alvarion®
Your Open WiMAX Choice

BreezeACCESS® SU-L

Product Manual

Software Version 3.1
December 2009
P/N 215461

Document History

Topic	Description	Date Issued
This is the document's first Release		October 2007
Main Menu Section 4.1.1	Added descriptions for new menu items	SW Version 5.5 October 2008
Wireless Settings Section 4.3	Added descriptions for new menu items: Security Mode, MIR uplink, MIR downlink, CIR uplink, CIR downlink, CIR delay, Burst duration, Min Contention Window, Max Contention Window, AIFS, Hardware retries, Preferred AU MAC Address, VLAN Support Mode (Link Type), VLAN Tag For Data Frames, Priority Tagging For Data Frames	SW Version 5.5 October 2008
get ClientSta Section 5.6.14	Updated section with new parameters: security-mode, MirDownlink, MirUplink, CirDownlink, CirUplink, CirDelay, BurstDuration, MinContentionWiodow, MaxContentionWindow, AIFS, HardwareRetries, PreferredAuMacAddress, EthernetLinkType, VlanDataID, VlanDataPriority	SW Version 5.5 October 2008
set ClientSta security-mode Section 5.9.2	New	SW Version 5.5 October 2008
set ClientSta HardwareRetries Section 5.9.13	New	SW Version 5.5 October 2008
set ClientSta PreferredAuMacAddress Section 5.9.14	New	SW Version 5.5 October 2008
VLAN Commands Section 5.10	New	SW Version 5.5 October 2008
Contention Commands Section 5.11	New	SW Version 5.5 October 2008
MIR/CIR Commands Section 5.10	New	SW Version 5.5 October 2008
Glossary	Added definitions for: AES-CCM, AIFS, CIR, MIR	SW Version 5.5 October 2008
Maximum Throughput Table 1-2	Updated Maximum Throughput from 2 Mbps upload / 3 Mbps download to 12 Mbps for both upload and download	SW Version 2.1 April 2009
Operating Channels Table 1-2	Added operating channels for Japan	SW Version 2.1 April 2009

Topic	Description	Date Issued
DFS parameters Section 4.3	New	SW Version 2.1 April 2009
Radar Status Section 4.7	New	SW Version 2.1 April 2009
Feature Upgrads Section 4.10	New	SW Version 2.1 April 2009
DFS Commands Section 5.14	New	SW Version 2.1 April 2009
Burst Time Sections 4.3, 5.7.14, 5.12	New	SW Version 3.0 October 2009
Traffic Prioritization Sections 4.3, 5.15	New	SW Version 3.0 October 2009
LED Operation Mode Sections 4.3, 5.4	New	SW Version 3.0 October 2009
CRC monitoring Section 4.5	New	SW Version 3.0 October 2009
Set Factory Defaults Utility Appendix B	New	SW Version 3.0 October 2009

Legal Rights

© Copyright 2009 Alvarion Ltd. All rights reserved.

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

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

Trade Names

Alvarion®, BreezeCOM®, WALKair®, WALKnet®, BreezeNET®, BreezeACCESS®, BreezeLINK®, BreezeMAX®, BreezeLITE®, BreezePHONE®, 4MOTION®, BreezeCONFIG™, AlvariSTAR™, AlvariCRAFT™, MGW™, eMGW™ and/or other products and/or services referenced here in are either registered trademarks, trademarks or service marks of Alvarion Ltd.

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

Statement of Conditions

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

Warranties and Disclaimers

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

Exclusive Warranty

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

(b) With respect to the Firmware, Alvarion warrants the correct functionality according to the attached documentation, for a period of fourteen (14) month from

invoice date (the "Warranty Period")". During the Warranty Period, Alvarion may release to its Customers firmware updates, which include additional performance improvements and/or bug fixes, upon availability (the "Warranty"). Bug fixes, temporary patches and/or workarounds may be supplied as Firmware updates.

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

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

Disclaimer

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

(b) PURCHASER'S SOLE REMEDY FOR BREACH OF THE EXPRESS WARRANTIES ABOVE SHALL BE REPLACEMENT OR REFUND OF THE PURCHASE PRICE AS SPECIFIED ABOVE, AT ALVARION'S OPTION. TO THE FULLEST EXTENT ALLOWED BY LAW, THE WARRANTIES AND REMEDIES SET FORTH IN THIS AGREEMENT ARE EXCLUSIVE AND IN LIEU OF ALL OTHER

WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING BUT NOT LIMITED TO WARRANTIES, TERMS OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, NON-INFRINGEMENT, AND ACCURACY OF INFORMATION GENERATED. ALL OF WHICH ARE EXPRESSLY DISCLAIMED. ALVARION' WARRANTIES HEREIN RUN ONLY TO PURCHASER, AND ARE NOT EXTENDED TO ANY THIRD PARTIES. ALVARION NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS.

