz bandwidth:

1 In units HW Revision B, if you wish to include frequency channel 5270 MHz in the set of frequencies to be used, then the Transmit Power parameter in the BU, and the Maximum Tx Power parameter in the RB, should not be set to a value above "17-Antenna Gain". If there is a need to use a higher value for these parameters, this frequency should not be used.

2 In units with HW Revision C, if you wish to include one or more of frequency channels 5270, 5275 and 5330 MHz in the set of frequencies to be used, then the Transmit Power parameter in the BU, and the Maximum Tx Power parameter in the RB, should not be set to a value above "20-Antenna Gain". If there is a need to use a higher value for these parameters, this frequency should not be used.

NOTE 2 (FCC 5.3 GHZ, 40 MHz Bandwidth):

For full compliance with FCC regulations, the following requirements should be followed in units using a 40 MHz bandwidth:

1. In units with HW Revision B, Frequency channels 5270 and 5280 MHz should not be used.
2. In units with HW rev C, if you wish to include frequency channel 5290 MHz in the set of frequencies to be used, then the Transmit Power parameter in the BU, and the Maximum Tx Power parameter in the RB, should not be set to a value above "25-Antenna Gain". If there is a need to use a higher value for these parameters, this frequency should not be used.
   If you wish to include frequency channel 5310 MHz in the set of frequencies to be used, then the Transmit Power parameter in the BU, and the Maximum Tx Power parameter in the RB, should not be set to a value above "29-Antenna Gain". If there is a need to use a higher value for these parameters, this frequency should not be used.

NOTE 3 (FCC 5.3 GHZ, 10 MHz Bandwidth):

For full compliance with FCC regulation of units with HW rev C using a 10 MHz bandwidth, if you wish to include frequency channel 5265 MHz in the set of frequencies to be used, then the Transmit Power parameter in the BU, and the Maximum Tx Power parameter in the RB, should not be set to a value above "25-Antenna Gain". If there is a need to use a higher value for these parameters, this frequency should not be used.

3.2 Using the Optional Y-cable (BU/RB-B10 ODU)

A special Y-cable, available from the supplier enables to connect a a portable PC directly to the IDU COM port of the BU/RB-B10 ODU. This enables the installer to perform the entire process of configuring basic parameters, aligning the antenna and verifying proper operation of the unit right after completing the installation, minimizing the number of times the installer must climb to the roof. It also enables simpler configuration/performance monitoring during various maintenance/testing actions.

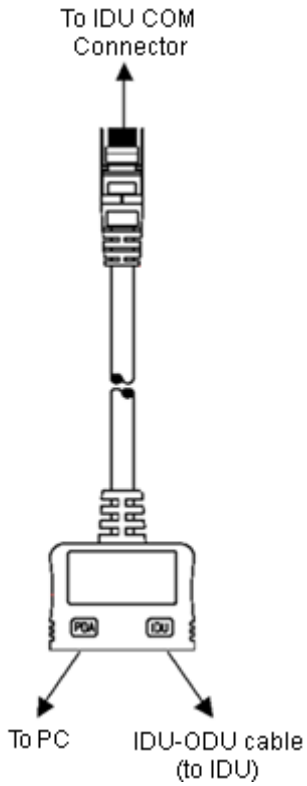


Figure 3-1: Connecting the Y-cable

3.3 Aligning the Antennas

An SNR bar display is located on the bottom panel of the ODU. The ten LEDs indicate the quality of the received signal. The higher the number of green LEDs indicating On, the higher the quality of the received signal. This section describes how to align the antennas using the SNR bar display.

NOTE



The behavior described above for the bar is called Normal Mode and is enabled by default. However, the LEDs' behavior can be customized by the user (see "LED Mode" on page 74). If this is the case, make sure that Normal Mode is enabled prior to aligning the antenna.

For optimal alignment, it is recommended to use the Continuous Average SNR/RSSI Display option (see Section 4.2.5.3.1). It is recommended to also verify the quality of the uplink using the Continuous Uplink Quality Indicator Display option (see Section 4.2.5.3.3) when there is traffic in the uplink.

NOTE



Antenna alignment using the SNR bar display or the Continuous Average SNR/RSSI Display is possible only after the RB is associated with a BU. Both units must be operational and configured with the correct basic parameters. Otherwise, the unit will not be able to synchronize with the BU. As the SNR measurement is performed on received frames, its results are meaningless unless the RB is associated with a BU.



To align the antenna:

1. Point the antenna of the BU (integrated into the front side of the ODU unit, or detached) towards the direction of the RB, and vice versa.
2. Verify that the power indication of the units is **On**.
3. Verify that the W LINK LED of the ODUs is on, indicating wireless link connectivity. If the W-LINK LED is off, check that the ESSID and Frequency parameters are correctly configured.
4. Rotate the antenna of the RB-ODU until the maximum SNR reading is achieved, where at least 1 green LED is on. If you encounter prolonged difficulty in illuminating the minimum required number of green LEDs, try to improve the reception quality by placing the antenna at a higher point or in an alternate location.

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

6 Secure the unit firmly to the pole.

7 You may need to repeat the process at the side of the BU (by using the Link Quality Indicator in Telnet).

NOTE



In some cases, the antenna may need to be tilted to ensure that the level at which the RB receives transmissions from the BU (and vice versa) is not too high. As a rule of thumb, if the RB is located at a distance of less than 300 meters from the BU, it is recommended to up-tilt the antennas by approximately 10° to 15°. To guarantee a safety margin from the saturation level, the SNR should not be higher than 50 dB. The orange LED of the SNR bar indicates that the SNR is higher than 50 dB.

3.4 Configuring the Maximum Modulation Level

This section describes how to configure the maximum modulation level for WB-B units.

NOTE

If the RB is associated with the BU, then the final configuration of the Maximum Modulation Level parameter may be performed remotely, for example, from the site of the BU or from another site.

To configure the Maximum Modulation Level:

1. If the SNR of the RB at the BU is too low, and vice versa, it is recommended that you configure the *Maximum Modulation Level parameter* to a value that is lower than the maximum supported by the unit. This can decrease the number of retransmissions due to attempts to transmit at modulation levels that are too high for the actual quality of the link.
2. Check the SNR of the RB at the BU. You can use Telnet to view the SNR values in *the MAC Address Database* of the BU, which can be accessed from the *Site Survey* menu. If the ATPC algorithm is not enabled in both units, the test should be done with the *Tx Power Level* parameters configured to their maximum values (subject to local regulatory limitations). If the SNR is lower than the values required for the maximum modulation level according to Table 3-3, it is recommended that you decrease the value of the Maximum Modulation Level.

NOTE

The SNR measurement at the BU is accurate only when receiving transmissions from the RB. If necessary, ping the BU to verify data transmission from the RB.

3. Configure the *Maximum Modulation Level* according to Table 3-3, using the typical SNR values. It is recommended that a 2 dB margin be added to compensate for possible measurement inaccuracy or variance in the quality of the link.
4. Repeat steps 2 - 3 for the BU, checking the SNR at which it is received at the RB using the *Continuous Link Quality Display* option in the *Site Survey* menu.

There is no need to ping the RB, since the SNR measurement at the RB is based on beacons which are continuously transmitted by the BU.

Table 3-3: 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

3.5 Operation Verification

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

3.5.1 Outdoor Unit Verification

To verify the correct operation of the Outdoor Unit, examine the LED indicators located on the bottom panel of the outdoor unit.

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

NOTE



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

Table 3-4: BU-ODU LEDs

Name		Description	Functionality
W-LINK		Wireless Link Indicator	■ Green - Unit is associated with an RB ■ Blinking red - Unit is not associated ■ Off - Wireless link is disabled
Status		Self-test and power indicator	■ 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 indicator	■ Green -Ethernet link detected. ■ Amber - No Ethernet connectivity between the indoor and outdoor units.
SNR BAR		Received signal strength Indicator (In Normal Mode)	See Table 3-6 for details. The SNR bar LEDs turn green only after receiving traffic from the RB side (SNR is updated based on uplink data or management frames)

Table 3-5: RB-ODU LEDs

Name		Description	Functionality
W-LINK		Wireless Link Indicator	■ Green - Unit is associated with a BU, 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 indicator	■ 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 indicator	■ 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		Received signal strength Indicator (In Normal Mode)	See Table 3-6 for details

Table 3-6: RB/BU-ODU SNR Bar LED Functionality (In Normal Mode)

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 IDU units.

The following table lists the LEDs of the PS1073 IDUs and their associated indications.

Table 3-7: PS1073 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. ■ Green- Self-test passed and Ethernet connection confirmed by the outdoor unit (Ethernet integrity check passed).

3.5.3 Verifying Data Connectivity

To verify data connectivity, from the end-user's PC or from a portable PC connected to the unit, ping the other unit or a station behind it.

Chapter 4

Operation

In This Chapter:

- "Working with the Monitor Program" on page 51
- "Menus and Parameters" on page 54