Limitation of Liability

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

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

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.

Radio Frequency Interference Statement

The SU-L Access Unit 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 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, the antenna used for this equipment must be fixed-mounted on outdoor permanent structures with a separation distance of at least 20 centimeters (8 inches) from al persons.

R&TTE Compliance Statement

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

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. The unit must be connected to an earthed (grounded) outlet to comply with international safety standards.

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, Alvarion is not liable for any injury, damage or regulation violations associated with or caused by installation, grounding or lightning protection.

Disposal of Electronic and Electrical Waste



Disposal of Electronic and Electrical Waste

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

《电子信息产品污染控制管理办法》
(第39号)
(又名中国RoHS)

产品内含危害物质揭露表						
零部件名称	危害物质项目					
	铅	**镉**	**汞**	**六价铬**	PBB	PBDE
	(Pb)	(Cd)	(Hg)	(Cr^{6+})	(多溴联苯)	(多溴二苯乙醚)
含铜线材	×	○	○	○	○	○
连接器	×	○	○	○	○	○
变压器	×	○	○	○	○	○
陶瓷电容	×	○	○	○	○	○
高温锡材	×	○	○	○	○	○

○：表示此部件使用的所有同类材料中此种有毒或有害物质的含量均低于 SJ/T11363-2006 规定的限制要求。
×：表示此部件使用的至少一种同类材料中，此种有毒或有害物质的含量高于 SJ/T11363-2006 规定的限制要求。

The above table provides information required under the following Chinese legislation:
Management methods for Controlling Pollution by Electronic Information Products(No.39)
(also known as China RoHS)

Important Notice

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

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

Some of the equipment provided by Alvarion and specified in this manual, is manufactured and warranted by third parties. All such equipment must be installed and handled in full compliance with the instructions provided by such manufacturers as attached to this manual or provided thereafter by Alvarion or

the manufacturers. Non-compliance with such instructions may result in serious damage and/or bodily harm and/or void the user's authority to operate the equipment and/or revoke the warranty provided by such manufacturer.

About This Manual

This manual describes the SU-L Subscriber Unit and details how to install, operate and manage it.

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

This manual contains the following chapters and appendices:

- **Chapter 1 - Product Description** - Describes the SU-L unit and its functionality.
- **Chapter 2 - Installation** - Describes how to install the SU-L and how to connect to subscriber's equipment.
- **Chapter 3 - Initial Configuration** - Describes how to initially configure the SU-L in order to test basic link operation.
- **Chapter 4 - Web-managed Configuration**- Describes advanced configuration of the SU-L using a web browser.
- **Chapter 5 - Command Line Interface** - Describes advanced configuration of the SU-L using Telnet.
- **Appendix A - Troubleshooting**

Table of Contents

Chapter 1 - Product Description 1

1.1 Introducing BreezeACCESS 3

1.2 The SU-L 4

1.3 Specifications 5

1.3.1 Radio 5
1.3.2 Sensitivity 7
1.3.3 Transmit Power 7
1.3.4 Configuration and Management 8
1.3.5 Mechanical 8
1.3.6 Electrical 8
1.3.7 Environmental 9
1.3.8 Standards Compliance 9

Chapter 2 - Hardware Installation 10

2.1 Installation Requirements 12

2.1.1 Packing List 12
2.1.2 Additional Equipment and Tools Required for Installation 13

2.2 Installation Steps 14

2.3 ODU Hardware Description 15

2.3.1 Integrated High-Gain Antenna 15
2.3.2 Ethernet Port 15
2.3.3 Ethernet Port Cover (Service Box) 15
2.3.4 Grounding Point 16
2.3.5 Water Tight Test Point 16
2.3.6 Pole-Mounting Bracket Attachment Points 16
2.3.7 LED Indicators 16