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 the Supplier's Customer Service and give them the challenge string (after user identification) to receive a one-time password. After 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 and location (if configured), SW version number and SW release date and time displayed in the **Main Menu** vary according to the selected unit and SW version.

```
<Unit Type>/<Unit Location>
Official Release Version - <Version Number>
Release Date: <Date and Time>
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 E 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 status information and 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 parameters that are also available in the *Basic Configuration* menu. 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: BU-B100, BU-B28, BU-B14, BU B10, RB B100, RB-B28, RB-B14 or RB-B10.
- **Unit MAC Address**: The unit's unique IEEE MAC address.
- **Unit Status** (RB only): The current status of the RB. There are two status options:
  - **SCANNING**: The RB is searching for a BU with which to associate. If DFS is enabled and the RB is currently looking for its previous BU, the BU's MAC Address will be displayed.
  - **ASSOCIATED**: The RB is associated with a BU.
  - **AUTHENTICATING**: This is typically a temporary status. For example, when an RB hears the beacons of a BU, tries to associate and the BU does not respond because it does not hear the RB's packets.
- **BU MAC Address** (RB only): The MAC address of the BU with which the unit is currently associated. If the unit is not associated with any BU, the address defaults to the IEEE broadcast address, which is FF FF FF FF FF FF.
- **Number of Associations Since Last Reset**: Displays the total number of associations since the last reset, including duplicate associations.
- **Number of Rejections since Last Reset**: Applicable only to BU when the Hidden ESSID feature is enabled. Displays the number of times that any unit

attempting to associate with the BU was rejected because of a non-matching ESSID (including multiple rejections of the same unit).

- **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.
- **Country Code**: The 3 or 4 digits Country Code used by the unit and its general description.
- **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 SW Version File Name
  - FTP Source Directory
- **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 Minimum Severity**
- **ATE Test Status**: Indicates the result of the unit's final testing in production. In units supplied with SW version 4.5 and higher should always be PASS. In units upgraded from a version below 4.5 this parameter will be NONE.

- **Serial Number**: The Serial Number of the unit. Applicable only to units supplied with SW version 4.5 and higher. In units upgraded from a version below 4.5 this parameter will be none (empty).

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, each bandwidth is associated with a different sub-band, as the bandwidth may affect the available frequencies. Currently, all Country Codes support bandwidths of 10 and 20 MHz. Where allowed, a bandwidth of 40 MHz (Turbo Mode) is also supported.

- **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 supported, this parameter displays the upper limit for the Maximum Burst Duration parameters.

- **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.

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
- Log Out Timer
- Ethernet Port Negotiation Mode
- Change System Location
- Event Log Menu
- Feature Upgrade
- SW Version Download
- Configuration File Upload/Download
- Change Unit Type to BU/RB
- LED Mode

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 4.2.3.12. 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 changed 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
	Unit Type
Air Interface Parameters	Selected Sub Band (BU)
	Frequency (BU)
	DFS Required by Regulations
	Frequency Subset (BU)
	Antenna Gain (BU)
Country Code Parameters	Selected Country Code

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 changed 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
	Unit Type
IP Parameters	IP Address
	Subnet Mask
	Default Gateway Address
	DHCP Option
	Access to DHCP
Security Parameters	Authentication Algorithm
	Default Key (RB)
	Data Encryption Mode
	Default Multicast Key (BU)
	Security Mode
	Key # 1 to Key # 4

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

Parameters Group	Parameter
Air Interface Parameters	ESSID
	Operator ESSID Option (BU)
	Operator ESSID (BU)
	Hidden ESSID Option (BU)
	Hidden ESSID Support (RB)
	Hidden ESSID Timeout (RB)
	Link Distance Mode (BU)
	Maximum Link Distance (BU)
	Fairness Factor (BU)
	Selected Sub Band (BU)
	Frequency (BU)
	DFS Required by Regulations
	Frequency Subset (BU)
	RB Waiting Option (BU)
	Channel Reuse Option (BU)
	Radar Activity Assessment Period (BU)
	Maximum Number of Detections in Assessment Period (BU)
	ATPC Option (BU)
	Transmit Power
	Maximum Tx Power (RB)
	Tx Control (BU)
	Best BU Support (BU)
	Preferred BU MAC Address (RBU)
	All Noise Immunity Control parameters
	All Noise Floor Calculation parameters
Network Management Parameters	Wi2 IP Address (RB)
Performance Parameters	Adaptive Modulation Decision Thresholds
Bridge Parameters	VLAN ID - Management

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

Parameters Group	Parameter
Service Parameters	Wireless Link Prioritization Option (BU-B14/28/100)
	Low Priority AIFS (BU- B14/28/100)
	Number of HW Retries for High Priority Traffic (BU- B14/28/100)
	Number of HW Retries for Low Priority Traffic (BU- B14/28/100)
	BU Burst Duration for High Priority Traffic (BU- B14/28/100)
	BU Burst Duration for Low Priority Traffic (BU- B14/28/100)
	RB Burst Duration for High Priority Traffic (BU- B14/28/100)
	RB Burst Duration for Low Priority Traffic (BU- B14/28/100)
	Low Priority Traffic Minimum Percent
Country Code Parameters	Selected Country Code

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 option is available only under Administrator access rights. It 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). A user with Installer access rights can view and change the passwords for Read Only and Installer levels. A user with Administrator access rights can view and change the passwords for all levels.

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 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.

4.2.3.7 Ethernet 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)

4.2.3.8 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.

4.2.3.9 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

4.2.3.9.1 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.

4.2.3.9.2 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).

4.2.3.9.3 Erase Event Log

The Erase Event Log option enables clearing the event log.

4.2.3.9.4 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 any procedure will automatically change its value in the menu for the other procedures.

4.2.3.10 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.

NOTE



If you are entering the license string using copy and paste operation, check carefully that the string is copied properly. You may have to enter it manually due to potential problems in performing copy and paste in Telnet.

The license string comprises 32 to 64 hexadecimal digits.

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

4.2.3.11 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.

4.2.3.12 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 any procedure will automatically change its value in the menu for the other procedures.

4.2.3.13 Change Unit Type to BU/RB

The Change Unit Type to BU/RB feature enables changing a unit's type from BU to RB and vice-versa. The Change Unit Type option can be executed only when the unit is running from the main software version.

NOTE

After changing the unit type the user must reset the unit for the change to take effect.

4.2.3.14 LED Mode

The LED Mode submenu controls the SNR bar's behavior. By default, the LEDs indicate the SNR level, which facilitates antenna's alignment. However, it is also possible to deactivate the LEDs or to customize the SNR bar to indicate when specific thresholds for RSSI, SNR, CRC percentage and average modulation are reached.

4.2.3.14.1 Change Mode

This submenu allows switching between the operation modes that are available for the LEDs. The following options are available:

- **Normal mode**: This is the default operation mode. The green LEDs on the bar indicate the SNR level. See "Outdoor Unit Verification" on page 46 for detailed information.

- **Threshold mode**: This mode allows users to define a custom behavior for each of the 8 SNR LEDs, based on the RSSI, SNR, CRC ratio or average modulation. See "Threshold Mode Settings" on page 74 for details on how to set it up.

  If all the thresholds that were set up are reached, the entire SNR bar will light up. For instance if LEDs 2, 5 and 6 have thresholds set for them (the rest of the SNR LEDs are disabled) and all these thresholds are reached, instead of having only LEDs 2, 5 and 6 light up, all the SNR LEDs will light up.

- **Stealth mode**: This setting completely shuts down all the SNR LEDs on the unit's panel, leaving only the Status, Ethernet and W-Link indicators active.

4.2.3.14.2 Threshold Mode Settings

This submenu allows users to define the behavior for each LED in the SNR bar when the Threshold Mode is employed.

4.2.3.14.2.1 LED 1 to 8

Selects the LED you wish to configure. You can define a threshold that must be reached for the LED to light up by using the menus described below.

4.2.3.14.2.1.1 Threshold Type

This option defines the parameter that is monitored and that the threshold is set for:

- **Disabled**: The LED is always off.

- **RSSI**: Sets up a threshold for the Received Signal Strength Indication

- **CRC %**: Sets up a threshold for the Cyclic Redundancy Check percentage
- **SNR**: Sets up a threshold for the Signal-to-Noise Ratio.
- **Average Modulation**: Sets up a threshold for the average modulation.

4.2.3.14.2.1.2 Threshold Mode

This option defines how the threshold parameter (see "Threshold Type" on page 74) relates to the threshold target value (see "Threshold Target" on page 75). The available operators are:

- **Equal or lower than**: The threshold parameter must be lower than or equal to the threshold target value for the LED to light up.
- **Equal or higher than**: The threshold parameter must be higher than or equal to the threshold target value for the LED to light up.
- **Equal to**: The threshold parameter must be equal to the threshold target value for the LED to light up.

4.2.3.14.2.1.3 Threshold Target

This option defines the threshold target value. Depending on the threshold type, the following value ranges apply:

Table 4-4: Threshold Target Value Ranges

Threshold Value	Value Range
RSSI	-108...0
CRC %	0...100
SNR	0...80
Average Modulation	1...8

4.2.3.14.2.2 Show LED stats

This option displays all the threshold settings that were applied for each LED in the SNR bar.

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 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.

4.2.4.2 Performance Parameters

- Maximum Modulation Level

Refer to Section 4.2.6.5 for a description of these parameters.

4.2.4.3 Network Management Parameters

- Wi2 IP Address (RB)

Refer to Section 4.2.6.3.8 for a description of this parameter.

4.2.4.4 Air Interface Parameters

- ESSID

- Operator ESSID Parameters (BU)
  - Operator ESSID Option
  - Operator ESSID
- Hidden ESSID Option (BU)
- Hidden ESSID (RB):
  - Hidden ESSID Support
  - Hidden ESSID Timeout
- Frequency Definition
  - Select Sub Band (BU, if more than one Sub Band is available)
  - Frequency (BU)
  - User Defined Frequency Subsets (RB)
  - DFS Parameters (if DFS is supported by Country Code):
    - DFS Required By Regulations
    - Frequency Subset Definition (BU)
    - Channel Check Time
    - Channel Avoidance Period
    - RB Waiting Option (BU)
    - Minimum Pulses to Detect
    - Channel Reuse Parameters
    - DFS Detection Algorithm (Universal Country Codes in 5.4/5.8 GHz bands)
    - Clear Radar Detected Channels after Reset

- Best BU Parameters (RB)
  - Best BU Support
  - Preferred BU MAC Address
- ATPC Parameters
  - ATPC Option
  - ATPC Minimum SNR Level (BU)
  - ATPC Delta from Minimum SNR Level (BU)
  - Minimum Interval Between ATPC Messages (BU)
  - ATPC Power Level Step (BU)
- Arbitration Inter-Frame Spacing (AIFS)
- Transmit Power
- Maximum Transmit Power (RB)
- Tx Control (BU)
- Antenna Gain
- Link Distance Parameters
  - Link Distance Option (BU)
  - Maximum Link Distance (BU)
  - Fairness Factor (BU)

Refer to Section 4.2.6.2 for a description of these parameters.

4.2.4.5 Country Code Parameters

- Country Code Select
- Re-apply Country Code Values

Refer to Section 4.2.6.8 for a description of these parameters.

4.2.4.6 Bridge Parameters

- VLAN ID - Management

Refer to Section 4.2.6.4.1 for a description of these parameters.

4.2.4.7 Security Parameters

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

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 BU, there is also an extensive database for the RB served by it.

- The Site Survey menu includes the following options:
- Traffic Statistics
- Ping Test

- MAC Address Database
- Link Quality (RB only)
- Hidden ESSID Table (RB only)
- Continuous Noise Floor Display (BU only)
- 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 media. Frames discarded by the unit's hardware filter are not counted by the Ethernet counters. For B14/B28 units 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 VLAN and CRC. For B100 units 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.

The unit transmits valid data frames received from the wireless media 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 data frame is transmitted, the unit waits for an acknowledgement (ACK) message from the receiving unit. Some control and wireless management frames are not acknowledged. If an ACK is not received after a predefined time, 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 mechanism (for more information see Section 4.2.6.6.3).

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

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 WB-B unit (whose MAC address is present in the Association database) via the wireless port (as opposed to messages intended for stations behind other WB-B 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 media. The total includes one count for each successfully transmitted frame (excluding retransmissions), and the number of transmitted

control and wireless management frames. In the BU, there are also separate counters for the following:

- Beacons
- Management and Other Data frames, including successfully transmitted unicast frames and multicast/broadcast data frames (excluding retransmissions, excluding Beacons in BU)

- **Total submitted frames (bridge)**: The total number of data frames submitted to the internal bridge for transmission to the wireless media. 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 media, 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 media. 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 media, 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 media 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.
  - Other

- **Total received concatenated frames**: The total number of concatenated frames received from the wireless media, 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 media 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**: The number of data frames received from the Ethernet port that were discarded by the MIR mechanism to avoid exceeding the maximum permitted information rate.

- **TX retransmission %**: The percentage of frames that were not transmitted properly and had to be retransmitted.

- **TX CRC %**: The percentage of Cyclic Redundancy Check errors that occurred over the air link.

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 (RB 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/RSSI 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) and Received Signal Strength Indication (RSSI) measurements.

The average RSSI is calculated using the formula:

NewAvgRSSI = (PrevAvgRSSI*HistWeight) + CrtRSSI*(1 - HistWeight), where:

- NewAvgRSSI = New Average RSSI

- PrevAvgRSSI = Previous Average RSSI

- CrtRSSI = RSSI of the current packet

- HistWeight = History Weight

The History Weight is given by the next formula:

HistWeight = 0.9 / (PastTime / 2SNR_Memory_Factor + 1), where

PastTime = time between the current packet and previous packet, in seconds

SNR_Memory_Factor = the Average SNR Memory Factor configurable parameter (see Section 4.2.6.5.7).

The SNR_Memory_Factor can be -1 in this case the history is not used and the Average RSSI is the RSSI of the current packet.

The same formula is used also for calculating Average SNR (SNR values are used instead of RSSI values).

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

4.2.5.3.2 Continuous Noise Floor Display

The **Continuous Noise Floor Display** option displays continuously updated information regarding the average noise floor in the wireless link. It also displays continuously updated information about the Signal Interference Ratio. Signal Interference Ratio (SIR) is the average SNR for all pulses and physical errors received by the unit. The average has the same formula used for calculation of SNR per unit.

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

4.2.5.3.3 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 BU, 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 RB and the BU. 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 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

The MAC Address Database submenu includes the following options:

- MAC Address Database in BU
- MAC Address Database in RB

4.2.5.4.1 MAC Address Database in BU

The **MAC Address Database** option in the BU displays information regarding the RB associated with it, as well as bridging (forwarding) information. The following options are available:

- **Display Bridging and Association Info**: The Display Bridging and Association Info option displays a list that includes the associated RB and stations in the BU's Forwarding Database. For stations behind an RB, the RB's MAC address is also displayed (RB 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 RB. For these addresses, learned from the wireless port, the address of the RB is also displayed (in parenthesis).
  - **St (Static)**: An associated RB. For this entry, the following RB details are also displayed: Unit Name, SW version, Unit Type, Distance from the BU, IP Address, Wi2 IP Address as defined in the RB (or 0.0.0.0 for none), ESSID.
  - **Sp (Special)**: 3 addresses that are always present, including:
    - The MAC address of the BU.
    - The Multicast address (01-20-D6-00-00-01). 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 RB 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 RBs (0 or 1).

NOTE



There is no aging algorithm for the associated RB. An RB is only removed from the Association Database under the following conditions:

- The RB failed to respond to 100 consecutive data frames transmitted by the BU and is considered to have "aged out".
- During the last 6 minutes (or more) the RB did not transmit any data frame, and failed to respond to certain frames that typically are transmitted by the BU every 10 seconds. Since the sampling interval for this state is about 10 minutes, it means that the decision to remove the RB from the Associations Database will take place between 6 to 16 minutes from the time the RB ceased sending data or responding to these "keep-alive" messages.

» 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 is **4093** (4096 minus the number of special Sp addresses as defined above) for Bridging Info, and 1 for Association Info.

- **Display Association Info**: Displays information regarding the RB associated with the BU. The entry includes the following information:

» The MAC Address of the associated RB

» Age in seconds, indicating the elapsed time since receiving the last packet from the RB.

» The value configured for the Maximum Modulation Level parameter of the RB

» The Status of the RB. There are three options:

1 Associated

2 Authenticated

3 Not Authenticated (a temporary status)

The various status states are described in Table 4-5 (this is a simplified description of the association process without the effects of the Best BU algorithm).

Table 4-5: Authentication and Association Process

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

- The SNR of the RB measured at the BU
- The RSSI of the RB measured at the BU
- The Unit Name of the RB
- The SW version of the RB.
- Unit Type.
- Distance from the BU.
- IP Address
- Wi2 IP Address as defined in the RB (or 0.0.0.0 for none)
- The ESSID of the RB

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 RBs (0 or 1).

NOTE



There is no aging algorithm for the associated RB. An RB is only removed from the Association Database under the following conditions:

- The RB failed to respond to 100 consecutive data frames transmitted by the BU and is considered to have "aged out".
- During the last 6 minutes (or more) the RB did not transmit any data frame, and failed to respond to certain frames that typically are transmitted by the BU every 10 seconds. Since the sampling interval for this state is about 10 minutes, it means that the decision to remove the RB from the Associations Database will take place between 6 to 16 minutes from the time the RB ceased sending data or responding to these "keep-alive" messages.

» 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 1.

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

4.2.5.4.2 MAC Address Database in RB

The **MAC Address Database** option in the RB displays information regarding the RB's bridging (forwarding) information. The following option is available:

- **Display Bridging and Association Info**: The Display Bridging and Association Info option displays a list of all the stations in the RB'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.
- **St (Static)**: The associated BU.
- **Wl (Wireless)**: An address of a node behind the associated BU, learned via the wireless port.
- **Sp (Special)**: 4 addresses that are always present, including:
  - The MAC address of the RB.
  - The Multicast address (01-20-D6-00-00-01. The system treats this address as a Broadcast address.
  - The 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 4092.

4.2.5.5 Continuous Noise Floor Display (BU only)

The **Continuous Noise Floor Display** option displays continuously updated information regarding the average noise floor in the wireless link. It also displays continuously updated information about the Signal Interference Ratio. Signal Interference Ratio (SIR) is the average SNR for all pulses and physical errors received by the unit. The average has the same formula used for calculation of SNR per unit.

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

4.2.5.6 Hidden ESSID Table (RB only)

An RB with Hidden ESSID Support enabled (for details see Section 4.2.6.2.2) that maintains a list with BUs that rejected association requests from the RB because of a wrong ESSID. A BU will be kept in this list until the Hidden ESSID Timeout expires for it or if the list is full and another BU that is not in the list rejects the BU because of wrong ESSID.

The Hidden ESSID Table displays for each BU included in the list its MAC Address and Age (elapsed time in minutes since it was added to the table).

4.2.5.7 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.

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

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

In the RB, 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.

4.2.5.8 Link Capability

The Link Capability option provides information on HW and SW capabilities of relevant units. In a BU, the information provided in the Link Capability reports is for the associated RB. In an RB, the Link Capability reports include information on all BUs in the neighboring BUs table (all BUs with whom the RB 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 differs between BUs and RBs:

4.2.5.8.1 Link Capability Options in RB

4.2.5.8.1.1 Show Link Capability-General

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

- **HwVer**: the hardware version of the unit.
- **Country**: The 3 or 4 digits country code supported by the unit.
- **SwVer**: The SW version used by the unit.

4.2.5.8.1.2 Show Link Capability-Wireless Link Configuration

Select this option to view information on current wireless link parameters of relevant BUs. For each relevant BU, 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.
- **TBD**: Enable or Disable.
- **Concatenation Option**: Enable or Disable.

4.2.5.8.1.3 Show Link Capability-Security Configuration

Select this option to view information on current security related parameters of relevant BUs. For each relevant BU, 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.

4.2.5.8.1.4 Show Link Capability by BU (RB only)

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

4.2.5.8.2 Link Capability Options in BU

In the BU, the Link Capability submenu includes a single option, Show Link Capability:

4.2.5.8.2.1 Show Link Capability

Select this option to view all capabilities information (General, Wireless Link Configuration, Security Configuration) of the associated RB. The displayed information includes:

General:

- **HwVer**: The hardware version of the unit.
- **CpldVer**: The version of the Complex Programmable Logic Device (CPLD) used in the RB.
- **Country**: The 3 or 4 digits country code supported by the unit.
- **BootVer**: The Boot Version of the unit.

Wireless Link Configuration:

- **ATPC Option**: Enable or Disable.
- **Adaptive Modulation Option**: Enable or Disable.
- **Burst Mode Option**: Enable or Disable.
- **DFS Option**: Enable or Disable. On RBs, this parameter displays the current option in the relevant BU. On BUs, it displays the DFS values configured in each RB.
- **Concatenation Option**: Enable or Disable.

Security Configuration:

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

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 DHCP 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 the following parameter, 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 BU is From Ethernet Only. The default for RB 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 BU. To facilitate easy addition of an RB to an existing network without a prior knowledge of which specific BU will serve it, and to support the Best BU feature, a secondary "global" ESSID, namely "Operator ESSID", can be configured in the BU. If the Operator ESSID Option is enabled at the BU, the Beacon frames transmitted by it

will include both the ESSID and Operator ESSID. The RB shall regard such frames if either the ESSID or the Operator ESSID matches it own ESSID. The ESSID of the BU with which the RB is eventually associated is defined as the Run-Time ESSID of the RB. Typically, the initial ESSID of the RB is configured to the value of the Operator ESSID. When the RB has become associated with a specific BU, its ESSID can be reconfigured to the value of the ESSID of the BU.

To support increased security the ESSID may be hidden. When this feature is activated in a BU it will not broadcast the ESSID in Beacon frames (null characters will be transmitted instead of the ESSID). The ESSID will not be transmitted also in Distance messages transmitted by either the BU or the associated RB.

The following frames will still contain the ESSID:

- Probe Request - generated by RBs when active scanning is used.
- Probe Response -generated by the BU as a response when the BU receives a Probe Request from an RB. This unicast frame is sent only to the RB that has sent the Probe Request, and it is sent only if the ESSID received in the Probe Request is the same as the BU's ESSID.
- The ESSID will be present also in the Association Request frame sent by RBs.

The impact of the Hidden ESSID feature on the RB's operation is as follows:

- If the Hidden ESSID Support parameter in the RB is set to Disable, the RB will not try to Associate with a BU that is working with Hidden ESSID Enabled
- If the Hidden ESSID Support parameter in the RB is set to Enable the RB will try to Associate with a BU that is working with Hidden ESSID. The RB will send the Association Request that will contain the ESSID of the RB; the BU will check the RB's ESSID versus its own ESSID and if there is a match the BU will associate the RB. If the RB uses a different ESSID the BU will reject it and the Association Response will include the reason for rejection. The RB will add this BU to a table that contains the BUs that rejected it because of wrong ESSID and it will not try again to associate with this BU until the Hidden ESSID Timeout expires.
- If Hidden ESSID Support parameter in the RB is set to Enable and the RB finds a BU that is not working with Hidden ESSID the RB will try to associate with this BU only if the BU's ESSID/Operator ESSID is the same as the RB's ESSID.

The impact of the Hidden ESSID feature on the BU's operation is as follows:

- When the BU receives Probe Request form an RB it will check if the ESSID in the Probe Request is that same as its own ESSID. It will generate the Probe Response only if there is a match.
- The Authentication process is not affected by the Hidden ESSID feature.
- When the BU receives an Association Request and the ESSID included in the frame matches its own ESSID the BU sends the Association Response with Status Code OK - meaning that the RB is associated. If there is no match the BU sends the Association Response with Status code Rejected - meaning that the RB is not associated, and the reason of rejection - wrong ESSID.

An RB that is trying to associate with BUs that are working with Hidden ESSID will keep a list with BUs that rejected it. The BU will be kept in this list until the Hidden ESSID Timeout expires for it or if the list is full and another BU that is not in the list rejects the RB because of wrong ESSID.

The BU that is working with Hidden ESSID enable will keep a counter that will be incremented for each RB that is rejected because of wrong ESSID.

The Operator ESSID feature still works when Hidden ESSID is enabled. The only differences is that the Runtime ESSID displayed by RB, when the RB is associated because of Operator ESSID, will be the ESSID of the RB and not the ESSID of the BU as it is when Hidden ESSID is disabled.

The ESSID related parameters are:

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 (BU 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 RBs.

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.

4.2.6.2.2.3 Hidden ESSID Option (AU only)

The Hidden ESSID Option enables or disables the Hidden ESSID feature. When enabled, the ESSID will not be broadcasted by the AU.

The default is Disable.

4.2.6.2.2.4 Hidden ESSID (SU only)

The Hidden ESSID submenu in the SU includes the following options:

4.2.6.2.2.4.1 Hidden ESSID Support

The Hidden ESSID Support option enables or disables the Hidden ESSID feature in the SU.

The default is Disable.

4.2.6.2.2.4.2 Hidden ESSID Timeout

The Hidden ESSID Timeout parameter defines the time that SU will not try again to associate with an AU that is working with Hidden ESSID if the AU rejected Association Request sent by the SU because of wrong ESSID.

The range is from 1 to 60 minutes.

The default is 10 minutes.

4.2.6.2.2.4.3 Show Hidden ESSID Parameters

Select this option to view the current values of Hidden ESSID Support and Hidden ESSID Timeout.

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 BU. 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 RB should be configured with a minimal set of parameters to ensure that it will be able to automatically detect and use the frequency used by the BU, including possible changes in this frequency (Automatic Sub Band Select feature).

To simplify the installation process the RB 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 BU feature is enabled, the RB will scan the defined subset and the operating frequency/bandwidth will be determined by the Best BU mechanism (including the optional use of the Preferred BU feature). Otherwise the RB will try to associate with the first BU it finds. If no BU is found, the RB 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 equipment does not interfere with certain radar systems in the 5 GHz band. If radar is being detected, the wireless equipment 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.

NOTE



Radar detection parameters that are enforced by Country Code specific regulations are editable only by users with Administrator privileges. When enabling a Country Code that requires particular DFS settings, the unit automatically applies these settings. Users with Installer privileges will be able to set a particular Country Code, but they will not be able to change its default DFS settings.

When DFS is enabled, the unit monitors the spectrum continuously, searching for signals with a specific pattern indicating radar activity. Upon detecting radar activity, the unit immediately stops transmitting on this frequency and starts

looking for another radar-free frequency. The subset of viable frequencies is configurable.

4.2.6.2.3.2.1 DFS implementation on the BU

The BU maintains a continuously updated database of all applicable frequencies, where each frequency is marked as Radar Free, Radar Detected or Adjacent to Radar. The BU attempts to check a new frequency only if it is marked as Radar Free. If there is no radar activity detected, the units may use this frequency to communicate. If a radar activity was detected on a certain frequency, it will be marked in the database as a Radar Detected frequency. The frequency will remain tagged as Radar Detected for a predefined period of time called Channel Avoidance Period. After this period expires, the frequency 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.

4.2.6.2.3.2.2 DFS implementation on the RB

When DFS is enabled on the RB, the unit uses a channel availability check mechanism that is similar to the BU's. Before associating to the BU, the RB picks a Radar Free frequency and:

- If the frequency was previously scanned and tagged as available, it immediately associates to the BU.

NOTE



Some country codes require a periodical revalidation of the Radar Free frequencies. So additionally, it might be required for the channel validation period not to have expired as well.

- If the frequency, is currently tagged as Radar Free as a result of a Radar Detected status that expired, or in some cases if the Radar Free validation has expired (see the note above), the RB will initiate its own channel availability check. As a result:
  - » If no radar signal is detected, the RB associates to the BU
  - » If the RB detects a radar, it will tag the frequency in its own database as Radar Detected, notify the BU and attempt to connect on another channel

While associated, the RB also performs In-Service Monitoring, meaning that it periodically scans the operating channel for radar signals. If radar is detected, it will notify the BU and stop transmitting on the respective frequency.

ETSI requirements enforce particular implementations for the DFS functionality on RBs. Implementations of DFS on the RB for ETSI 5.8 and ETSI 5.4 based country codes are compared in Table 4-6.

Table 4-6: DFS behavior on RBs using ETSI based country codes

Feature	ETSI 5.8 based country codes	ETSI 5.4 based country codes
Applicable country codes	■ ETSI 5.8 ■ Other country codes based on ETSI 5.8 (UK 5.8, Germany 5.8 and Universal 5.8 with Detection Algorithm set to ETSI)	■ ETSI 5.4 ■ Other country codes based on ETSI 5.4 (ETSI F 5.4 and Universal 5.4 with Detection Algorithm set to ETSI)
Startup	RB checks each frequency and tags it as either Radar Free or Radar Detected.	All frequencies are tagged as Radar Free by default
Operating Frequency	RB performs In-Service Monitoring and dissasociates when radar is detected.	RB performs In-Service Monitoring and dissasociates when radar is detected.
Radar Detected or Adjacent to Radar frequency	Expires after a predefined Channel Avoidance Period. The frequency's status is then set to Radar Free, but the RB needs to check for radar before using it to associate.	Expires after a predefined Channel Avoidance Period. The frequency's status is then set to Radar Free, but the RB needs to check for radar before using it to associate.
Radar Free frequency	Expires. Afterward, the frequency is still tagged as Radar Free, but the RB needs to check for radar before using it to associate.	No revalidation required. The RB may use the frequency to associate at any time.

4.2.6.2.3.2.3 Channel shutdown

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

Table 4-7: Comparison between DFS implementations for various country codes on the RB

Action	Parameter	ETSI 5.4 GHz	ETSI 5.8 GHz	Universal	FCC
When reverting the unit to factory default settings	DFS Option	According to country code definition	According to country code definition	false	According to country code definition
When upgrading from a previous software version	DFS Option	false	According to country code definition	false	Unchanged
When changing the country code	DFS Option	According to country code definition	According to country code definition	false	■ BU - According to country code definition ■ RB - false
	Channel Check Time	60 sec. (600 sec. for freq. between 5600 and 5650 MHz)	60 sec. (600 sec. for freq. between 5600 and 5650 MHz)	60 sec.	60 sec.
	Channel Avoidance Period	30 min.	30 min.	30 min.	30 min.
	Minimum Pulses to Detect	4	4	4	4
	Frequency Subset Definition	According to country code definition	According to country code definition	According to corresponding ETSI 5.4/5.8	ALL

4.2.6.2.4 Frequency Definition Submenu in BU

The Frequency Definition submenu in BU 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.

NOTE



For compliance with ETSI regulations, the bandwidth used in the default Sub Band for units in the 5.4 GHz band is 20 MHz. The use of a Sub Band with a 40 MHz bandwidth (Turbo Mode) in the 5.4 GHz band is allowed only if approved by the applicable local regulatory administration.

4.2.6.2.4.2 Frequency

The Frequency parameter defines the transmit/receive frequency when DFS is not enabled. If DFS 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.

NOTE 1 (FCC 5.3 GHZ, 20 MHz Bandwidth):

For full compliance with FCC regulations, the following requirements should be followed in units using a 20 MHz bandwidth:

1. In units HW Revision B, if you wish to include frequency channel 5270 MHz in the set of frequencies to be used, then the Transmit Power parameter in the BU, and the Maximum Tx Power parameter in the RB, should not be set to a value above "17-Antenna Gain". If there is a need to use a higher value for these parameters, this frequency should not be used.
2. In units with HW Revision C, if you wish to include one or more of frequency channels 5270, 5275 and 5330 MHz in the set of frequencies to be used, then the Transmit Power parameter in the BU, and the Maximum Tx Power parameter in the RB, should not be set to a value above "20-Antenna Gain". If there is a need to use a higher value for these parameters, this frequency should not be used.

NOTE 2 (FCC 5.3 GHZ, 40 MHz Bandwidth):

For full compliance with FCC regulations, the following requirements should be followed in units using a 40 MHz bandwidth:

1. In units with HW Revision B, Frequency channels 5270 and 5280 MHz should not be used.
2. In units with HW rev C, if you wish to include frequency channel 5290 MHz in the set of frequencies to be used, then the Transmit Power parameter in the BU, and the Maximum Tx Power parameter in the RB, should not be set to a value above "25-Antenna Gain". If there is a need to use a higher value for these parameters, this frequency should not be used.
   If you wish to include frequency channel 5310 MHz in the set of frequencies to be used, then the Transmit Power parameter in the BU, and the Maximum Tx

Power parameter in the RB, should not be set to a value above "29-Antenna Gain. If there is a need to use a higher value for these parameters, this frequency should not be used.

NOTE 3 (FCC 5.3 GHZ, 10 MHz Bandwidth):

For full compliance with FCC regulation of units with HW rev C using a 10 MHz bandwidth, if you wish to include frequency channel 5265 MHz in the set of frequencies to be used, then the Transmit Power parameter in the BU, and the Maximum Tx Power parameter in the RB, should not be set to a value above "25-Antenna Gain". If there is a need to use a higher value for these parameters, this frequency should not be used.

4.2.6.2.4.3 DFS Parameters

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

Note that starting on SW version 5.2, the DFS feature is supported (although disabled by default) for units using Country Codes 1060 and 1064 (Universal 5.4 GHz and Universal 5.8 GHz). When a unit using either one of these Country Codes is upgraded from a SW version lower than 5.2 the feature will not be automatically applicable. If the user wants to use the DFS feature he must re-apply the Country Code values (see Section 4.2.6.8.2). Note also that for these units, if the user changes the working sub-band the DFS Option will be automatically set to No. For other Country Codes that support DFS when sub-band is changed the DFS Option is forced to Yes.

The DFS Parameters submenu includes the following parameters:

4.2.6.2.4.3.1 DFS Required by Regulations

The DFS Required by Regulations option enables defining whether DFS should be used for compliance with applicable local regulations. The options are Yes or No. Selection of the No option will disable the radar detection and dynamic frequency selection mechanism.

The default depends on the Country Code (No for Universal Country Codes in the 5.4 and 5.8 GHz bands, Yes for all other Country Codes that support DFS as required by applicable regulations).

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 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 unit does not transmit.

The range is 1 to 3600 seconds.

The default is 60 seconds.

NOTE



When ETSI country codes are applied, on operating channels overlapping partially or totally with frequency range 5600 - 5650 MHz, the Channel Check Time is forced to minimum 600 seconds (10 minutes).

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 RB Waiting Option

The RB Waiting Option defines whether the disassociation message sent by the BU, after detecting radar activity on the current frequency, will include a message instructing the RB to search only for the BU before attempting to search for another BU. The message includes also the time period during which the RB should not search for any other BU. 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 4 pulses.

4.2.6.2.4.3.7 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, 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.

4.2.6.2.4.3.8 DFS Detection Algorithm

The DFS Detection Algorithm option is applicable only to units using a Universal Country Code in either the 5.4 GHz or the 5.8 GHz band (Country Codes 1060 and 1064), enabling to select the DFS detection algorithm if DFS should be enabled.

The available options are ETSI and FCC.

The default is ETSI.

4.2.6.2.4.3.9 Remote Radar Event Reports (ETSI Country Codes in 5.4/5.8 GHz bands)

If the associated RB reports a radar presence on a particular channel in a limited period of time, the BU will initiate the DFS mechanism on that channel. The Remote Radar Event Reports defines this minimum number of radar reports required for the BU to initiate the DFS.

The range is 0 to 512 radar detections. When set to 0, the mechanism is disabled.

The default is 1.

4.2.6.2.4.3.10 Remote Radar Events Monitoring Period (ETSI Country Codes in 5.4/5.8 GHz bands)

The Remote Radar Events Monitoring Period defines the maximal time interval in which the Remote Radar Event Reports must be collected for the BU to initiate the DFS.