2.4 Mounting the SU-L ODU 18

2.5 Connecting Cables to the Outdoor Unit 23

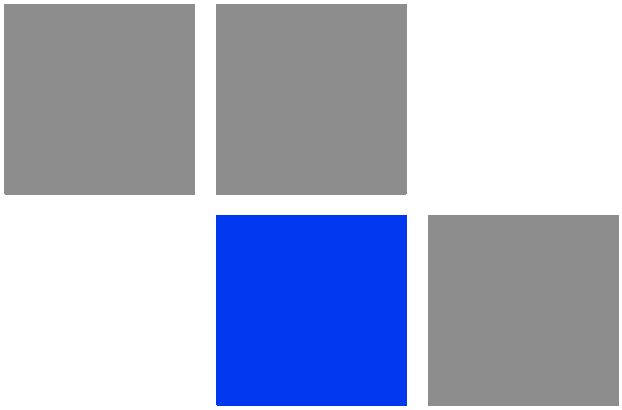
2.5.1 IDU-ODU Cables 23

2.5.2 Preparing and Connecting the IDU-ODU Cable 24
2.5.3 Grounding Wire 25
2.6 The Power Injector IDU 27
2.7 Connecting the Power Injector IDU Cables 28
2.8 Align the Antenna 30
Chapter 3 - Initial Configuration 32
3.1 Introduction 34
3.2 Setting the Regulatory Domain 35
3.3 Configuring Basic Parameters 37
3.3.1 Accessing the Web Management Interface 37
3.3.2 Basic Parameters 38
Chapter 4 - Web-managed Configuration 40
4.1 Introduction 42
4.1.1 Main Menu 42
4.2 Management Settings 47
4.3 Wireless Settings 49
4.4 Saving Settings 61
4.5 Status Information 62
4.6 Site Survey 64
4.7 Radar Status 64
4.8 Managing the SU-L Configuration 66
4.9 Upgrading SU-L Firmware 68
4.10 Feature Upgrade 69
Chapter 5 - Command Line Interface 72
5.1 Using the Command Line Interface 74
5.1.1 Accessing the CLI 74
5.1.2 Telnet Connection 74
5.2 Entering Commands 76

5.2.1 Minimum Abbreviation 76
5.2.2 Command Completion 76
5.2.3 Getting Help on Commands 77
5.2.4 Partial Keyword Lookup 78
5.2.5 Command Line Processing 78
5.3 General Commands 79
5.3.1 exit 79
5.3.2 ping 79
5.3.3 reboot 81
5.4 LED Operation Mode Commands 82
5.4.1 set ClientSta ledMode 82
5.4.2 set ClientSta led1Type ~ led7Type 82
5.4.3 set ClientSta led1Mode ~ led7Mode 83
5.4.4 set ClientSta led1Target ~ led7Target 84
5.5 Regulatory Domain Commands 85
5.5.1 regdomain 85
5.5.2 addfreq 86
5.5.3 dynamicfreq 87
5.5.4 delfreq 88
5.5.5 getfreq 88
5.6 Password Commands 90
5.6.1 set system password 90
5.6.2 passwd 91
5.7 File Commands 92
5.7.1 save-running 93
5.7.2 set config default 93
5.7.3 set ClientSta status-update 93
5.7.4 set tftpftp ftppass 94
5.7.5 set tftpftp ftpuser 94
5.7.6 set tftpftp ptype 95
5.7.7 set tftpftp rfile 95
5.7.8 set tftpftp sip 95
5.7.9 set tftpftp start 96
5.7.10 get tftpftp 96
5.7.11 get config 97

5.7.12 get interface 98
5.7.13 get system 98
5.7.14 get ClientSta 100
5.8 SNMP Commands 105
5.8.1 set ClientSta snmp-rocommunity 105
5.9 Ethernet Interface Commands 106
5.9.1 set ClientSta bridge-mip 106
5.9.2 set ClientSta bridge-static-ip 106
5.9.3 set ClientSta default-gw 107
5.9.4 set ClientSta dhcpc 107
5.10 Wireless Commands 109
5.10.1 set ClientSta authentication 110
5.10.2 set ClientSta security-mode 110
5.10.3 set ClientSta data-encryption-option 111
5.10.4 set ClientSta default-key 111
5.10.5 set ClientSta distance 112
5.10.6 set ClientSta key 112
5.10.7 set ClientSta linkrate 113
5.10.8 set ClientSta mangVLAN 113
5.10.9 set ClientSta modulation 114
5.10.10set ClientSta rtsthreshold 114
5.10.11set ClientSta txpowerlevel 115
5.10.12set ClientSta wireless-essid 116
5.10.13set ClientSta HardwareRetries 116
5.10.14set ClientSta PreferredAuMacAddress 116
5.10.15set ClientSta bandwidth 117
5.10.16get BSSList 117
5.10.17set CStatus clear-cnt yes 118
5.10.18get CStatus 118
5.11 VLAN Commands 121
5.11.1 set ClientSta EthernetLinkType 121
5.11.2 set ClientSta VlanDataID 121
5.11.3 set ClientSta VlanDataPriority 122
5.12 Contention Commands 123
5.12.1 set ClientSta AIFS 123