The range is 1 to 30 minutes.

The default is 30.

4.2.6.2.4.3.11 Enhanced ETSI Radar Detection (Only for ETSI Based Country Codes)

This mechanism is designed to offer the ability to switch between the “old” and “new” ETSI DFS Radar detection mechanisms. Its functionality is the following:

- **On**: The Radar detection mechanism supports Staggered PRF detection in the entire 5.4GHz band and increases detection sensitivity (see Table 4-8 for complete list of changes).
- **Off**: The Radar detection mechanism supports Staggered PRF detection in the 5600-5650MHz band only and maintains “legacy” detection sensitivity (present in previous SW versions up to 5.5.12)

Table 4-8: Enhanced ETSI Radar Detection Behavior

Enhanced ETSI Radar Detection	On	Off
Enhanced ETSI Radar Detection	full 5.4GHz band	5600-5650MHz
Staggered PRF minimum pulses to detect	A number of Staggered PRF signal groups equal to the maximum between (Minimum Pulses to Detect /2) and 4	

4.2.6.2.4.3.12 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 BU will start operation using its default frequency.

The default is Disable.

4.2.6.2.4.3.13 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).

4.2.6.2.4.4 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 RB

4.2.6.2.5.1 Sub Band Select

This parameter is available only if the country code supports two or more Sub Bands. The Sub-Band Select option in the RB enables defining the sub band to be used during Spectrum Analysis (see Section 4.2.6.2.13). It has no affect on the frequencies to be used during regular operation, which are defined using the User Defined Frequency Subsets menu described below. 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.

4.2.6.2.5.2 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 RB when scanning for a BU. 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.

4.2.6.2.5.3 DFS Parameters

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

Note that starting on SW version 5.2, the DFS feature is supported (although disabled by default) for units using Country Codes 1060 and 1064 (Universal 5.4 GHz and Universal 5.8 GHz). When a unit using either one of these Country Codes

is upgraded from a SW version lower than 5.2, the feature will not be automatically applicable. If the user wants to use the DFS feature, he must re-apply the Country Code values (see section "Re-apply Country Code Values" on page 183). Note also that for these units, if the user changes the working sub-band the DFS Option will be automatically set to No. For other Country Codes that support DFS when sub-band is changed the DFS Option is forced to Yes.

The DFS Parameters submenu includes the following parameters:

4.2.6.2.5.3.1 DFS Required by Regulations

The DFS Required by Regulations option enables defining whether DFS should be used for compliance with applicable local regulations. The options are Yes or No. Selection of the No option will disable the radar detection and dynamic frequency selection mechanism.

The default depends on the Country Code (No for Universal Country Codes in the 5.4 and 5.8 GHz bands, Yes for all other Country Codes that support DFS as required by applicable regulations).

4.2.6.2.5.3.2 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 unit does not transmit.

The range is 1 to 3600 seconds.

The default is 60 seconds.

NOTE



When ETSI country codes are applied, on operating channels overlapping partially or totally with frequency range 5600 - 5650 MHz, the Channel Check Time is forced to minimum 600 seconds (10 minutes).

4.2.6.2.5.3.3 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.

4.2.6.2.5.3.4 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 4 pulses.

4.2.6.2.5.3.5 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.

4.2.6.2.5.3.6 DFS Detection Algorithm

The DFS Detection Algorithm option is applicable only to units using a Universal Country Code in either the 5.4 GHz or the 5.8 GHz band (Country Codes 1060

and 1064), enabling to select the DFS detection algorithm if DFS should be enabled.

The available options are ETSI and FCC.

The default is ETSI.

4.2.6.2.5.4 Show Frequency Definitions

Upon selecting the Show Frequency Definitions, the selected frequencies in each of the available Sub Bands and the current operating frequency will be displayed.

4.2.6.2.6 Best BU Parameters (RB)

In certain applications multiple BUs may be used to provide redundancy for high availability. An RB that can communicate with more than one BU using the same ESSID may become associated with the first BU it "finds", not necessarily the best choice in terms of quality of communication.

The need to create best throughput conditions for the RB led to the creation of the Best BU feature, to enable an RB to connect to the best BU in its neighborhood.

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

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

The Best BU Parameters menu includes the following options:

4.2.6.2.6.1 Best BU Support

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

The default is Disable.

NOTE



If the Best BU feature is not used, the RB associates with the first free BU 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 BU option is enabled, the RB gathers information on neighboring free BUs 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 RB is not operational.

Valid values: 1 - 255.

Default value: 4.

4.2.6.2.6.3 Preferred BU MAC Address

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

Valid values: A MAC address string.

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

4.2.6.2.6.4 Show Best BU Parameters and Data

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

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

- **MAC Address**
- **SNR** of the received signal
- **RSSI** of the received signal
- **Mark** - The computed quality mark for the BU.
- **Full** - The association load status of the BU. It is defined as full if it is already associated with an RB. A BU whose associations load status is full cannot be selected as the Best BU, even if its computed mark is the highest.

- **ESSID** - The ESSID of the BU.

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

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

4.2.6.2.7 Scanning Mode (RB only)

The Scanning Mode parameter defines whether the RB will use Passive or Active scanning when searching for a BU.

In passive scanning, the RB "listens" to the wireless media 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 RB decides that it should start searching for another BU, is approximately seven seconds when the **Roaming Option** is disabled.

In some situations when there is a high probability that RB might need to roam among different BUs, 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 enabled on the RB, 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 the RB according to the actual level at which it is received by the BU. To support proper operation of the system with optimal performance and minimum interference between neighboring systems, the ATPC algorithm should be enabled in both BU and RB.

The algorithm is controlled by the BU that calculates for each received frame the average SNR at which it receives transmissions from the RB. 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 BU transmits to the RB a power-up or a power-down message. The target is that the RB 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 RB tries to associate with the BU (following either a reset or loss of synchronization), it will initiate transmissions using its **Transmit Power** parameters. If after a certain time the RB does not succeed to synchronize with the BU, it will start increasing the transmit power level.

In a BU 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 short links and to minimize the interference with the operation of neighboring systems, or for compliance with local regulatory requirements.

In some cases the maximum transmit power of the RB 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 BU, the Transmit Power parameter defines the fixed transmit power level and is not part of the ATPC algorithm.

In the RB, 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 loosing synchronization with the BU.

The minimum value for the Transmit Power Parameter is -10 dBm (the ATPC may reduce the actual transmit power of the RB to lower values). The maximum value

of the Transmit Power Parameter depends on several unit properties and parameters:

- 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 RB 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 (RB 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 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 BU

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 the RB to be received at the BU (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 RB to be received at the BU (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 2.4, 5.4and 5.8 GHz bands. 8 (dB) for units operating in the 5.2 or 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 the RB. Setting a low value for this parameter may lead to higher overhead and to an excessive rate of power level changes at the RBs High values for this parameter increase the time it will take the RB 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 RB 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 RB

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 Tx 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 (BU only)

The Tx Control option enables turning Off/On the BU's transmitter, or having the BU 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 BU Transmitter will be switched to Off.
- If the Ethernet link is up, the BU 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 lower limit for the Antenna Gain parameter is 0 (dBi). The upper limit for the Antenna Gain is Regulation Max EIRP + 10 in dBi (since the minimum Tx Power is -10dBm), up to a maximum of 50 (dBi). If Regulation Max EIRP is No Limit, the upper limit is 50 (dBi). 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 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 is typically Don't Care for units delivered to countries where there are no regulatory limitations regarding EIRP. When applicable regulations limit the EIRP, then the default is 21 (not changeable) for units with an integral antenna and Not Set Yet for units with a detached antenna.

4.2.6.2.10 Link Distance Parameters (BU only)

The higher the distance between the RB and the BU that is serving it, the higher the time it takes for messages sent by one of them to reach the other. The time that a unit waits for a response message before retransmission (acknowledge time

delay) should take into account the round trip propagation delay between the two units (the one-way propagation delay at 5 GHz is 3.3 microseconds per km / 5 microseconds per mile). The higher the distance between the BU and the RB, the higher the acknowledge time delay used by both units should be. The ACK timeout in microseconds is: 20+Distance (km)*2*3.3 or 20+Distance (miles)*2*5.

The distance between the BU and the RB can be determined either manually or automatically. In manual mode, this distance is configured manually. In automatic mode, the BU uses a special algorithm to estimate its distance from the RB.

The Link Distance Parameters menu includes the following parameters:

4.2.6.2.10.1 Link Distance Mode

The Link Distance Mode option defines whether the distance between the BU and the RB will be determined manually (using the Maximum Link Distance parameter) or automatically.

The Options are Automatic or Manual.

The default is Automatic.

4.2.6.2.10.2 Maximum Link Distance

The Maximum Link Distance parameter allows configuring the distance between the BU and the RB when the Link 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 defines the effect of the Link Distance (calculated or configured manually) on the slot size. In good quality links, the minimal slot size (9 microseconds) can be used, providing maximum throughput. In a link with poor conditions (such as a high interference level), the slot size should be increased to enable better performance. The higher the Fairness Factor, the higher is the impact of the Link Distance on the actual slot size.

The range is 0 to 100 (%)

The default is 100 (%), meaning maximum impact of the distance on the slot size.

4.2.6.2.10.4 Show Link Distance Parameters

Select Show Link Distance Parameters to view the Link Distance parameters. In addition, the Measured Maximum Link Distance and the MAC address of the RB are displayed.

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 “Minimum Contention Window” on page 156 after reaching a decision that the medium has become free.

DIFS equals SIFS plus AIFS, where AIFS can be configured to a value from 1 to 50 time slots. A unit with a lower AIFS has an advantage over units with a higher AIFS, since it has a better chance to gain access to limited wireless link resources. 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 “Minimum Contention Window” on page 156) 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 range is from 1 to 50 (time slots).

The default is 2 time slots.

NOTE



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 Wireless Link Trap Threshold (BU 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 (%).

4.2.6.2.13 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 all the frequencies included in the selected sub-band.

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:

4.2.6.2.13.1 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.

4.2.6.2.13.2 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.

4.2.6.2.13.3 Automatic Channel Selection (BU only)

The Automatic Channel selection option defines weather the BU 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.

4.2.6.2.13.4 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.

4.2.6.2.13.5 Reset Spectrum Analysis Information

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

4.2.6.2.13.6 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 Max SNR**: The maximum 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.
- **OFDM SNR**: The average SNR (in dB) of OFDM frames received in the channel.

- **OFDM Max SNR**: The maximum SNR (in dB) of OFDM frames received in the channel.
- **Noise Floor Avg**: The average Noise Floor (in dBm) calculated for the channel.
- **Noise Floor Max**: The maximum Noise Floor (in dBm) calculated for the channel.

4.2.6.2.13.7 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.

4.2.6.2.13.8 Show Spectrum analysis Parameters & Data

The Show Spectrum analysis Parameters & Data option enables viewing the Spectrum analysis test parameters and the last test results.

4.2.6.2.14 Lost Beacons Transmission Watchdog Threshold (BU only)

When it is unable to send beacon frames for a predetermined period of time, such as in the case of interferences, the BU 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, its default value being 218. When the parameter is set to 0, this feature is disabled, i.e. internal refresh will never be performed.

4.2.6.2.15 Noise Immunity Control

Noise Immunity Control parameters are available only in units with HW Revision C and higher, except to the Pulse Detection Sensitivity parameter that is available also in units with HW Revision B.

The Adaptive Noise Immunity (ANI) mechanism is designed to reduce the wireless physical layer errors and by that enhance the 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 the Supplier's experts before switching to manual mode and modifying any of the parameters.

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

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

CAUTION



In a unit managed over the wireless link, do not change any Noise Immunity Control parameters (except the Noise Immunity State Control) from remote, as it may result in loss of connectivity to the unit.

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). To ensure that sensitivity is not reduced too much, verify that the Age (see Display Association Info) of the RB in the BU's MAC Address Database is below 20 seconds.

Do not activate the OFDM Weak Signal parameter if the SNR is below 36 dB. Under normal conditions, the OFDM Weak Signal should never be activated in the BU, since the SNR of the RB it serves will be below 36 dB when ATPC is enabled

The Noise Immunity Control submenu includes the following options:

4.2.6.2.15.1 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.

4.2.6.2.15.2 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.

4.2.6.2.15.3 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.

4.2.6.2.15.4 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 low SNR.

The default is 0.

4.2.6.2.15.5 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 or during a Spectrum Analysis test, the Pulse Detection Sensitivity is set internally to High (regardless of the configured value).

The default is Low.

4.2.6.2.15.6 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.

4.2.6.2.16 Noise Floor Calculation Parameters

The Noise Floor calculation mechanism incorporated in the units is used for estimating the level of the noise floor. This value is used for estimating SNR values and for decisions on existence of signals in the channel. In some cases, especially when a very strong signal exists in neighboring channels, the noise floor calculated by the built-in mechanism may be significantly below the actual noise floor level.

Typically, the expected noise floor level is:

- 10 MHz bandwidth: -99 (dBm)
- 20 MHz bandwidth: -96 (dBm)
- 40 MHz bandwidth: -93 dBm

The default calculation mode is Fully Automatic, using only the built-in mechanism. If you experience problems in the wireless link such as excessively long association process or very low throughput, it may be caused by errors in noise floor calculation. In this case, it is recommended to perform a Spectrum Analysis (see Section 4.2.6.2.13) and view the Average Noise Floor values. If the calculated Noise Floor is lower by more than 5 dB from the expected value, it is recommended to change the calculation mode to Automatic with Minimum Value, using the expected value as the minimum (Forced Value).

Note that if the SNR of received signals is very low (typically below 10 dB), it is recommended to maintain the default calculation mode (Fully Automatic). Changing the calculation mode to Automatic with Minimum Value may result in loss of connectivity with units for which the calculated SNR before the change was relatively low.

The Noise Floor Calculation Parameters submenu includes the following options:

4.2.6.2.16.1 Calculation Mode

The Calculation Mode defines the method used for calculation the Noise Floor value to be used by the device for estimating the quality of received signals. The available options are:

- **Fully Automatic**: According to the built-in noise floor calculation mechanism.
- **Forced**: The Noise Floor value is set manually to the value configured for the Forced Value parameter (see below). Typically this mode should be used only for special testing purposes.
- **Automatic with Minimum Value**: If the calculated Noise Floor using the built-in mechanism is higher than the value configured for the Forced Value parameter, the calculated value will be used. Otherwise, the Forced Value will be used.

The default option is Fully Automatic.

4.2.6.2.16.2 Forced Value

The Forced Value parameter enables configuring the Noise Floor to be used if the selected Calculation Mode is Forced. This is also the minimum value to be used if the selected Calculation Mode is Automatic with Minimum Value.

If you decided to change the calculation mode to Automatic with Minimum Value and you still experience problems in the link (long association time, exceptionally low throughput), try to improve it by increasing the configured Forced Value.

The available range is from -107 to -55 (dBm)

The default value is:

- 10 MHz bandwidth: -99 (dBm)
- 20 MHz bandwidth: -96 (dBm)
- 40 MHz bandwidth: -93 dBm

4.2.6.2.16.3 Show Noise Floor Calculation

Select this option to view the current values of the Noise Floor Calculation parameters and the Noise Floor Current Value (the actual current value used by the device).

4.2.6.2.17 Calibration of Noise Floor Indication

The Calibration of Noise Floor Indication feature has been introduced to overcome possible inaccuracies in the Noise Floor Calculation mechanism. The calibrated Noise Floor Indication is used for correcting the displayed Noise Floor values versus the values that are calculated/used by the internal noise floor calculation mechanism.

The Calibration of Noise Floor Indication submenu includes the following options:

4.2.6.2.17.1 Run Calibration

Select the Run Calibration option to perform a new calibration process. Typically this should be performed for a new unit when Factory calibration is not available, whenever the bandwidth (sub-band) is being changed, or if the previous calibration process has failed.

Calibration can be performed only under the following conditions:

- The Spectrum Analyser is not in progress
- There is no active TFTP or FTP session

- In an RB, only if the RB is associated

If the calibration has started the unit will reset itself, will perform the calibration and after that it will reset again and return to normal mode of operation.

The calibration process may take several minutes: 6 seconds for each of the channels available in the tested sub-band, plus two resets.

If the calibration is running the user will not be able to start a spectrum analysis or a TFTP/FTP session.

If the calibration failed the results of the previous successful calibration will be kept. If the calibration passed, the new results will be used for Noise Floor Indication.

4.2.6.2.17.2 Select Calibration Option to Use

This option enables selection of the calibration option to be used by the device. The available options are None, Field and Factory.

If Factory option is available, indicating that the unit was calibrated in the factory (in the current version Factory calibration is not available), this is the option that should be used.

If Factory option is not available, a Field calibration should be performed (using the Run Calibration option), and the Field option should be selected.

The None option should be used only if the Field Calibration is repeatedly failing (see Show Noise Floor Calibration below), or if the RSSI displayed when using the Field option (following a "successful" Field calibration) is clearly inaccurate, indicating erroneous results.

The default is None.

4.2.6.2.17.3 Show Noise Floor Calibration

Select this option to view the current status and parameters of Calibration of Noise Floor Indication. The displayed parameters are:

- **Field Calibration Status**: Indicating the result of the last Field calibration process (Passed, Failed or None if no Field calibration has been done).

- **Last Field Calibration Result**: Indicating the result of the last Field Calibration process (Success or Failed).

- **Bandwidth Used for Last Field Calibration**: The bandwidth used by the device during the last Field Calibration. A new Field Calibration should be performed after changing the bandwidth (sub-band) used by the device.

- **Available Calibration Options**: Indicating whether Field, Factory or both Field and Factory Calibration options are available for selection.

- **Selected Calibration Option**: The currently selected Calibration Option to Use.

4.2.6.2.18 Interference Mitigation (2.4 GHz units and BU/RB-B10 only)

The Interference Mitigation functionality allows users to configure the unit's operating channel and noise floor level in order to meet particular requirements regarding throughput and distance. The unit will scan and analyse the spectrum, and, depending on the detected noise levels, it will choose an optimal operating channel and noise floor level.

There are two types of optimization mechanisms available. The unit can either find settings that will ensure the best range for a given throughput or settings that will ensure the best throughput for a given range. Based on the topography, the unit estimates a theoretical link budget, and matches it against the noise levels detected during the scan to identify the settings that best meet the user's requirements.

The Interference Mitigation offers a quick and efficient mechanism for setting up links, when the operator doesn't have the time or the expertise required for a full spectrum analysis and channel optimization. For optimal results however, a thorough radio planning performed by a radio specialist is always recommended.

CAUTION



Upon activating the Interference Mitigation, the unit will automatically reset. The unit will enter passive scanning mode for a definite period of time, during which information will be gathered. During the information-gathering period, the unit will not receive nor transmit data. Also, it will not be able to synchronize/associate, meaning that it cannot be managed via the wireless link. At the end of the period, the unit will reset automatically regaining normal operability upon start up.

NOTE



When performing calculations, the Interference Mitigation mechanism also takes into consideration the following parameters which are set in their specific menus:

- Antenna Gain [see "Antenna Gain" on page 120]
- Country Code [see "Country Code Parameters" on page 183] as it affects EIRP and Maximum TX Power limits
- TX Power (BU) [see "Transmit Power" on page 116) and Maximum TX Power (RB) [see "Maximum Transmit Power (RB only)" on page 117)
- Sub-band [see "Sub Band Select" on page 110) as channel bandwidth affects Noise Floor which in turn affects maximum distance

Make sure those parameters are properly configured before activating Interference Mitigation. It is recommended to re-run Interference Mitigation after changing any of the above.

4.2.6.2.18.1 Basic Settings

The Basic Settings menu is used for collecting the primary input required for the analysis process.

4.2.6.2.18.1.1 Installation Model

This setting defines the topography:

- 0 - **LOS**: Units have clear line of sight between them
- 1 - **Near LOS**: Units have minor obstacles in their path, which are easily avoidable through multipath
- 2 - **Non LOS**: Units are obstructed and the signal must travel through longer paths or less permissive media

The default is Near LOS.

4.2.6.2.18.1.2 Minimum Desired Performance

This setting defines the minimum throughput that must be ensured when optimizing the achievable distance. Not applicable when the Optimize Performance for Minimum Desired Distance optimization criterion is used.

The available range is from 500 to 6000 (kbps).

The default is 3000 (kbps).

4.2.6.2.18.1.3 Minimum Desired Distance

This setting defines the minimum achievable distance that must be reached when optimizing the throughput. Not applicable when the Optimize Distance for Minimum Desired Performance optimization criterion is used.

The available range is from 500 to 54000 (meters).

The default is 1400 (meters).

4.2.6.2.18.1.4 Channel Selection Optimization Criteria

This setting allows you to select the optimization mechanism that will be employed:

- 0 - **Optimize Performance for Minimum Desired Distance**: Ensures the best throughput while preserving the Minimum Desired Distance
- 1 - **Optimize Distance for Minimum Desired Performance**: Ensures the best achievable distance while preserving the Minimum Desired Performance

The default is Optimize Distance for Minimum Desired Performance.

4.2.6.2.18.1.5 Scanning Type

This setting defines the output of the analysis process performed by the Interference Mitigation mechanism:

- 0 - **Clear Channel Selection + Automatic Noise Floor Selection**: For optimizing both the operating channel and noise floor level (AU only)
- 1 - **Automatic Noise Floor Selection**: For optimizing only the noise floor level
- 2 - **Clear Channel Selection**: For optimizing only the operating channel (AU only)
- 3 - **Statistics Only**: For performing only a spectrum analysis, without modifying the operating channel or noise floor level

The default is Clear Channel Selection + Automatic Noise Floor Selection.

4.2.6.2.18.2 Advanced Settings

Use this menu to provide additional parameters that will refine the analysis performed by the Interference Mitigation mechanism. The default values for Advanced Settings have been selected to optimize the results while complying with the typical hardware configuration and installation, therefore you may safely ignore these parameters, leaving their default settings in place. However,

experienced users may find some benefit from adjusting the parameters, thus optimizing the results for their specific needs.

4.2.6.2.18.2.1 BU Height

Indicates the height (in meters) of the BU antenna. It is useful for calculating the distance.

The available range is from 15 to 200 (meters).

The default is 30 (meters).

4.2.6.2.18.2.2 BU/RB Antenna Gain

- **RB Antenna Gain**: The antenna gain (in dBi) for a typical RB (BU only).

  The available range is from 9 to 20 (dBi).

  The default is 10 (dBi).

- **BU Antenna Gain**: The antenna gain (in dBi) for the BU (RB only).

  The available range is from 9 to 20 (dBi).

  The default is 10 (dBi).

4.2.6.2.18.2.3 BU/RB Maximum Modulation

- **RB Maximum Modulation**: The maximum modulation of the RBs in the link.

  The available range is from 1 to 8.

  The default is 5.

- **BU Maximum Modulation**: The maximum modulation of the BU in the link.

  The available range is from 1 to 8.

  The default is 8.

4.2.6.2.18.2.4 KeepLink (BU only)

Use this option to instruct the BU to maintain sufficient fade margin after the Noise Floor selection, in order to keep the current association. When this option is enabled, the algorithm considers the uplink SNR of the RB currently in its Association Database and calculates an upper limit for the Noise Floor. When this

option is disabled, there is no upper limit to the Noise Floor value on the BU (except the one imposed by the available range), possibly leading to loss of association for the an RB with lower SNR:

- 0 - **Disable KeepLink**
- 1 - **Enable KeepLink**

The default is 1 (Enabled).

4.2.6.2.18.2.5 Channel Scan Period

The period of time, in seconds, the unit will stay on each channel to gather information. The unit may stop recording prematurely if a 100 000 events limit is reached.

The available range is from 2 to 30 seconds.

The default is 5 seconds.

4.2.6.2.18.2.6 Automatic Scan Period

The period of time, in minutes, after which the unit will rerun the Interference Mitigation channel scan. Setting this value to 0 will disable periodicity, allowing only one-time manually triggered Interference Mitigation scans.

The available range is 0 (disabled) or 10 - 10080 (minutes)

Default value is 0 (disabled).

4.2.6.2.18.2.7 Frequency Subset (BU only)

This setting allows you to select the channels that will be scanned during the Interference Mitigation process. All the defined frequencies and their indexes will be displayed. Frequencies are indexed with consecutive numbers starting from 1. Enter the desired channels' corresponding indexes separated by commas (for example: 1, 4, 5, 6, 14, 18, 19) or enter A to select all defined frequencies.

4.2.6.2.18.3 Activation

Starts the Interference Mitigation process. Keep in mind that during the scan, the BU will lose connectivity to the associated RB. A final validation is required prior to the scan:

- 0 - **Cancel Operation**
- 1 - **Activate Interference Mitigation (Causes Automatic Reset)**

After reset, the Interference Mitigation statistics file will be updated, and depending on the Scanning Type you defined, the unit may be configured to a new

operating channel and/or noise floor. During the Interference Mitigation process, the scan readings and calculation results are updated in real-time in the Event Log. At the end of the process, following the second reset, all feedback from Interference Mitigation can be displayed by reading the Event Log [see "Event Log Menu" on page 67] or by downloading the log file [see Appendix B].

4.2.6.2.18.4 Delete Statistics File

Deletes the Interference Mitigation statistics file created during the previous scan. A final validation is required prior to deletion:

- 0 - **Cancel Operation**
- 1 - **Delete File**

4.2.6.2.18.5 Show Interference Mitigation Parameters & Data

This feature displays a review of the Interference Mitigation settings and the statistics generated during the latest scan (if the statistics file was not deleted in the meanwhile). These statistics include for each defined channel the following parameters:

- Frequency
- Noise Floor
- Achievable Distance
- Maximum Throughput

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 in the RB the IP

address of a connected AP client device to facilitate in the future remote management of a WiFi Access Point connected to the RB.

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 (BU Only)
- Wi2 IP Address (RB 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 RB 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 (BU Only)

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.

Starting on SW Version 5.0, traps are generated and sent only by the BU: relevant events in an RB are reported by the RB to the serving BU that generates the applicable trap on behalf of the RB.

For more details on the system traps see the relevant Traps document.

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 Wi2 IP Address (RB Only)

This parameter is intended for future use to support solutions where WB-B serves as a backhaul link for a WiFi Access Point. The Wi2 IP Address parameter enables the installer to configure in the RB 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 Wi2 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

- Ethernet Broadcast/Multicast Limiter
- Bridge Aging Time
- Roaming Option (RB only)
- Send Broadcasts/Multicasts as Unicasts (BU 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 WB-B 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 WB-B units supports frame routing by port information, whereby each port is connected to only one VLAN.

The VLAN Support menu includes the following parameters:

- VLAN Link Type
- VLAN ID - Data (RB only)
- VLAN ID - Management
- VLAN Forwarding
- VLAN Traffic Priority
- VLAN Extended Access (RB only)
- VLAN ID - Extended Trunk (RB only)

4.2.6.4.1.1 VLAN ID-Data (RB 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 tagged management frames with a matching VLAN ID received on either the Ethernet or wireless link ports are forwarded to the unit.
- A VLAN Management Tag is inserted in all management frames generated by the unit before transmission on either the Ethernet or wireless link port. The tag includes the values of the **VLAN ID-Management** and the **VLAN Priority-Management** parameters.

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

- Only untagged management frames received on either the Ethernet or wireless link ports are forwarded to the unit.
- Management frames generated by the unit are not tagged.

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

Table 4-9: VLAN Management Port Functionality

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

Table Legend:

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

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 and Access Link (Access Link option is available only in RBs).

The default selection is Hybrid Link.

4.2.6.4.1.3.1 Access Link (RB 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 4-10 summarizes the functionality of the data port for an Access link.

Table 4-10: VLAN Data Port Functionality - Access Link

Action	Data Port - RB
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.

Table 4-11 summarizes the functionality of the data port for a Trunk link.

Table 4-11: VLAN Data Port Functionality - Trunk Link

Action	Data Port - BU and RB
Accept from Ethernet	Tagged frames. If Forwarding is enabled, only frames with VLAN ID values which are included in the Forwarding list

Table 4-11: VLAN Data Port Functionality - Trunk Link

Action	Data Port - BU and RB
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 4-12 summarizes the functionality of the data port for a Hybrid link.

Table 4-12: VLAN Data Port Functionality - Hybrid Link

Action	Data Port - BU and RB
Accept from Ethernet	All
Accept from Wireless	All
Tag Insert	No
Tag Remove	No

4.2.6.4.1.4 VLAN Forwarding (BU and RB)

The VLAN Forwarding feature is applicable for Trunk Links only. It enables defining the VLAN ID values to be included in the VLAN Forwarding List. If the Link Type is defined as a Trunk Link and the VLAN Forwarding option is enabled, a data frame received with a VLAN ID that is not a member of the unit's VLAN Forwarding List is discarded.

The VLAN Forwarding submenu provides the following options:

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.

4.2.6.4.1.5 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 WB-B system, including VLAN-based prioritization, are located in the Traffic Prioritization menu.

The VLAN Traffic Priority menu includes the following parameters:

- VLAN Priority - Data (RB only)
- VLAN Priority - Management

4.2.6.4.1.5.1 VLAN Priority - Data (RB only)

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

Valid values range from 0 to 7.

The default value is 0.

4.2.6.4.1.5.2 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 RBs and 0 for BUs.

4.2.6.4.1.6 VLAN Extended Access (RB only)

The VLAN Extended Access menu allows users to define up to 8 different rules for applying VLAN and priority tags on Ethernet to WLAN traffic. Different rules may apply the same VLAN ID.

4.2.6.4.1.6.1 VLAN Rule

Each rule comprises the following parameters:

Table 4-13: VLAN Rule # Parameters

Parameter	Description
VLAN Rule	Defines the type of rule that is going to be applied: ■ **noRule** - No rule is applied. Use this option to deactivate a rule that is currently in use. ■ **srcMac** - The rule will be applied on frames with matching source MAC addresses. ■ **dstMac** - The rule will be applied on frames with matching destination MAC addresses. ■ **srcIp** - The rule will be applied on frames with matching source IP addresses. ■ **dstIp** - The rule will be applied on frames with matching destination IP address. ■ **srcUdpPort** - The rule will be applied on UDP frames with matching source UDP ports. ■ **dstUdpPort** - The rule will be applied on UDP frames with matching destination UDP ports. ■ **srcTcpPort** - The rule will be applied on TCP frames with matching source TCP ports. ■ **dstTcpPort** - The rule will be applied on TCP frames with matching destination TCP ports. ■ **IpProtocol** - The rule will be applied on frames with matching IP protocols. ■ **default** - This rule will be applied on frames that don't match any of the remaining rules. By default, each rule is populated with the **noRule** setting. When a frame matches multiple rule types, the rule type that is highest in the list above (except for the noRule type) will have precedence and any other matching rule will be ignored. For instance, a srcMac rule will have precedence over a dstMac rule, which in turn will have precedence over a srcIp rule, etc. If there are multiple rules of the same type, the lower the rule number, the higher the precedence. For instance, Rule 1 will have precedence over Rule 2, which will have precedence over Rule 3, if rules 1, 2 and 3 have the same type.

Table 4-13: VLAN Rule # Parameters

Parameter	Description
VLAN ID	Defines the VLAN ID tag that is going to be applied to untagged frames in the Ethernet to WLAN traffic. Also, any incoming WLAN traffic tagged with this ID will be routed to Ethernet untagged. This parameter must be configured in order to save the rule. Valid values range from 1 to 4094. If no value is defined for this entry, 0 is returned.
VLAN Priority	Defines the priority tag that is going to be applied to untagged frames in the Ethernet to WLAN traffic. This parameter must be configured in order to save the rule. Valid values range from 0 to 7. If no value is defined for this entry, 255 is returned.
VLAN Multicast Allowed	Defines whether multicast frames are filtered when applying the rule. The available options are: ■ 0 - Multicast frames not allowed ■ 1 - Multicast frames allowed The default value is 0. This setting applies only to Layer 2 multicast frames. It does not apply to Layer 2 broadcast frames or to Layer 3 broadcast or multicast frames. For more information on this topic, see Table 4-14.
VLAN Rule Data Type	Defines the type of data that is defined in the VLAN Rule Data field. The available options are: ■ **1 - Value** - A single value is entered ■ **2 - Range** - A range of consecutive values is entered by typing the first and the last value in the range separated by a space or by a minus symbol (-). ■ **3 - Mask** - An address - mask pair of entries is typed separated by a space or comma symbol (,). The subnet defined in this manner will be the applicable domain for the rule. ■ **4 - Enum** - A set of values is typed separated by comma symbols (,). The default setting is Value.

Table 4-13: VLAN Rule # Parameters

Parameter	Description
VLAN Rule Data	Defines the actual value(s) of the parameters defined in the VLAN Rule and VLAN Rule Data Type fields. Depending on the type of parameter, the following rules apply: ■ **MAC addresses** - The following types of inputs are supported: Value, Range, Mask MAC addresses must be typed in hexadecimal format. All symbols must be adjacent to each other. No separators are allowed inside the address representation. The default setting is 00-00-00-00-00-00. ■ **IP addresses** - The following types of inputs are supported: Value, Range, Mask The default setting is 0.0.0.0. ■ **Port numbers** - The following types of inputs are supported: Value, Range, Enum The default setting is 0. ■ **IP protocols** - The following types of inputs are supported: Value, Enum Each IP protocol is indicated by its protocol number assigned in accordance with the IANA Allocation Guidelines for the Protocol Field (RFC 5237) The default setting is 0.
Save VLAN Rule	Once all the parameters have been set up, use this option to apply the rule
Show VLAN Rule	Displays the rule's parameters values in both its **New** state (settings that were entered but haven't been saved yet) and.**Current** state (settings that are currently in use).

Table 4-14 describes how Layer 2 broadcast and multicast frames are handled and how the VLAN Multicast Allowed setting affects this behavior.

Table 4-14: Layer 2 Broadcast/Multicast Frames' Behavior

Rule Match		Broadcast Frames	Multicast Frames
The frame matches at least one rule		Frame is handled according to the rule with the highest precedence	
No match	VLAN Multicast Allowed Enabled	Frame is multiplied and tagged with each distinct VLAN ID that was specified in the rules.	Frame is multiplied and tagged with each distinct VLAN ID that was specified in the rules.
	VLAN Multicast Allowed Disabled		Frame is dropped

NOTE



An Ethernet frame is considered multicast if the LSB (Least Significant Bit) of the first byte of its MAC address has the value 1.

4.2.6.4.1.6.2 Show Rule List

Lists all the 8 rules along with their current parameters.

4.2.6.4.1.7 VLAN ID - Extended Trunk (RB only)

Indicates the VLAN ID that is going to be tagged into the VLAN untagged frames arriving via Ethernet or removed from the VLAN tagged frames arriving via WLAN when working in Extended Trunk mode.

Valid values range from 1 to 4094.

4.2.6.4.1.8 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 (RB only)

The Ethernet Broadcast Filtering menu enables defining the layer 2 (Ethernet) broadcast and multicast filtering capabilities for the selected RB. 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 RB.

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 BU and RB, 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 RBs, 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 RB 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.

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 WB-B units.