5.12.2 set ClientSta burstTime 123
5.12.3 set ClientSta MinContentionWindow 124
5.12.4 set ClientSta MaxContentionWindow 124
5.13 MIR/CIR Commands 126
5.13.1 set ClientSta MirDownlink 126
5.13.2 set ClientSta MirUplink 126
5.13.3 set ClientSta CirDownlink 127
5.13.4 set ClientSta CirUplink 127
5.13.5 set ClientSta BurstDuration 128
5.14 DFS Commands 129
5.14.1 set ClientSta dfsOption 129
5.14.2 set ClientSta dfsChannelCheckTime 130
5.14.3 set ClientSta dfsChannelAvoidancePeriod 130
5.14.4 set ClientSta dfsClearRadarDetectedChannels 130
5.14.5 set ClientSta dfsMinimumPulseToDetect 131
5.14.6 set ClientSta dfsDetectionAlgorithm 131
5.15 Traffic Prioritization Commands 133
5.15.1 set ClientSta VlanPriorityThreshold 133
5.15.2 set ClientSta ToSPrioritizationOption 134
5.15.3 set ClientSta IPToSPrecedenceThreshold 134
5.15.4 set ClientSta DSCPThreshold 135
5.15.5 set ClientSta UdpTcpPortRangesPrioOpt 135
5.15.6 set ClientSta UdpPortPriRtpRtcp 136
5.15.7 set ClientSta TcpPortPriRtpRtcp 136
5.15.8 set ClientSta UdpPortRanges 137
5.15.9 set ClientSta TcpPortRanges 137
5.15.10set ClientSta IpRangeOption 138
5.15.11set ClientSta IpRangeIpAddress 138
5.15.12set ClientSta IpRangeMask 138
Appendix A - Troubleshooting 140
Appendix B - Using the Set Factory Defaults Utility 143
Glossary 146



Chapter 1

Product Description

In This Chapter:

- "Introducing BreezeACCESS" on page 3
- "The SU-L" on page 4
- "Specifications" on page 5

1.1 Introducing BreezeACCESS

BreezeACCESS VL is a high capacity, IP services oriented Broadband Wireless Access system. The system employs wireless packet switched data technology to support high-speed IP services including fast Internet and Virtual Private Networks. BreezeACCESS VL users are provided with a network connection that is always on, supporting immediate access to the Internet and other IP services at high data rates. The system is designed for cellular-like deployment, enabling the system architecture to vary in size and structure. A system can include any number of cells, each containing several Access Units for better coverage of densely populated areas.

With a range of up to 12 Km and lower equipment and deployment costs, BreezeACCESS enables service providers to wirelessly extend their services to customers who were previously unable to afford them, while securing rapid ROI. Remote residential areas can now benefit from high-speed Internet access, Web browsing and e-mail, and advanced applications such as multi-media services.

An out-of-the-box solution with immediate available local stock, BreezeACCESS enables virtually instant network expansion and simplified deployment. BreezeACCESS presents a step forward in overcoming the digital divide by providing an affordable solution that offers vast opportunities for enhanced communication, education, business, social development and improved quality of life.

BreezeACCESS products operate in unlicensed frequency bands 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, the system enables operation in near-line-of-sight environments. These qualities enable service providers to reach a previously inaccessible and broader segment of the subscriber population.

The Access Units are currently available in several 5 GHz frequency bands. 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.

The SU-L CPEs supports all frequencies from 4.900 to 5.875 GHz with automatic band and frequency detection, enabling fast and simple plug-and-play installation.

1.2 The SU-L

The Outdoor SU-L is a wireless client CPE that provides a connection to a remote AU Access Unit. When connected to an AU-VL, the SU-L operates using the proprietary VL wireless link protocol, enabling to benefit from some of the unique features and capabilities provided by the VL solution.

The SU-L Subscriber Unit includes the following components:

- Indoor Unit (IDU)
- Outdoor Unit (ODU)

The IDU connects to the network through a standard IEEE 802.3 Ethernet 10/100BaseT (RJ 45) interfaces and is powered from the 110/220 VAC mains. The IDU is connected to the ODU via a Category 5 Ethernet cable. This cable carries Ethernet traffic between the indoor and the outdoor units, and also transfers power (54 VDC) from the indoor unit to the outdoor unit.

The ODU outdoor unit contains the processing and radio modules and includes an integrated high-gain antenna. The ODU is housed in a weatherproof enclosure for mounting outdoors and includes its own bracket for attaching to a pole, radio mast, or tower structure.

The SU-L CPEs supports all frequencies from 4.900 to 5.875 GHz with automatic frequency detection, enabling fast and simple plug-and-play installation.

1.3 Specifications

The SU-L can be managed through an easy-to-use web interface, CLI, or SNMP. SU-L subscriber units provide a more affordable alternative to SU-A/E CPEs, while delivering similar functionalities.