The available range is 20 to 2000 seconds.

The default value is 300 seconds.

4.2.6.4.5 Roaming Option (RB 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 BU after losing connectivity with the current BU only after 7 seconds during which no beacons were received from the current BU. This will prevent scanning for another BU in cases where no beacons were received due to a short temporary problem.

When set to Enable, the RB will wait only one second before it starts scanning for another BU. In addition, when the Roaming Option is enabled, the RB will send Roaming SNAP messages upon associating with a new BU. This enables fast distribution of the new location for all clients that are behind the RB. In this case, the RB will send multicast SNAP messages via the wireless link each time it associates with a new BU, except for the first association after reset. The RB 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 BU that receives this SNAP message learns from it the new location of the clients. It forwards the SNAP to other BUs and Layer-2 networking

equipment via its Ethernet port, to facilitate uninterrupted connectivity and correct routing of transmissions to these clients.

The default is Disable.

4.2.6.4.6 Ports Control (RB only)

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

4.2.6.4.6.1 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.

4.2.6.4.7 Send Broadcasts/Multicasts as Unicasts (BU only)

Starting on SE Version 4.5, Broadcasts and Multicasts are sent by the BU as Unicasts, thus improving communication reliability (Unicasts are acknowledged by the receiving side). The Send Broadcasts/Multicasts as Unicasts option allows disabling or enabling this feature.

The default is Enable.

4.2.6.4.8 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 WB-B wireless link.

The Performance Parameters menu includes the following parameters:

- RTS Threshold
- Minimum Contention Window
- Maximum Contention Window
- Maximum Modulation Level
- Multicast Modulation Level (BU only)
- Control Modulation Level

- Average SNR Memory Factor
- Number of HW Retries
- Burst Mode
- Adaptive Modulation
- Ethernet Frame Size (B10 only)
- 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 4092 bytes.

The default value for BU/RB-B14 and BU/RB-B28 units is 2200 bytes (this is the largest packet size that can be supported by these units when concatenation is enabled).

The default value for BU/RB-B10 and BU/RB-B100 units is 4092 bytes.

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 WB-B system uses a special mechanism based on detecting the presence of a carrier signal to estimate the activity of another unit. 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 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 below) after reaching a decision that the medium has become free.

DIFS equal SIFS plus AIFS, where AIFS is two time slots (in BU/RB-B14/28/100, AIFS for low priority packets can be configured to a value higher than 2 when the Wireless Link Prioritization feature is enabled. See Section 4.2.6.6.3.6).

The system uses an exponential Back-off algorithm to resolve contention between two units that want to access the wireless medium. The method requires each unit 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 AIFS plus N time slots, always checking if another 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 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.

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 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 link.

The link quality can be estimated based on the SNR measurement of the RB at the BU, which can be viewed in the MAC Address Database option in the Site Survey menu, and on the SNR measurement of the BU at the RB, which can be viewed using the Continuous Link Quality Display option. If the measured SNR is less than a certain threshold, it is recommended that the maximum modulation level be decreased in accordance with Table 4-15, 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 BU is accurate only when receiving transmissions from the applicable RB. 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 and maximum values for the Maximum Modulation Level parameter are defined 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.

For BU-B14/28, the maximum modulation with 40 MHz is 5, while for BU-B100 the Maximum Modulation is 8.The default is the highest supported modulation level (modulation level 8 for BU-B100 and modulation level 5 for BU-B14/28).

Table 4-15: 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

Table 4-15: Recommended Maximum Modulation Level*

SNR	Maximum Modulation Level
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 Max Modulation Level according to the Sub Band.

4.2.6.5.5 Multicast Modulation Level (BU 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 intended to unknown recipients. Beacons and other wireless management and control frames are always transmitted at the lowest modulation level according to the Sub Band.

The minimum and maximum values for the Multicast Modulation Level parameter are defined 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.

For BU-B14/28, the maximum modulation with 40 MHz is 5, while for BU-B100 the Maximum Modulation is 8.The default is the lowest supported modulation level (modulation level 1).

4.2.6.5.6 Control Modulation Level

This feature controls the modulation for ACK frames sent by the unit. The ACK modulation can either be set dynamically based on the modulation of the frame it acknowledges or it can be enforced to modulation level 1. The latter is particularly useful for asymmetric links.

For instance, if one unit in the link is capable of receiving frames in modulation 8, while the other can only receive in modulation 2, in theory one of the units should send its data traffic using modulation 8. However, unless it receives the corresponding ACK feedback in modulation 2 or 1, it will not be able to

synchronize and will bring its own Tx modulation down as a result. Setting the ACK modulation to level 1 at the other side of the link will fix this, allowing the unit to acknowledge that frames sent in modulation 8 are successfully received.

The available options are:

- **Basic Rate** - Sets 3 modulation thresholds for the sent ACK frames depending on the modulation of the received frame:

Table 4-16: Basic Rate Mechanism

Received Frame Modulation	Sent ACK Frame Modulation
1,2	1
3,4	3
5,6,7,8	5

- **Modulation Level 1** - Sends all ACK frames in modulation 1.

The default setting is Basic Rate.

4.2.6.5.7 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 BU and is also included in the Adaptive Modulation algorithm information messages transmitted by the BU and the RB. 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

4.2.6.5.8 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.

4.2.6.5.9 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.

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

In RBs and BUs with HW Revision B, Burst Mode cannot be activated when using WEP for data encryption. In units with HW Revision B, 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.

4.2.6.5.9.1 Burst Mode Option

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

The default is Enable.

4.2.6.5.9.2 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).

4.2.6.5.10 Adaptive Modulation

The Adaptive Modulation algorithm enables adapting the modulation level of transmitted data to the prevailing conditions of the applicable radio link. 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.

4.2.6.5.10.1 Adaptive Modulation Option

This submenu allows users to enable/disable the Adaptive Modulation Algorithm. The default selection is Enable.

4.2.6.5.10.2 Adaptive Modulation Algorithm In Use

This submenu allows users to choose between the basic Adaptive Modulation algorithm and the Statistics-Based Rate Control algorithm.

- **Adaptive Modulation**: 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 the last transmission to the relevant unit, and the recent history of successful and unsuccessful transmissions/retransmissions.

  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 the first transmission trial fails, 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.

- **Statistics-Based Rate Control**: The Statistics-Based Rate Control decision algorithm uses statistical analysis of the successfully/unsuccessfully sent packets to determine when lowering the modulation would increase the actual data rate. If the connection is stable, it will periodically check the unit's behavior on the next higher modulation (except on modulation 8) in an attempt to increase the modulation.

In general, the Statistics-Based Rate Control algorithm provides an overall better performance in case of interference and a decrease in the retransmissions' percentage over the original Adaptive Modulation algorithm.

4.2.6.5.10.3 Statistics-Based Rate Control Parameters

NOTE



Statistics-Based Rate Control is only supported in units with HW Revision C or higher.

This submenu configures parameters for the Statistics-Based Rate Control algorithm. When enabled, the Statistics-Based Rate Control algorithm, constantly evaluates the achievable throughput for a particular modulation by counting the number of packets that are successfully transmitted and the packets that are not received and that need to be retransmitted. Based on these statistics, and on each modulation's specific data rate, it will calculate the real throughput that the unit can support in the current conditions for a particular modulation.

When choosing between modulations, up to a limit, a small number of retransmissions on a higher modulation is compensated by the overall better performance ensured by that modulation. When a critical retransmissions percentage is reached however, it is necessary to decrease the modulation to achieve better throughputs as shown in Table 4-17.

Table 4-17: Retransmission Percentage Equivalence

Modulation Level	PHY Rate (Mbps)	PHY Rate Difference Compared to Previous Modulation (Mbps)	Retransmission Percentage Equivalent to PHY Rate Difference
8	54	54-48=6	6/54=11%
7	48	48-36=12	12/48=25%
6	36	36-24=12	12/36=33%
5	24	24-18=6	6/24=25%
4	18	18-12=6	6/18=33%
3	12	12-9=3	3/12=25%
2	9	9-6=3	3/9=33%
1	6		

When the above mentioned retransmission percentages are reached, the Statistics-Based Rate Control algorithm will lower the modulation.

If the connection is stable on a particular modulation, the unit will periodically check whether it can further increase the modulation (except on modulation 8), by

sending a number of test packets using this higher modulation and checking the retransmission rate.

The user can configure a Packet Threshold to Test Up Rate parameter to define the number of successfully transmitted frames after which the unit will test the higher modulation. The number of frames used for this test can also be configured by the user via the Packet No On Upper Rate parameter.

When a frame needs to be retransmitted, the Statistics-Based Rate Control algorithm may gradually decrease the modulation used for retransmitting that particular frame. Based on the Number of HW retries parameter (see "Number of HW Retries" on page 160 for more details), the unit will try to perform the three final retransmission attempts at progressively lower modulations.

The retransmission mechanism described above does not apply for test frames sent for evaluating link quality on higher modulations. If the number of HW retries is lower than 3 or if the initial modulation is lower than 4, the number of modulations used for retransmission will be limited as shown in Table 4-18.

Table 4-18: Examples of Retransmissions on Different Modulation Levels

Scenario	Transmission Attempts	
	Modulation	Tries
Initial Modulation: 8 Number of HW Retries: 10 Total Number of Tries: 1+10 = 11	8	8
	7	1
	6	1
	5	1
Initial Modulation: 6 Number of HW Retries: 5 Total Number of Tries: 1+5 = 6	6	3
	5	1
	4	1
	3	1
Initial Modulation: 7 Number of HW Retries: 2 Total Number of Tries: 1+2 = 3	7	1
	6	1
	5	1
Initial Modulation: 3 Number of HW Retries: 12 Total Number of Tries: 1+12 = 13	3	11
	2	1
	1	1

4.2.6.5.10.3.1 Packet Threshold To Test Up Rate

When the number of frames transmitted on the current modulation reaches this number, the Statistics-Based Rate Control algorithm will test the upper modulation.

The available range is between 10 and 10000.

The default value is 30.

4.2.6.5.10.3.2 Packet No On Upper Rate

This option indicates the number of frames used by the Statistics-Based Rate Control algorithm to test upper modulations.

The available range is between 1 and 3.

The default value is 3.

4.2.6.5.10.3.3 Retries on Lower Modulations

This option enables/disables the retransmissions on lower modulations mechanism described “Statistics-Based Rate Control Parameters” on page 163.

The default value is Enable.

4.2.6.5.10.3.4 RTS Duration Mode

If the RTS mechanism is enabled, when attempting to retransmit frames on lower modulations, the RTS employed may be adjusted so that it pertains to either the initial transmission modulation or the lower retransmission modulation. The available options are:

- **Short RTS Duration**: Retransmission attempts on lower modulations use the RTS duration that applies to the initial transmission modulation.
- **Long RTS Duration**: Retransmission attempts on lower modulations use the RTS duration that applies to the corresponding lower retransmission modulation.

The default value is Short RTS Duration.

4.2.6.5.10.4 Adaptive Modulation Parameters

This submenu configures parameters for the basic Adaptive Modulation 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.

4.2.6.5.10.4.1 Minimum Interval Between Adaptive Modulation Messages

The Minimum Interval Between Adaptive Modulation Messages sets the minimum interval between two consecutive adaptive modulation messages, carrying information on the SNR of received signals.

The available range is from 1 to 3600 seconds.

The default is 4 seconds.

4.2.6.5.10.4.2 Adaptive Modulation Decision Thresholds

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

The default is Normal.

4.2.6.5.11 Ethernet Frame Size (B10 only)

This option configures the maximum Ethernet fame size to either 1600 or 2000 bytes. The 2000 bytes maximal frame size will be enabled only if it is set as such at both ends of the link. If one of the units (BU or RB) uses 1600 bytes frames, the link will use 1600 bytes frames as well.

The available settings are:

- 1600 Bytes
- 2000 Bytes

The default is 1600 bytes.

4.2.6.5.12 Concatenation Parameters

The Concatenation mechanism enables bundling several data frames into a single frame for transmission to the wireless link. This feature improves throughput and reduces the overhead in the wireless medium, by reducing the overhead associated with each transmission. When concatenation is enabled, data packets in the queue of the internal bridge can be accumulated before the concatenated frame is transmitted to the wireless medium. Data frames can be concatenated up to a maximum frame size of 2200 bytes for BU/RB-B14 and BU/RB-B28 units, and 4032 bytes for BU/RB-B10 and BU/RB-B100 units.

A frame is a candidate for bundling into a concatenated frame if all the following conditions are met:

- The frame is a data frame
- The destination is an entity behind the destination BU/RB.
- The destination unit can support the feature (uses SW version 3.0 or higher).

NOTE



If the destination unit uses SW version 3.0 (learned during the Link Capability exchange process), the maximum number of data frames that can be concatenated is limited to two. If the destination unit uses SW version 3.1, the maximum number of data frames that can be concatenated is limited to eight.

When a frame is identified as an eligible candidate for concatenation, it is marked accordingly and will be processed according to the following:

- If there is no other concatenated frame in the queue:
  - » If the hardware queue is empty - the frame is transmitted immediately.
  - » Otherwise (the queue is not empty) - the frame is inserted to the queue.
- If a concatenated frame exists in the queue:
  - » If the combined size of both frames is above the maximum allowed concatenated frame size - both frames are transmitted as two separate frames.
  - » Otherwise (the combined frames size is below the maximum size) - the new frame is added to the concatenated frame. If the number of data frames in the concatenated frame has reached the maximum allowed (applicable only if the destination unit uses SW version 3.0 or 3.1) - the concatenated frame will be transmitted to the wireless medium. Otherwise - the concatenated frame remains in the queue (until the hardware queue becomes free).

NOTE



When a frame is marked as a candidate for concatenation, it will be transmitted as a concatenated frame. If it is not bundled with another data frame before transmission, it will be a concatenated frame with a single data frame (Concatenated Frame Single). If it is bundled with two or more data frames, it will be a concatenated frame with either double data frames (Concatenated Frame Double) or more data frames (Concatenated Frame More).

The Concatenation Parameters submenu includes:

4.2.6.5.12.1 Concatenation Option

The Concatenation Option enables or disables the concatenation mechanism.

The default is Enable.

4.2.6.5.12.2 Maximum Concatenated Frame Size

The Maximum Concatenated Frame Size parameter defines the maximum length (in bytes) for a concatenated frame.

The range for this parameter is:

- 256 to 2200 bytes for BU/RB-B14, BU/RB-B28 units.
- 256 to 4032 bytes for BU/RB-B10, BU/RB-B100 units.

The default values for this parameter are:

- 2200 for BU/RB-B14 and BU/RB-B28 units.
- 4032 for BU/RB-B10, BU/RB-B100 units.

4.2.6.6 Service Parameters

The Service Parameters menu enables defining user filtering, MIR parameters and Traffic Prioritization parameters.

The Service Parameters menu includes the following parameters:

- User Filtering Parameters (RB only)
- MIR Parameters
- Traffic Prioritization

4.2.6.6.1 User Filtering Parameters (RB only)

The User Filtering Parameters submenu enables defining the IP addresses of user devices authorized to access the wireless medium for security and/or control purposes. In addition, it can be used to enable the transmission and reception of specific protocol frames. These filtering options do not affect management frames sent to or generated by the unit.

The User Filtering Parameters menu provides the following options:

4.2.6.6.1.1 User Filtering Option

The User Filtering Option disables or enables the User Filtering feature. The following options are available:

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

The default selection is Disable.

4.2.6.6.1.2 Set/Change Filter IP Address Range

The Set/Change Filter IP Address Ranges option enables defining/updating up to 8 IP address ranges to/from which IP frames are to pass if the User Defined Addresses Only option is selected in the User Filtering Option parameter.

The default Filter IP Address Range is 0.0.0.0 TO 0.0.0.0 (all 8 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).

4.2.6.6.1.3 Delete Filter IP Address Range

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

4.2.6.6.1.4 Delete All User Filtering Entries

The Delete All User Filtering Entries option enables deleting all entries from the Filter IP Address Ranges list.

4.2.6.6.1.5 DHCP Unicast Override Filter

When user filtering is activated, unicast DHCP messages are filtered out; therefore the unit cannot communicate with the DHCP server. The DHCP Unicast Override Filter option enables to overcome this problem. When enabled, unicast DHCP messages pass, overriding the user filtering mechanism.

The default is Disable DHCP Unicast.

4.2.6.6.1.6 Show User Filtering Parameters

The Show All User Filtering Parameters option displays the current value of the User Filtering Option and the list of User Filtering addresses, subnet masks and ranges.

4.2.6.6.2 MIR Parameters

The Maximum Information Rate (MIR) value specifies the maximum data rate available for burst transmissions, enabling to limit it to a value lower than the maximum supported by the unit. The MIR values indicate the achievable net throughput for FTP applications.

The MIR algorithm uses buffers to control the flow of data. To balance the performance over time, a special Burst Duration algorithm is employed to enable higher transmission rates after a period of inactivity. If no data is received from the Ethernet port during the last N seconds, the unit is allowed to transmit N times its allowed IR value without any delay. For example, if the Burst Duration is set to 0.5 second (or more), then after a period of inactivity of 0.5 seconds up to 128 Kbits x 0.5 = 64 Kbits may be transmitted to a unit whose IR is 128 Kbps, without any delay (provided overall conditions in the wireless link allow this burst).

NOTE



RB-B10 units support asymmetric MIR settings, which means that only the aggregated throughput (uplink + downlink) is limited. Setting either the uplink or downlink MIR to a value, will limit the other one to a combined throughput of 10 Mbps. Consequently, when trying to increase one MIR setting, you might have to decrease the other one first, so that the 10 Mbps aggregated limit is never exceeded.

4.2.6.6.2.1 MIR: Downlink (RB only)

Sets the Maximum Information Rate of the downlink from the BU to the RB.

Available values are:

RB-B10: 128 to 4992 Kbps (128 to 9856 Kbps with Balanced MIR)

RB-B14: 128 to 6912 Kbps

RB-B28: 128 to 22016 Kbps

RB-B100: 128 to 107,904 Kbps.

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

The default value is:

RB-B10: 4992 Kbps

RB-B14: 6912 Kbps

RB-B28: 22016 Kbps

RB-B100: 107,904 Kbps

4.2.6.6.2.2 MIR: Uplink (RB only)

Sets the Maximum Information Rate of the uplink from the RB to the BU.

Available values are:

RB-B10: 128 to 4992 Kbps (128 to 9856 Kbps with Balanced MIR)

RB-B14: 128 to 6912 Kbps

RB-B28: 128 to 22016 Kbps

RB-B100: 128 to 107,904 Kbps.