Table 1-1: SU-L Subscriber Unit Types

SU Type	MIR Uplink (Mbps)	MIR Downlink (Mbps)	CIR Uplink (Mbps)	CIR Downlink (Mbps)
SU-3-L	2	3	2	3
SU-6-L	4	6	4	6
SU-12-L	12	12	10	10

1.3.1 Radio

Table 1-2: Radio Specifications

Item	Description
Radio Protocol	CSMA-CA (IEEE 802.11a based)
Frequency Band	4900-5865 MHz multi-band with automatic frequency detection
Operating Channels	■ FCC: 5.260, 5.280, 5.300, 5.320, 5.500, 5.520, 5.540, 5.560, 5.580, 5.600, 5.620, 5.640, 5.660, 5.680, 5.700, 5.745, 5.765, 5.785, 5.805, 5.825 GHz ■ UK: 5.740, 5.750, 5.760, 5.770, 5.780, 5.830, 5.840 GHz ■ ETSI: 5.500, 5.520, 5.540, 5.560, 5.580, 5.600, 5.620, 5.640, 5.660, 5.680, 5.700 GHz ■ Japan: 4.920, 4.940, 4.960, 4.980 GHz ■ Universal: 4.900 ~ 5.865 GHz in 5 MHz steps
Operation Mode	Time Division Duplex (TDD)
Channel Bandwidth	20 MHz and 10 MHz
Data Rates	Normal Mode: 6, 9, 12, 18, 24, 36, 48, 54 Mbps per channel
Maximum Throughput	12 Mbps upload, 12 Mbps download
Radio Technology	Orthogonal Frequency Division Multiplexing (OFDM)

Table 1-2: Radio Specifications

Item	Description
Modulation Technique	Binary Phase Shift Keying (BPSK) @ 6 and 9 Mbps Quadrature Phase Shift Keying (QPSK) @ 12 and 18 Mbps 16-Quadrature Amplitude Modulation (QAM) @ 24 & 36 Mbps 64-QAM @ 48 & 54 Mbps
FEC Coding Rates	1/2 2/3, 3/4
Max Tx Power Levels at Antenna Port	18 dBm*
TPC (Transmit Power Control)	100%, 50%, 25%, 12.5%, Min (0 dBm).
Antenna	Integrated Flat Panel Antenna, 17dBi, 24°AZ x 18°EL.

*The maximum value can be lower depending on the radio band and modulation used. Check Table 1-4 for details

1.3.2 Sensitivity

Table 1-3: Sensitivity

Data Rate	Sensitivity (dBm)			
Modulation/Rate	**5.150-5.250 GHz**	**5.250-5.350 GHz**	**5.500-5.700 GHz**	**5.725-5.875 GHz**
BPSK (6 Mbps)	-89	-89	-89	-89
BPSK (9 Mbps)	-88	-88	-88	-88
QPSK (12 Mbps)	-86	-86	-86	-87
QPSK (18 Mbps)	-84	-84	-84	-84
16 QAM (24 Mbps)	-81	-81	-81	-80
16 QAM (36 Mbps)	-77	-77	-77	-77
64 QAM (48 Mbps)	-73	-73	-73	-71
64QAM (54 Mbps)	-71	-71	-70	-67

1.3.3 Transmit Power

Table 1-4: Transmit Power

	Maximum Output Power (dBm)			
Data Rate	**5.150-5.250 GHz**	**5.250-5.350 GHz**	**5.500-5.700 GHz**	**5.725-5.875 GHz**
6 Mbps	18	18	18	18
9 Mbps	18	18	18	17
12 Mbps	18	18	18	17
8 Mbps	18	18	18	17
24 Mbps	18	18	18	17
36 Mbps	18	18	18	17
48 Mbps	17.5	17	17	16.5
54 Mbps	17.5	17	16.5	15

1.3.4 Configuration and Management

Table 1-5: Configuration and Management

Item	Description
Management options	■ Web-based (HTTP/HTTPS) ■ Telnet, SSH (CLI) ■ SNMP
SNMP agent	V1, supports 802.11 MIB, RFC-1213 MIB II and private MIB.
Management access	From Wired LAN, Wireless Link
Management access protection	Access Password
Encryption	WEP 152-bits
Allocation of IP parameters	Configurable or automatic (DHCP client)
Software upgrade	HTTPS/FTP/TFTP
Configuration Upload/Download	HTTPS

1.3.5 Mechanical

Table 1-6: Mechanical Specifications

Item	Description
Dimensions	195mm (W) X 190mm (H) X 74mm (D)
Weight	1.47Kg
Mounting Bracket Rotation	+/- 360º

1.3.6 Electrical

Table 1-7: Ethernet Pin-Out Assignments

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

Table 1-8: Electrical Specifications

Type	Details
AC Power Supply	100-240VAC, 50-60Hz, maximum power consumption 1.5A, meet LPS request
ODU Power supply	55 VDC from the IDU over the indoor-outdoor Ethernet cable