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

The default value is:

RB-B10: 4992 Kbps

RB-B14: 6912 Kbps

RB-B28: 22016 Kbps

RB-B100: 107,904 Kbps

4.2.6.6.2.3 Maximum Burst Duration

Sets the maximum time for accumulating burst transmission rights according to the Burst Duration algorithm.

Available values range from 0 to 2000 (milliseconds).

The default value is 5 (milliseconds), enabling a maximum burst of (0.005 X MIR) Kbps after a period of inactivity of 5 milliseconds or more.

4.2.6.6.2.4 Show MIR Parameters (RB only)

Displays the current values of the MIR parameters.

4.2.6.6.3 Traffic Prioritization

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

The prioritization of the packets is done using different classifiers:

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

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

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

The Low Priority Traffic Minimum Percent parameter can be used to prevent starvation of low priority traffic by ensuring that a certain number of low priority packets is transmitted even at the expense of high priority traffic.

In addition, the Wireless Link Prioritization, which is available in BU B14/28/100 units, enables to configure parameters that affect the prioritization of traffic in the wireless link for packets with high/low priority from different units.

4.2.6.6.3.1 VLAN Priority Threshold

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

Valid values range from 0 to 7.

The default value is 7, which means that all packets get a low priority (equivalent to disabling the VLAN-based classifier).

4.2.6.6.3.2 ToS Prioritization

The ToS Prioritization parameters enable defining prioritization in accordance with either the 3 IP Precedence bits in the IP header in accordance with RFC 791, or the 6 DSCP (Differentiated Services Code Point) bits in accordance with RFC 2474. The ToS Prioritization menu includes the following parameters:

4.2.6.6.3.2.1 ToS Prioritization Option

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

- Disable
- Enable IP Precedence (RFC791) Prioritization
- Enable DSCP (RFC2474) Prioritization

The default is Disable.

4.2.6.6.3.2.2 IP Precedence Threshold

The IP Precedence Threshold parameter is applicable when the ToS Prioritization Option is set to Enable IP Precedence (RFC791) Prioritization. If the value of the 3 IP Precedence bits in the IP header is higher than this threshold, the packet is routed to the High queue. If the value is lower than or equal to this threshold, the packet will be transferred to the Low queue (unless it is assigned a High priority by another classifier).

Valid values range from 0 to 7.

The default value is 4.

4.2.6.6.3.2.3 DSCP Threshold

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

Valid values range from 0 to 63.

The default value is 32.

4.2.6.6.3.3 UDP/TCP Port Ranges Traffic Prioritization

The UDP/TCP Port Ranges Traffic Prioritization parameters enable defining prioritization in accordance with the UDP and/or TCP destination port ranges. The UDP/TCP Port Ranges Traffic Prioritization menu includes the following parameters:

4.2.6.6.3.3.1 UDP/TCP Port Ranges Prioritization Option

The UDP/TCP Port Ranges Prioritization Option defines whether port ranges based prioritization is enabled or disabled. The following options are available:

- Disable
- Enable Only for UDP
- Enable Only for TCP
- Enable for both UDP and TCP

The default is Disable.

4.2.6.6.3.3.2 UDP Port Ranges

The UDP Port Ranges menu enables defining port ranges to be used as priority classifiers when the UDP/TCP Port Ranges Prioritization Option is set to either Enable Only for UDP or Enable for both UDP and TCP. All packets whose destination is included in the list will be routed to the High queue. All other packets will be routed to the Low queue (unless they were assigned a High priority by another classifier).

The UDP Port Ranges menu includes the following options:

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

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

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

  The available options are:

  - » RTP & RTCP
  - » RTP Only

  The default is RTP & RTCP

- **Add UDP Port Ranges**: This option enables adding UDP port ranges to the list of priority port numbers. The list can include up to 64 ranges. It is possible to add discrete port numbers and/or ranges. In ranges, a hyphen is used to separate between start and end port numbers. A comma is used to separate entries. For example: 8900,9000-9005,9010,9016-9017.

- **Delete UDP Port Ranges**: This option enables deleting UDP port ranges from the list of priority port numbers. It is possible to delete discrete port numbers and/or ranges. In ranges, a hyphen is used to separate between start and end port numbers. A comma should be used to separate between entries.

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

- **Delete All UDP Port Ranges**: This option enables deleting all UDP port ranges from the list of priority port numbers.

- **Show UDP Port Ranges**: Select this option to view the current UDP RTP/RTCP Prioritization option and the list of UDP Port Ranges.

4.2.6.6.3.3.3 TCP Port Ranges

The TCP Port Ranges menu enables defining port ranges to be used as priority classifiers when the UDP/TCP Port Ranges Prioritization Option is set to either Enable Only for TCP or Enable for both UDP and TCP. All packets whose destination is included in the list will be routed to the High queue. All other packets will be routed to the Low queue (unless they were assigned a High priority by another classifier).

The TCP Port Ranges menu includes the following options:

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

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

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

The available options are:

» RTP & RTCP

» RTP Only

The default is RTP & RTCP

- **Add TCP Port Ranges**: This option enables adding TCP port ranges to the list of priority port numbers. The list can include up to 64 ranges. It is possible to add discrete port numbers and/or ranges. In ranges, a hyphen is used to separate start and end port numbers. A comma is used to separate entries.

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

- **Delete TCP Port Ranges**: This option enables deleting TCP port ranges from the list of priority port numbers. It is possible to delete discrete port numbers and/or ranges. In ranges, a hyphen is used to separate start and end port numbers. A comma is used to separate entries.

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

- **Delete All TCP Port Ranges**: This option enables deleting all TCP port ranges from the list of priority port numbers.

- **Show TCP Port Ranges**: Select this option to view the current TCP RTP/RTCP Prioritization option and the list of TCP Port Ranges.

4.2.6.6.3.4 IP Range Prioritization

The IP Range Prioritization menu allows prioritization based on the frame's source and/or destination IP address. Frames with matching IPs are allocated to the High Priority queue, while the rest of the frames are allocated to the Low Priority queue.

4.2.6.6.3.4.1 IP Range Prioritization Option

This submenu sets up the type of IP prioritization employed

- **Disable**: The IP prioritization is disabled.

- **Source IP Prioritization**: Frames with matching source IP addresses will be allocated to the High Priority queue.
- **Destination IP Prioritization**: Frames with matching destination IP addresses will be allocated to the High Priority queue.
- **Source or Destination IP Prioritization**: Frames with either source or destination IP addresses within the IP range will be allocated to the High Priority queue.

4.2.6.6.3.4.2 IP Range Address

This option defines the base IP address which, in conjunction with the range mask, defines the IP range used for prioritization.

The values are entered as 4 groups of up to 3 digits separated by dots.

The default value is 0.0.0.0.

4.2.6.6.3.4.3 IP Range Mask

This option defines the range mask which, in conjunction with the base IP address, defines the IP range used for prioritization.

The values are entered as 4 groups of up to 3 digits separated by dots.

The default value is 255.0.0.0.

4.2.6.6.3.5 Low Priority Traffic Minimum Percent

This feature ensures that a certain amount of low priority packets, specified by the Low Priority Traffic Minimum Percent (LPTMP) parameter, is transmitted even at the expense of high priority traffic.

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

The range is between 0 and 100 (%).

The default value is 0 (%).

NOTE



The Low Priority Traffic Minimum Percent parameter is not applicable when the Wireless Link Prioritization Option is enabled.

4.2.6.6.3.6 Wireless Link Prioritization Parameters (BU-B14/28/100)

To better support delay-sensitive and other high-priority traffic, a set of Wireless Link Prioritization parameters enables configuring parameters that affect the processes of gaining access to the wireless media and the of transmitting high/low priority packets.

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

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

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

Under regular conditions, AIFS is configured to two time slots. To support prioritization in the wireless link, we can configure a higher AIFS for low priority traffic (AIFS of two time slots will always be used for high priority traffic as well as BU's transmissions of broadcasts/multicasts and beacons). This will give advantage to units that need to transmit high priority traffic (depending also on the configured values for the Contention Window parameters).

Other parameters related to transmission to the wireless media that can be configured separately for high/low priority packets are the Number of HW Retries and Burst Duration.

Typically, a lower value of Number of HW Retries should be configured for traffic such as VoIP, which on the one hand is sensitive to delays and on the other hand is less sensitive to missing packets than data traffic.

The Burst Duration, which defines the maximum duration of a burst, should be set to a lower value for delay sensitive traffic.

When the Wireless Link Prioritization feature is enabled, the following parameters are not applicable:

- Arbitration Inter-Frame Spacing (AIFS)

- Number of HW Retries
- Burst Mode Option
- Burst Mode Time Interval
- Low Priority Traffic Minimum Percent

The Wireless Link Prioritization Parameters menu includes the following:

4.2.6.6.3.6.1 Wireless Link Prioritization Option

The Wireless Link Prioritization Option enables or disables the Wireless Link Prioritization feature.

The default option is Disable.

4.2.6.6.3.6.2 Low Priority AIFS

The Low Priority AIFS defines the AIFS number of time slots that will be used by the BU and the RB served by it for low priority traffic.

The range is from 3 to 50 (time slots).

The default is 10.

4.2.6.6.3.6.3 Number of HW Retries for High Priority Traffic

The Number of HW Retries for High Priority Traffic defines the maximum number of times that an unacknowledged high priority unicast packet can be retransmitted. This is the value that will be used by the ABU and by the RB served with it.

The range is from 1 to 14 times.

The default is 10 times.

4.2.6.6.3.6.4 Number of HW Retries for Low Priority Traffic

The Number of HW Retries for Low Priority Traffic defines the maximum number of times that an unacknowledged low priority unicast packet can be retransmitted. This is the value that will be used by the BU and by the RB served with it.

The range is from 1 to 14 times.

The default is 10 times.

4.2.6.6.3.6.5 BU Burst Duration for High Priority Traffic

The BU Burst Duration for High Priority Traffic parameter defines the maximum duration of a burst that can be made by the BU for high priority packets.

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

The default is 20 (5 milliseconds).

4.2.6.6.3.6.6 BU Burst Duration for Low Priority Traffic

The BU Burst Duration for Low Priority Traffic parameter defines the maximum duration of a burst that can be made by the BU for low priority packets.

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

The default is 12 (3 milliseconds).

4.2.6.6.3.6.7 RB Burst Duration for High Priority Traffic

The RB Burst Duration for High Priority Traffic parameter defines the maximum duration of a burst that can be made by the RB for high priority packets.

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

The default is 20 (5 milliseconds).

4.2.6.6.3.6.8 RB Burst Duration for Low Priority Traffic

The RB Burst Duration for Low Priority Traffic parameter defines the maximum duration of a burst that can be made by the RB for low priority packets.

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

The default is 12 (3 milliseconds).

4.2.6.6.4 Show Service Parameters

Displays the current values of the Service Parameters.

4.2.6.7 Security Parameters

WB-B can support encryption of authentication messages and/or data frames using one of the following encryption standards:

- **WEP** Wired Equivalent Privacy algorithm. WEP is defined in the IEEE 802.11 Wireless LAN standard and is based on the RSA's RC4 encryption algorithm.

- **AES OCB** Advanced Encryption Standard. AES is defined by the National Institute of Standards and Technology (NIST) and is based on Rijndael block cipher. AES OCB (Offset Code Book) is a mode that operates by augmenting the normal encryption process by incorporating an offset value.

- **FIPS 197** is certified for compliance with Federal Information Processing Standards. It provides encryption and message integrity in one solution and implements the Advanced Encryption Standard using Rijndael block cipher.

The following parameters are available through the Security Parameters menu (in certain units some or all of the security options may not be available):

- Authentication Algorithm
- Data Encryption Option
- Security Mode
- Default Key (RB only)
- Default Multicast Key (BU only)
- Key # 1 to Key # 4
- Promiscuous Authentication (BU only)

4.2.6.7.1 Authentication Algorithm

The Authentication Algorithm option determines the operation mode of the selected unit. The following two options are available:

- **Open System**: An RB configured to Open System can only associate with a BU also configured to Open System. In this case, the authentication encryption algorithm is not used.
- **Shared Key**: The authentication messages are encrypted. An RB configured to use a Shared Key can only be authenticated by a BU configured to use a Shared Key, provided the applicable Key (which means both the key number and its content) in the BU is identical to the key selected as the Default Key in the RB.

  The default is Open System.

NOTE



The Shared Key option cannot be selected before at least one Key is defined. In the RB, a Default Key that refers to a valid Key must be selected.
The BU and the RB it serves should be configured to the same Authentication Algorithm option.

4.2.6.7.2 Data Encryption Option

The Data Encryption Option allows enabling or disabling data encryption. When enabled, all data frames, including frames using management protocols such as Telnet, FTP, TFTP, SNMP, DHCP and ICMP, are encrypted.

The default is Disable.

NOTE



- The BU and the RB it serves should be configured to the same Data Encryption Option.
- A unit with Data Encryption Option enabled can accept non-encrypted data frames

4.2.6.7.3 Security Mode

The Security Mode option enables selecting the algorithm to be used for encrypting the authentication messages and/or data frames.

The available options are WEP, AES OCB and FIPS 197.

The default is WEP.

NOTE



The BU and the RB it serves should be configured to the same Security Mode option.

4.2.6.7.4 Default Key (RB only)

The Default Key defines the Key to be used for encrypting/decrypting the authentication messages (Shared Key mode) and/or data frames (Data Encryption enabled). The BU learns the Default Key from the RB.

Available values range from 1 to 4.

The default is KEY # 1.

4.2.6.7.5 Default Multicast Key (BU only)

The Multicast Default Key defines the Key to be used for encrypting multicasts and broadcasts when Data Encryption is enabled.

Available values range from 1 to 4.

The default is KEY # 1.

4.2.6.7.6 Key # 1 to Key # 4

The Key # options enables defining the encryption key to be used for initializing the pseudo-random number generator that forms part of the encryption/decryption process. The Keys must be set before the Shared Key

authentication algorithm or Data Encryption can be used. To support proper operation, both the Key # and the content must be identical at both sides of a wireless link.

Each Key is a string of 32 hexadecimal numbers. For security reasons, it is a "write only" parameter, displayed as a string of asterisks ("*").

The default for all 4 Keys is 000…0 (a string of 32 zeros), which means no key.

4.2.6.7.7 Promiscuous Authentication (BU only)

The Promiscuous Authentication mode enables a new RB to become associated with a BU where Shared Key operation and/or Data Encryption are used, even if this RB does not have the correct security parameters. In promiscuous mode, all downlink transmissions (from BU to RB) are not encrypted, allowing remote configuration of security parameters, regardless of the current settings in the RB of the parameters related to data encryption. After the RB is associated it should be remotely configured with the proper parameters (or upgraded). When the RB is configured properly, the Promiscuous Mode should be disabled.

The default is Disable.

NOTE



Do not leave the BU in the enabled Promiscuous Authentication mode for prolonged periods. Use it only when absolutely necessary, perform the required actions as quickly as possible and disable it. The unit will return automatically to Promiscuous Authentication disabled mode after reset.

4.2.6.8 Country Code Parameters

4.2.6.8.1 Country Code Select

The Country Code Select option enables changing the Country Code used by the unit.

The default Country Code is set in factory according to the destination country.

CAUTION



The selected Country Code must comply with applicable local radio regulations.

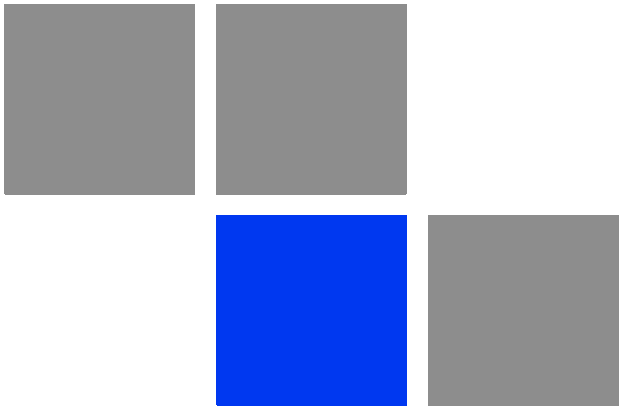
4.2.6.8.2 Re-apply Country Code Values

After loading a new SW version with any changes in the relevant Country Code, the Re-apply Country Code Values option must be activated for the changes to take effect. Following activation of this feature, the unit must be reset to fully apply the changes.



NOTE

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



Chapter A

Software Version Loading Using TFTP

Firmware upgrades to the unit's FLASH memory can be performed by a simple loading procedure using a TFTP application. Before performing an upgrade procedure, be sure you have the correct files and most recent instructions.

NOTE



Shutting down power to the unit before completion of the loading procedure may cause the unit to be inoperable.



To load software versions:

1. Verify that IP connectivity to the required unit is established.
2. Ensure that the IP address of the PC from which the upgrade is to be performed belongs to the same subnet as the unit to be upgraded, unless the unit is behind a router. If the unit is behind a router, verify that the unit is configured with the correct **Default Gateway Address**.
3. To view the current IP parameters of the unit, use the Monitor program by connecting the PC to the unit either directly or via Telnet. To access the IP parameters via the Monitor program:
   a. From the *Main Menu* select **1 - Info Screens**.
   b. From the *Info Screen* menu select **2 - Show Basic Configuration**. The current basic configuration is displayed, including the run time values for the IP Address, Subnet Mask and Default Gateway Address parameters.
4. To modify any of the IP parameters:
   a. From the *Main Menu*, select **3 - Basic Configuration**.
   b. To configure the IP address, select: **1 - IP Address**.
   c. To configure the subnet mask, select **2 - Subnet Mask**.
   d. To configure the default gateway address, select **3 - Default Gateway Address**.
   e. Reset the unit to apply the new IP parameters.
5. To verify the connection, PING the unit's IP address and verify that PING replies are being received.
6. Use the TFTP utility, with the following syntax, to perform the upgrade:

tftp -i hostaddress put sourcefile [destinationfile]

where *-i* is for binary mode and *hostaddress* is the IP address of the unit to be upgraded. *put* causes the PC client to send a file to the *hostaddress*.

7 The original *sourcefile* name of SW files is in the structure uX_Y_Z.bz, where u is the unit type (a for BU, s for RB) and X.Y.Z is the version number.

8 *destinationfile* is the name of the file to be loaded. Use the SNMP write community <SnmpWriteCommunity>.bz to define the destination filename. The default SNMP write community is private. For example, to load the upgrade file a5_0_13.bz to a BU whose IP address is *206.25.63.65: tftp -i 206.25.63.65 put a5_0_13.bz private.bz*

9 When the loading is complete, the following message is displayed, indicating completion of the TFTP process:

Download operation has been completed successfully

10 The unit decompresses the loaded file and checks the integrity of the new version. The new version replaces the previous shadow version only after verification. If verification tests fail, the loaded version will be rejected. Among other things that are tested, the unit will reject a file if either the file name or the version number matches either the current Main or Shadow versions. The unit will also reject a file designated for a different unit type, e.g. a BU upgrade file with the prefix a in the original file name will not be accepted by RBs.

11 The FLASH memory can store two software versions. One version is called *Main* and the second version is called *Shadow*. The new version is loaded into the Shadow (backup) FLASH memory. To check that the new firmware was properly downloaded and verified, view the firmware versions stored in the FLASH, as follows:

a From the Main Menu, select **2 - Unit Control**.

b From the Unit Control menu, select **5 - Flash Memory Control**.

c From the *Flash Memory Control* menu, select **S - Show Flash Versions**. The following information is displayed:

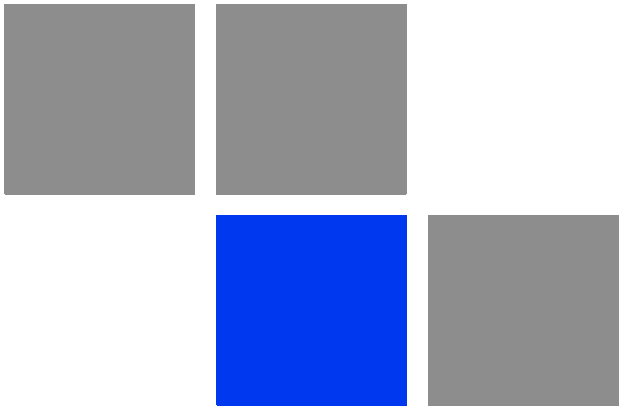
```
Flash Versions
============
Running from                :Main Version
Main Version File Name      :4_5_16.bz
Main Version Number         :4.5.16
```

Shadow Version File Name :5_0_13.bz
File Name Number :5.0.13

NOTE



After loading a new SW version with any changes in the relevant Country Code, these changes must be applied by activation the Re-apply Country Code Values option in the Unit Control Menu. Note that following activation of the Re-apply Country Code Values option, all parameters that are affected by the Country Code (frequency parameters, transmit power parameters, DFS operation, modulation level parameters, burst mode parameters) revert to their factory default values and must be re-configured.



Chapter B



File Download and Upload Using TFTP

The WB-B File Download/Upload feature simplifies the task of remotely configuring a large number of units using TFTP protocol. By downloading the configuration file to a PC it is possible to view all the parameters configured for the unit, as a plain ASCII text file. It is necessary to edit the file using a simple editor and remove certain parameters or change their values prior to uploading the configuration to another unit. The file loading procedure can also be used for uploading a feature license file to multiple units.

When multiple configurations are being done simultaneously, that is, the file is being uploaded to several units, it is recommended that the file will include only the required parameters.

In the configuration file, the following three fields represent each parameter:

1. A symbolic string similar to the name of the parameter in the Monitor program, followed by "=".
2. The value of the parameters, which uses the same values as the Monitor program.
3. An optional comment. If used, the comment should start with a ";" character.

An unknown parameter or a known parameter with a value that is invalid or out of range will be ignored.

Use the SNMP write community string (the default is "private") to define both the uploaded file (*put*) and the downloaded file (*get*). The file should be transferred in ASCII mode.

Use the extension .cfg for a configuration file.

Use the extension .cmr for the Operator Defaults file.

Use the extension .fln for a Feature License file.

Feature license files include multiple strings, where each string is applicable only for a certain unit identified by its MAC address. When uploading a feature license file to multiple units, each unit will accept only the parts that are applicable for itself.

Use the SNMP read community string (the default is "public") to define the downloaded log file (get). The log file should be transferred in binary image mode (-i option).

Examples:

1. To upload the configuration file using a DOS based TFTP Client to an RB whose IP address is 206.25.63.65, enter:
   tftp 206.25.63.65 put Suconf private.cfg

2 To download the Operator Defaults file from the same unit, enter:
tftp 206.25.63.65 get private.cmr Suconf

3 To upload the Feature Upgrade file to the same unit, enter:
tftp 206.25.63.65 put Suconf private.fln

4 To download the Counter Debug file from the same unit, enter:
tftp 206.25.63.65 get private.cdf Suconf

5 To download the Log file from the same unit, enter:
tftp -i 206.25.63.65 get public.log Suconf

NOTE



The Configuration File Loading mechanism is common to BWA VL and WB-B product lines. The Configuration File includes also parameters that are applicable only to BWA VL products. Do not attempt to change the default values of these parameters.

Chapter C

Using the Set Factory Defaults Utility

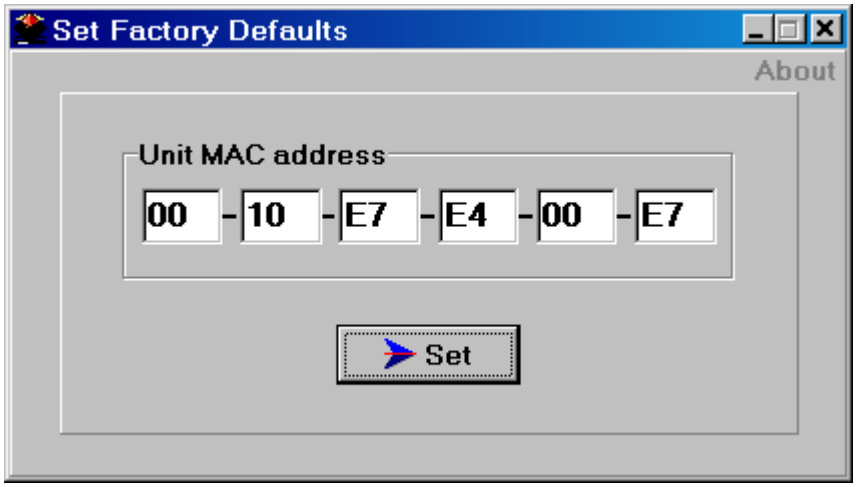
The Set Factory Defaults Utility is intended to enable management access to a unit in cases where such access is not possible due to wrong or unknown configuration of certain parameters. This includes cases such as unknown Management VLAN ID and wrong management access filtering.

The utility accesses the unit by sending a special packet. Access to the unit is based on its MAC address, which must be entered in the **Unit MAC address** field.

The set unit defaults feature is only available via the Ethernet port.

To set factory defaults:

1 Connect the PC with the Set Factory Defaults utility to the Ethernet port of the unit.



2 Enter the unit's MAC address.

3 Click on the **Set** button.

This utility performs the same operation as Set Complete Factory Defaults, restoring the default factory configuration of all parameters, except to Passwords, general FTP parameters and BU's Frequency.

Chapter D

Preparing the Indoor to Outdoor Cable

The Indoor-to-Outdoor cable provides pin-to-pin connection on both ends.

Figure D-1 shows the wire pair connections required for the Indoor-to-Outdoor cable.

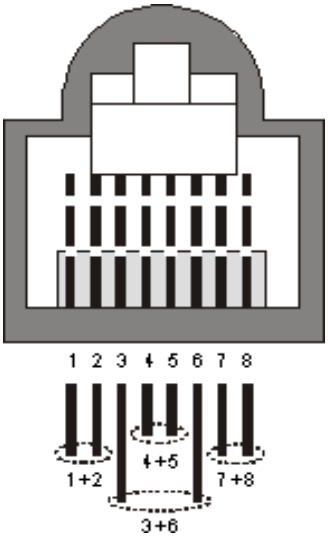


Figure D-1: Ethernet Connector Pin Assignments

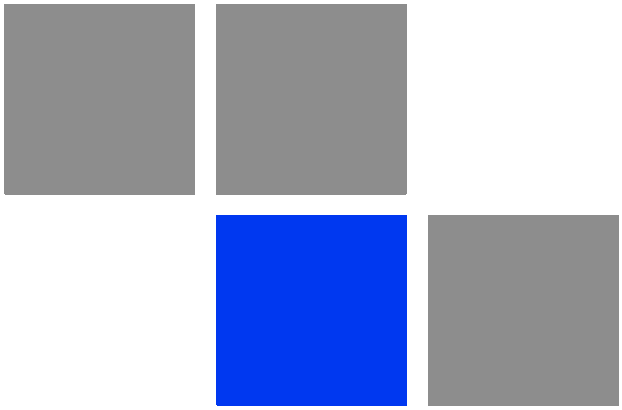
The color codes used in cables that are supplied with crimped connectors are as listed in the following table:

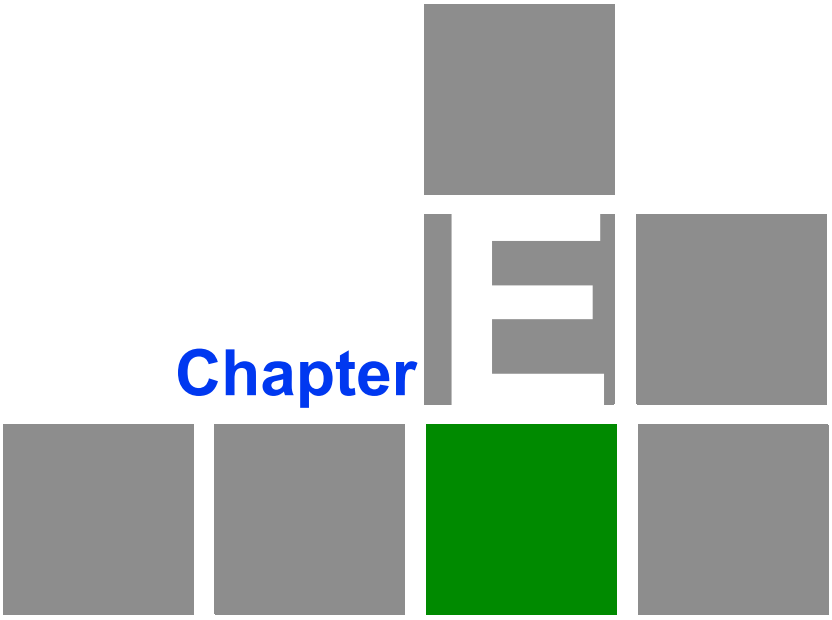
Table D-1: Cable Color Codes

Wire color	Pin
Blue	1
Blue/white	2
Orange	3
Orange/white	6
Brown	4
Brown/white	5
Green	7
Green/white	8

Use a crimp tool for RJ-45 connectors to prepare the wires, insert them into the appropriate pins and use the crimp tool to crimp the connector. Make sure to do the following:

1. Remove as small a length as possible of the external jacket. Verify that the external jacket is well inside the service box to ensure good sealing.
2. Take back the shield drain wire before inserting the cable into the RJ-45 connector, to ensure a good connection with the connector's shield after crimping.





Chapter 13

Parameters Summary

In this Appendix

The tables provide an at a glance summary of the configurable parameters, value ranges, and default values. In addition, each parameter entry also includes an indication as to whether the parameter is updated in run-time or whether the unit must be reset before the modification takes effect ("No" in the Run-Time column indicates that a change to the parameter will take effect only after reset).

E.1 Parameters Summary

E.1.1 Unit Control Parameters

Parameter	Unit	Range	Default	Run-Time
Change Unit Name	BU, RB	Up to 32 printable ASCII characters	None	Yes
Change Unit Type To BU / RB	BU, RB	■ Disable ■ Enable	Disable	No
Change Read Only Password	BU, RB	Up to 8 printable ASCII characters	public	No
Change Installer Password	BU, RB	Up to 8 printable ASCII characters	user	No
Change Administrator Password	BU, RB	Up to 8 printable ASCII characters	private	No
FTP SW Version File Name	BU, RB	Up to 20 printable ASCII characters. An empty string is not allowed.	VxWorks.bz	Yes
Configuration File Name	BU, RB	Up to 20 printable ASCII characters. An empty string is not allowed.	config.cfg	Yes
Operator Defaults File Name	BU, RB	Up to 20 printable ASCII characters. An empty string is not allowed.	operator.cmr	Yes
FTP Source Dir	BU, RB	Up to 80 printable ASCII characters. Use "." to clear.	None (empty)	Yes
FTP Server IP Address	BU, RB	IP address	10.0.0.253	Yes
FTP Gateway IP Address	BU, RB	IP address	None (empty)	Yes
FTP User Name	BU, RB	Up to 18 printable ASCII characters	vx	Yes
FTP Password	BU, RB	Up to 18 printable ASCII characters	vx	Yes
FTP Log File Name	BU, RB	Up to 20 printable ASCII characters	logfile.log	Yes
FTP Log File Destination Directory	BU, RB	Up to 80 printable ASCII characters. Use "." to clear.	None (empty)	Yes

Parameter	Unit	Range	Default	Run-Time
Event Log Policy	BU, RB	■ Message ■ Warning ■ Error ■ Fatal ■ Log None	Warning	Yes
Log Out Timer	BU, RB	1 999 minutes	5	Yes
Ethernet Port Negotiation Mode	BU, RB	■ 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	Auto Negotiation	No
Change System Location	BU, RB	Up to 34 printable ASCII characters	None	Yes
Manual Feature Upgrade	BU, RB	License string: 32 to 64 hexadecimal digits	None	No
Change Mode	BU, RB	■ Normal Mode ■ Threshold Mode ■ Stealth Mode	Normal Mode	Yes
Threshold Type	BU, RB	■ Disabled ■ RSSI ■ CRC % ■ SNR ■ Average Modulation	Disabled	Yes
Threshold Mode	BU, RB	■ Equal or lower than ■ Equal or higher than ■ Equal to	Equal to	Yes

E.1.2 IP Parameters

Parameter	Unit	Range	Default	Run-Time
IP Address	BU, RB	IP address	10.0.0.1	No
Subnet Mask	BU, RB	IP address	255.0.0.0	No
Default Gateway Address	BU, RB	IP address	0.0.0.0	No
DHCP Option	BU, RB	■ Disable ■ DHCP Only ■ Automatic	Disable	No
Access to DHCP	BU, RB	■ From Wireless Only ■ From Ethernet Only ■ From Both Wireless and Ethernet	BU: From Ethernet Only RB: From Wireless Only	No

E.1.3 Air Interface Parameters

Parameter	Unit	Range	Default	Run-Time
ESSID	BU, RB	Up to 31 printable ASCII characters	ESSID1	No
Operator ESSID Option	BU	■ Disable ■ Enable	Enable	No
Operator ESSID	BU	Up to 31 printable ASCII characters	ESSID1	No
Hidden ESSID Option	BU	■ Disable ■ Enable	Disable	No
Hidden ESSID Support	RB	■ Disable ■ Enable	Disable	No
Hidden ESSID Timeout	RB	1 - 60 (minutes)	10 (minutes)	Yes
Arbitration Inter-Frame Spacing (AIFS)	BU, RB	1 - 50 (time slots)	2 (time slots)	Yes
Best BU Support	RB	■ Disable ■ Enable	Disable	No
Number of Scanning Attempts	RB	1 - 255	4	No

Parameter	Unit	Range	Default	Run-Time
Preferred BU MAC Address	RB	MAC Address	00-00-00-00-00-00 (no preferred BU)	No
Scanning Mode	RB	Passive, Active	Passive	No
Wireless Link Trap Threshold	BU	1-100 (%)	30 (%)	No
Sub Band Select*	BU	According to the Country Code	1	Yes
Frequency	BU	According to the Sub Band	The lowest frequency in the Sub Band	Yes
User Defined Frequency Subsets	RB	All frequencies in the available Sub Bands	All available frequencies in all available Sub Bands	Yes
DFS Required by Regulations **	BU, RB	■ No ■ Yes	Dependent on Country Code	Yes****
Frequency Subset Definition (in BU)**	BU	According to the Sub Band. A list of frequency indexes or A for all frequencies supported by the Sub Band	A (All)	Yes
Channel Check Time**	BU, RB	1 - 3600 (seconds)	60 (seconds)	Yes
Channel Avoidance Period**	BU, RB	1 - 60 (minutes)	30 (minutes)	Yes
RB Waiting Option**	BU	■ Disable ■ Enable	Enable	Yes
Minimum Pulses to Detect**	BU, RB	1-100	4 for FCC 8 for other (ETSI)	Yes
Channel Reuse Option**	BU, RB	■ Disable ■ Enable	Disable	Yes
Radar Activity Assessment Period**	BU, RB	1 - 12 hours	5 hours	Yes
Maximum Number of Detections in Assessment Period**	BU, RB	1 - 10 detections	5 detections	Yes

Parameter	Unit	Range	Default	Run-Time
DFS Detection Algorithm	BU, RB	Applicable only for Universal Country Code in 5.4/5.8 GHz: ■ ETSI ■ FCC	ETSI	Yes
Clear radar Detected Channels After Reset**	BU	■ Disable ■ Enable	Disable	Yes
Transmit Power	BU, RB	-10 dBm to a value that depends on HW revision and Country Code / Antenna Gain	The highest allowed value	Yes
Maximum Tx Power	RB	-10 dBm to a value that depends on HW revision and Country Code / Antenna Gain	The highest allowed value	Yes
ATPC Option	BU, RB	■ Disable ■ Enable	Enable	Yes
Delta from Minimum SNR Level	BU	4-20 (dB)	Units in 2.4, 5.4 or 5.8 GHz bands: 5 Units in 5.2 or 5.3 GHz bands: 8	Yes
Minimum SNR Level	BU	4-60 (dB)	28 (dB)	Yes
Minimum Interval Between ATPC Messages	BU	1-3600 (seconds)	30 (seconds)	Yes
ATPC Power Level Steps	BU	1-20 (dB)	4	Yes
Link Distance Mode	BU	Automatic, Manual	Automatic	No
Maximum Link Distance	BU	0-54 (Km) 0 means no compensation	0 (no compensation(	Yes
Fairness Factor	BU	0-100 (%)	100 (%)	Yes
Tx Control	BU	■ Off ■ On ■ Ethernet Status Control	On	Yes

Parameter	Unit	Range	Default	Run-Time
Antenna Gain***	BU, RB	Minimum: 0 (dBi) Maximum: 50 or Regulation Max EIRP+10 (the lower of the two values).	"Don't Care" or "Not Set Yet" or 21 (depending on unit type and regulations)	No
Spectrum Analysis Channel Scan Period	BU, RB	2 - 30 seconds	5 seconds	Yes (Configured per analysis)
Spectrum Analysis Scan Cycles	BU, RB	1 - 100 cycles	2 cycles	Yes (Configured per analysis)
Automatic Channel Selection	BU	■ Disable ■ Enable	Disable	Yes (Configured per analysis)
Lost Beacons Watchdog Threshold	BU	100 - 1000, 0 means Not Used	218	Yes
Noise Immunity State Control	BU, RB	■ Automatic ■ Manual	Automatic	Yes
Noise Immunity Level	BU, RB	0 - 4 Use only 0 or 4	0	Yes
Spur Immunity Level	BU, RB	0 - 7	0	Yes
OFDM Weak Signal	BU, RB	0 (not active) or 1 (active)	0	Yes
Pulse Detection Sensitivity	BU, RB	■ Low ■ High	Low	Yes
Noise Floor Calculation Mode	BU, RB	■ Fully Automatic ■ Forced ■ Automatic with Minimum Value	Fully Automatic	Yes
Noise Floor Forced Value	BU, RB	-107 to -55 (dBm)	10 MHz bandwidth: -99 20 MHz bandwidth: -96 40 MHz bandwidth: -93	Yes

Parameter	Unit	Range	Default	Run-Time
Select Calibration Option to Use	BU, RB	■ None ■ Field ■ Factory (not available in current release)	None	Yes
Installation Mode	2.4 GHz and BU/RB-B10	■ LOS ■ Near LOS ■ Non LOS	Near LOS	No
Minimum Desired Performance	2.4 GHz and BU/RB-B10	500 to 6000 (kbps)	3000 kbps	No
Minimum Desired Distance	2.4 GHz and BU/RB-B10	500 to 54000 (meters)	1400 (meters)	No
Channel Selection Optimization Criteria	2.4 GHz and BU/RB-B10	■ Optimize Performance for Minimum Desired Distance ■ Optimize Distance for Minimum Desired Performance	Optimize Distance for Minimum Desired Performance	No
Scanning Type	2.4 GHz and BU/RB-B10	■ Clear Channel Selection + Automatic Noise Floor Selection ■ Automatic Noise Floor Selection ■ Clear Channel Selection ■ Statistics Only	Clear Channel Selection + Automatic Noise Floor Selection	No
BU Height	2.4 GHz and BU/RB-B10	15 to 200 (meters)	30 (meters)	No
RB Antenna Gain	2.4 GHz and BU-B10	9 to 20 (dBi)	10 (dBi)	No
BU Antenna Gain	2.4 GHz and RB-B10	9 to 20 (dBi)	10 (dBi)	No

Parameter	Unit	Range	Default	Run-Time
RB Maximum Modulation	2.4 GHz and BU/RB-B 10	1 to 8	5	No
BU Maximum Modulation	2.4 GHz and BU/RB-B 10	1 to 8	8	No
Keep Link	2.4 GHz and BU-B10	■ Disable KeepLink ■ Enable KeepLink	Enabled	No
Channel Scan Period	2.4 GHz and BU/RB-B 10	2 to 30 (seconds)	5	No
Automatic Scan Period	2.4 GHz and BU/RB-B 10	0 (disabled) or 10 - 10080 (minutes)	0 (disabled)	No

* Not applicable if only one Sub Band is available for the applicable Country Code
** Applicable only if DFS is supported by the Sub Band
*** Configurable only in units without an integral antenna.
**** Partial (only after the unit re-enters radar scanning, for example after a frequency change, sub-band change, etc.)

E.1.4 Network Management Parameters

Parameter	Unit	Range	Default	Run-Time
Access to Network Management	BU, RB	■ From Wireless Link Only ■ From Ethernet Only ■ From Both Ethernet and Wireless Link	From Both Ethernet and Wireless Link	No

Parameter	Unit	Range	Default	Run-Time
Network Management Filtering	BU, RB	■ Disable ■ Activate Management IP Filter On Ethernet Port ■ Activate Management IP Filter On Wireless Port ■ Activate Management IP Filter On Both Ethernet and Wireless Ports	Disable	No
Set Network Management IP Address	BU, RB	IP address	0.0.0.0 (all 10 entries)	No
Set/Change Network Management IP Address Ranges	BU, RB	<start address> to <end address> or, <base address> mask <mask>	0.0.0.0 TO 0.0.0.0 (all 10 entries)	No
Send SNMP Traps	BU	■ Disable ■ Enable	Disable	Yes
SNPM Traps IP Destination	BU	IP address	0.0.0.0 (all 10 entries)	No
SNMP Traps Community	BU	Up to 14 printable ASCII characters	public (all 10 entries)	No
Wi2 IP Address	RB	IP address	0.0.0.0 (none)	Yes

E.1.5 Bridge Parameters

Parameter	Unit	Range	Default	Run-Time
VLAN ID Data	RB	1 - 4094	1	No
VLAN ID - Management	BU, RB	1 - 4094, 65535	65535 (no VLAN)	No
VLAN Link Type	BU, RB	■ Hybrid Link ■ Trunk Link ■ Access Link (only in RB)	Hybrid Link	No
VLAN Forwarding Support	BU, RB	Disable, Enable	Disable	No

Parameter	Unit	Range	Default	Run-Time
VLAN Forwarding ID	BU, RB	1 - 4094 (up to 20 entries)	Empty list	No
VLAN Priority - Data	RB	0 - 7	0	No
VLAN Priority - Management	BU, RB	0 - 7	0	No
Bridge Aging Time	BU, RB	20 - 2000 seconds	300	No
Ethernet Broadcast Filtering Options	RB	■ Disable, ■ On Ethernet Port Only ■ On Wireless Port Only ■ On Both Wireless and Ethernet Ports	Disable	Yes
DHCP Broadcast Override Filter	RB	■ Disable ■ Enable	Disable	Yes
PPPoE Broadcast Override Filter	RB	■ Disable ■ Enable	Disable	Yes
ARP Broadcast Override Filter	RB	■ Disable ■ Enable	Enable	Yes
Ethernet Broadcast/Multicast Limiter Option	BU, RB	■ Disable ■ Limit only Broadcast Packets ■ Limit Multicast Packets that are not Broadcasts ■ Limit All Multicast Packets (including broadcast)	Disable	Yes
Ethernet Broadcast/Multicast Limiter Threshold	BU, RB	0 - 204800 (packets/second)	50	Yes
Ethernet Broadcast/Multicast Limiter Send Trap Interval	BU, RB	1 - 60 (minutes)	5 (minutes)	Yes
Roaming Option`	RB	■ Disable ■ Enable	Disable	No

Parameter	Unit	Range	Default	Run-Time
Ethernet Port Control	RB	■ Disable ■ Enable	Enable	Yes
Send Broadcasts/Multicasts as Unicasts	BU	■ Disable ■ Enable	Enable	Yes

E.1.6 Performance Parameters

Parameter	Unit	Range	Default	Run-Time
RTS Threshold	BU, RB	20 - 4092 (bytes)	■ 2200 for BU/RB B14, BU/RB B28 ■ 4092 for BU/RB-B10, BU/RB B100	Yes
Minimum Contention Window	BU, RB	0, 7, 15, 31, 63, 127, 255, 511, 1023	15	No
Maximum Contention Window	BU, RB	7, 15, 31, 63, 127, 255, 511, 1023	1023	No
Maximum Modulation Level	BU, RB	According to the Min/Max Modulation Level defined for the Sub Band	The highest available value	Yes
Multicast Modulation Level	BU	According to the Min/Max Modulation Level defined for the Sub Band	The lowest available value	Yes
Number of HW Retries	BU, RB	1 - 14	10	Yes
Control Modulation Level	BU, RB	■ Basic Rate ■ Modulation Level 1	Basic Rate	Yes
Average SNR Memory Factor	BU, RB	-1 to 32	5	Yes
Burst Mode Option*	BU, RB	■ Disable ■ Enable	Enable (If Burst Mode is supported by the Sub Band)	No

Parameter	Unit	Range	Default	Run-Time
Burst Mode Time Interval*	BU, RB	1 to the value defined in the Sub Band for Maximum Burst Duration (milliseconds)	5 milliseconds or the value of Maximum Burst Duration defined for the Sub Band (the lower of the two values).	Yes
Adaptive Modulation Algorithm	BU, RB	■ Adaptive Modulation ■ Statistics-Based Rate Control	Adaptive Modulation	No
Adaptive Modulation Option	BU, RB	■ Disable ■ Enable	Enable	No
Minimum Interval Between Adaptive Modulation Messages	BU, RB	1-3600 (seconds)	4 (seconds)	Yes
Adaptive Modulation Decision Thresholds	BU, RB	■ Normal ■ High	Normal	No
Packet Threshold To Test Up Rate	BU, RB	10-10000	100	No
Packet No On Upper Rate	BU, RB	1-3	1	No
Retries on Lower Modulations	BU, RB	■ Disable ■ Enable	Disable	No
RTS Duration Mode	BU, RB	■ Short RTS Duration ■ Long RTS Duration	Short RTS Duration	No
Concatenation Option	BU, RB	■ Disable ■ Enable	Enable	No
Maximum Concatenated Frame Size	BU, RB	■ 256 to 2200 bytes for BU/RB-B14 and BU/RB B28 ■ 256 to 4032 bytes for BU/RB-B10, BU/RB-B100	■ 2200 for BU/RB B14, BU/RB B28 ■ 4032 for BU/RB-B10, BU/RB B100	Yes

* Applicable only if Burst Mode is supported by the Sub Band.

E.1.7 Service Parameters

Parameter	Unit	Range	Default	Run-Time
User Filtering Option	RB	■ Disable ■ IP Protocol Only ■ User Defined Addresses Only ■ PPPoE Protocol Only	Disable	Yes
Set/Change Filter IP Address Ranges	RB	<start address> to <end address> or, <base address> mask <mask>	0.0.0.0 TO 0.0.0.0 (all 8 entries)	No
DHCP Unicast Override Filter	RB	■ Disable DHCP Unicast ■ Enable DHCP Unicast	Disable DHCP Unicast	Yes
MIR: Downlink	RB	RB-B10: 128 - 4992 (Kbps) RB-B14: 128 - 6912 (Kbps) RB-B28: 128 - 22016 (Kbps) RB-B100: 128 - 107904 (Kbps)	RB-B10: 4992 RB-B14: 6912 RB-B28: 22016 RB-B100:107904	Yes
MIR: Uplink	RB	RB-B10: 128 - 4992 (Kbps) RB-B14: 128 - 6912 (Kbps) RB-B28: 128 - 22016 (Kbps) RB-B100: 128 - 107904 (Kbps)	RB-B10: 4992 RB-B14: 6912 RB-B28: 22016 RB-B100: 107904	Yes
Maximum Burst Duration	RB	0 - 2,000 (ms)	5 (ms)	No
VLAN Priority Threshold	BU, RB	0 - 7	7	No
ToS Prioritization Option	BU, RB	■ Disable ■ Enable IP Precedence (RFC791) Prioritization ■ Enable DSCP (RFC2474) Prioritization	Disable	No
IP Precedence Threshold	BU, RB	0 - 7	4	No
DSCP Threshold	BU, RB	0 - 63	32	No

Parameter	Unit	Range	Default	Run-Time
UDP/TCP Port Ranges Prioritization Option	BU, RB	■ Disable ■ Enable Only for UDP ■ Enable Only for TCP ■ Enable for both UDP and TCP	Disable	No
UDP RTP/RTCP Prioritization	BU, RB	■ RTP & RTCP ■ RTP Only	RTP & RTCP	No
TCP RTP/RTCP Prioritization	BU, RB	■ RTP & RTCP ■ RTP Only	RTP & RTCP	No
IP Range Prioritization Option	BU, RB	■ Disable ■ Source IP Prioritization ■ Destination IP Prioritization ■ Source or Destination IP Prioritization	Disable	No
IP Range Address	BU, RB	4 groups of up to 3 digits separated by dots	0.0.0.0	No
IP Range Mask	BU, RB	4 groups of up to 3 digits separated by dots	255.0.0.0	No
Low Priority Traffic Minimum Percent	RB	0 - 100 (%)	0	Yes
Wireless Link Prioritization Option*	BU-B14/ 28/100	■ Disable ■ Enable	Disable	Yes
Low Priority AIFS*	BU-B14/ 28/100	3-50	3	Yes
Number of HW Retries for High Priority Traffic*	BU-B14/ 28/100	1-14	10	Yes
Number of HW Retries for Low Priority Traffic*	BU-B14/ 28/100	1-14	10	Yes
BU Burst Duration for High Priority Traffic*	BU-B14/ 28/100	0-40 (in 0.25 milliseconds units)	16 (4 milliseconds)	Yes
BU Burst Duration for Low Priority Traffic*	BU-B14/ 28/100	0-40 (in 0.25 milliseconds units)	20 (5 milliseconds)	Yes

Parameter	Unit	Range	Default	Run-Time
RB Burst Duration for High Priority Traffic*	BU-B14/ 28/100	0-40 (in 0.25 milliseconds units)	8 (2 milliseconds)	Yes
RB Burst Duration for Low Priority Traffic*	BU-B14/ 28/100	0-40 (in 0.25 milliseconds units)	20 (5 milliseconds)	Yes

E.1.8 Security Parameters

Parameter	Unit	Range	Default	Run-Time
Authentication Algorithm*	BU, RB	■ Open system ■ Shared Key	Open system	No
Data Encryption Option*	BU, RB	■ Disable ■ Enable	Disable	No
Security Mode*	BU, RB	■ WEP ■ AES/OCB ■ FIPS-197	WEP	No
Default Key	RB	1-4	1	No
Default Multicast Key	BU	1-4	1	No
Key # 1 to Key # 4	BU, RB	32 hexadecimal digits	0…0 (all 0=no key)	No
Promiscuous Authentication	BU	■ Disable ■ Enable	Disable	Yes (Disable after reset)

* Applicable only if supported by the Sub Band.