1.3.7 Environmental

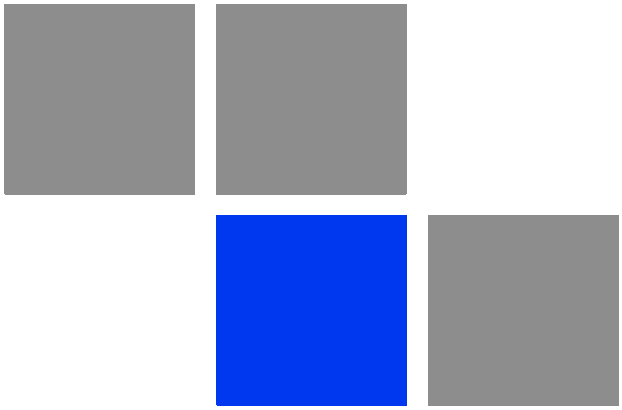
Table 1-9: Environmental Specifications

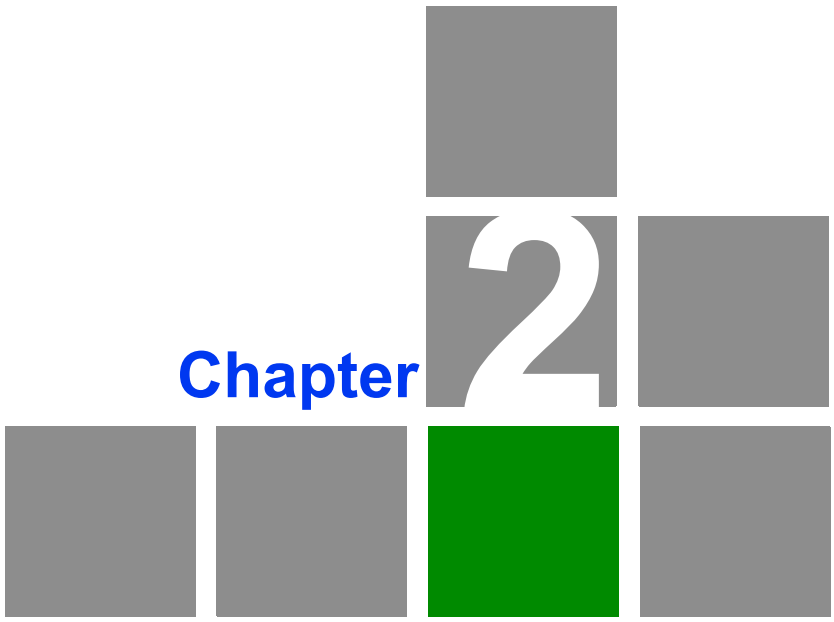
Item	Details
Operating Temperature	Outdoor Unit: -40ºC to 55ºC Indoor Unit: 5ºC to 50ºC
Humidity	Maximum 95%, non-condensing.
Water Proof (ODU)	IP-67

1.3.8 Standards Compliance

Table 1-10: Standards Compliance

Type	Standard
EMC	■ EN55022 CE Class B ■ FCC Class B Part 15 ■ VCCI Class B
Safety	■ UL / CUL (CSA60950-1, UL60950-1) ■ CE / CB (EN60950-1/IEC 60950-1)
Lightning	The unit withstand at +4KV of Input surge, 1.2usec rise/fall time, 50µsec duration, every 10 seconds, for all interfaces.
Radio	■ ETSI 301 893 (11a) ■ ETSI 301 489 (DC power) ■ FCC Part 15 (11a) ■ RSS210 (Canada)





Chapter 2

Hardware Installation

In This Chapter:

- "Installation Requirements" on page 12
- "Installation Steps" on page 14
- "ODU Hardware Description" on page 15
- "Mounting the SU-L ODU" on page 18
- "Connecting Cables to the Outdoor Unit" on page 23
- "The Power Injector IDU" on page 27
- "Connecting the Power Injector IDU Cables" on page 28
- "Align the Antenna" on page 30

2.1 Installation Requirements

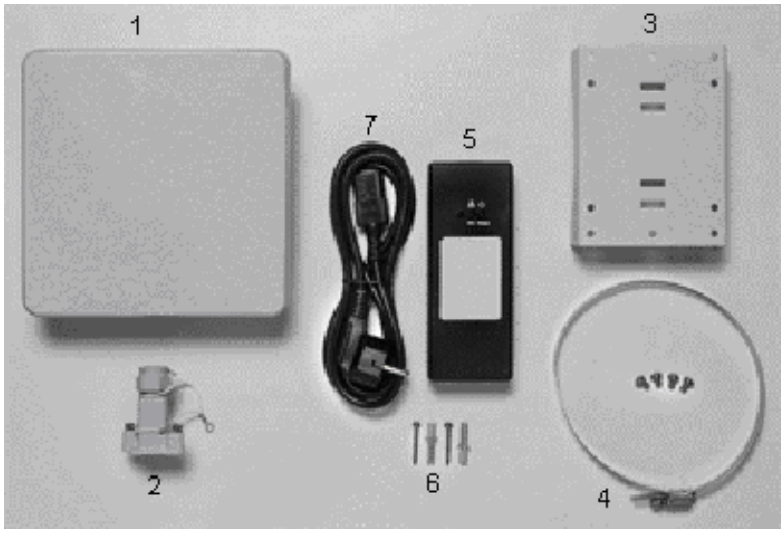
2.1.1 Packing List

The SU-L package includes the following components:

- SU-L CPE Outdoor Unit with integrated antenna (1)
- A Service Box (Sealing Assembly for the ODU's Ethernet connector) (2)
- A pole mounting kit for the SU-L, including a mounting plate (3) and a metal band and four screws (4)
- IDU Indoor Unit (5) with two screws and two anchors (6) for wall-mounting the IDU
- Mains power cord (7)

In addition:

- Two sets of stickers (with the ODU). Each set includes two stickers, one with the ODU's MAC address and one with the S/N details.
- Quick Installation Guide.



2.1.2 Additional Equipment and Tools Required for Installation

- Ethernet cable for connecting to the user's data equipment (straight-through for connecting to a switch/hub/router, or cross-over for connecting to a PC).
- Indoor-to-outdoor Category 5E Ethernet cable. Use only Category 5E cables approved by the supplier. The length of the Indoor-to-Outdoor cable should not exceed 90 meters. The length of the Indoor-to-Outdoor cable, together with the length of the Ethernet cable connecting the IDU to the data equipment, should not exceed 100 meters.
- Two shielded RJ-45 connectors, and a suitable crimping tool.
- Grounding cable with appropriate terminations.
- Mains plug adapter or termination plug (if the power plug on the supplied AC power cord does not fit local power outlets).
- Portable PC/Notebook for configuring parameters using either Telnet (CLI) or a web browser.
- Installation tools and materials, including appropriate means (e.g. a pole) for installing the outdoor unit.

2.2 Installation Steps



CAUTION

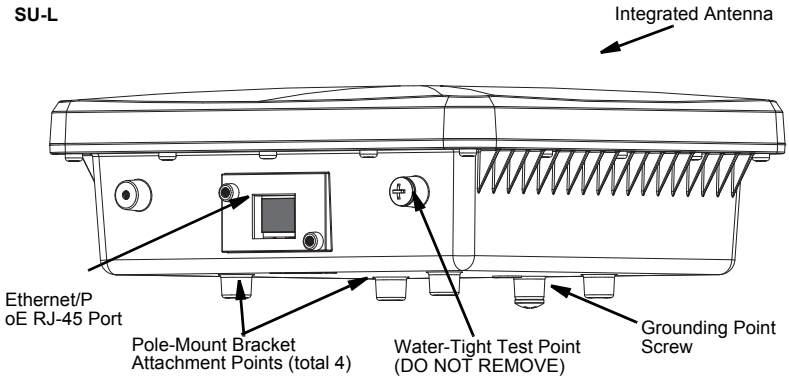
ONLY experienced installation professionals who are familiar with local building and safety codes and, wherever applicable, are licensed by the appropriate government regulatory authorities should install outdoor units and antennas.

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

Hardware installation of the SU-L involves these steps:

1. Mount the outdoor unit on a pole, mast, or tower using the mounting bracket.
2. Connect the Ethernet cable and a grounding wire to the unit.
3. Connect the power injector IDU to the Ethernet cable, user's data equipment, and an AC power source.
4. Align the antenna for optimal performance.

2.3 ODU Hardware Description



2.3.1 Integrated High-Gain Antenna

The SU-L ODU includes an integrated high-gain (17 dBi) flat-panel antenna for 5 GHz operation.

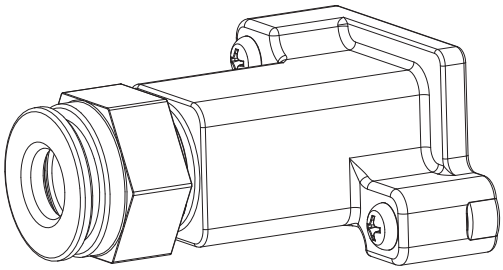
2.3.2 Ethernet Port

The SU-L ODU has one 10BASE-T/100BASE-TX RJ-45 port that connects to the power injector IDU using an Ethernet cable. The Ethernet port connection provides power to the SU-L as well as a data link to the local network via the IDU.

The unit appears as an Ethernet node and performs a bridging function by moving packets from the wired LAN to the remote Access Unit (from here on in referred to as AU.)

2.3.3 Ethernet Port Cover (Service Box)

The SU-L's RJ-45 Ethernet port requires the use of a weatherproof cover to seal the unit.



2.3.4 Grounding Point

Even though the SU-L includes its own built-in lightning protection, it is important that the unit is properly connected to ground. A grounding screw is provided for attaching a ground wire to the unit.

2.3.5 Water Tight Test Point

CAUTION

Do no remove or loosen this screw. Doing so could lead to damage of the unit.

2.3.6 Pole-Mounting Bracket Attachment Points

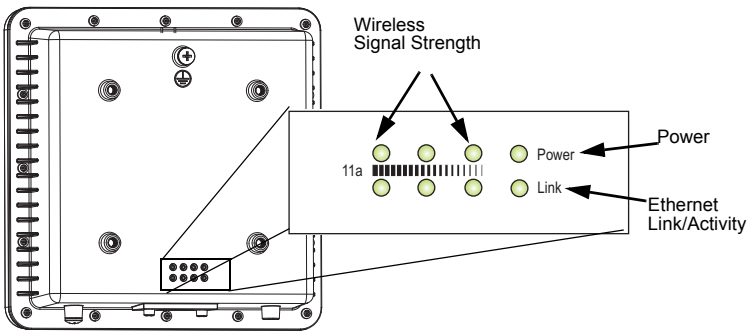
The SU-L includes a bracket kit that can be used to mount the unit to a pole, radio mast, or part of a tower structure.

2.3.7 LED Indicators

NOTE

The behavior described below for the LEDs is called Normal Mode and is enabled by default. However, the LEDs' behavior can be customized by the user (see "LED Operation Mode Commands" on page 82). For details on how the LEDs behave in Threshold mode, read the above mentioned section.

The SU-L includes status LED indicators located on the base of the unit, as indicated in the following figure.



The following table describes the system status LEDs:.

LED	Status	Description
Power	On Green	Indicates that the system is working normally.
	On Amber	Indicates a system reset.

LED	Status	Description
Link	On Green	Indicates a valid 10/100 Mbps Ethernet cable link.
	Flashing Green	Indicates that the SU-L is transmitting or receiving data on a 10/100 Mbps Ethernet LAN. Flashing rate is proportional to network activity.

The three pairs of the 11a LEDs display the received signal strength and can be used for aligning antennas in the wireless link.

The following table describes the wireless status LEDs:

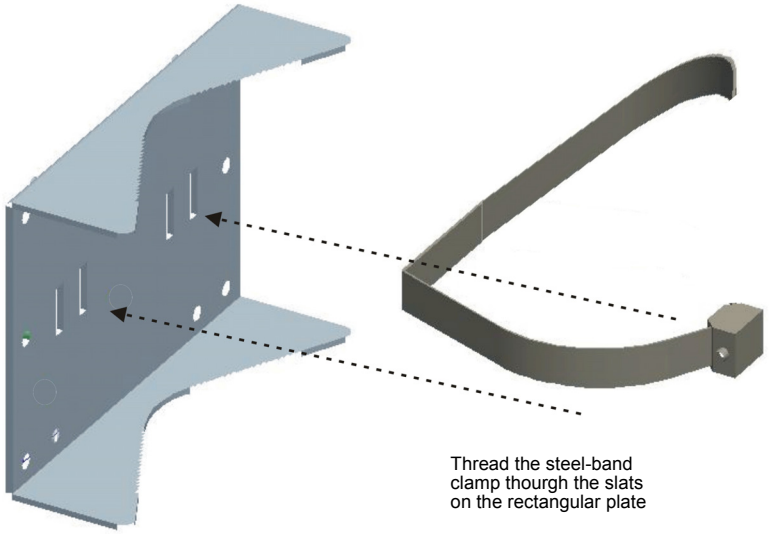
11a LEDs Status			Description
Right Pair	Center Pair	Left Pair	
Off	Off	Off	The radio is disabled or unit is still booting up
Blinking-slowly	Off	Off	No signal detected or RSSI is below -88 dBm
Blinking-fast	Off	Off	RSSI is between -88 dBm and -87 dBm
Blinking-very fast	Off	Off	RSSI is between -86 dBm and -85 dBm
On	Off	Off	RSSI is between -84 dBm and -82 dBm
On	Blinking-slowly	Off	RSSI is between -81 dBm and -80 dBm
On	Blinking-fast	Off	RSSI is between -79 dBm and -78 dBm
On	Blinking-very fast	Off	RSSI is between -77 dBm and -76dBm
On	On	Off	RSSI is between -75 dBm and -74 dBm
On	On	Blinking-slowly	RSSI is between -73 dBm and -72 dBm
On	On	Blinking-fast	RSSI is between -71 dBm and -70 dBm
On	On	Blinking-very fast	RSSI is between -69 dBm and -68 dBm
On	On	On	RSSI is over -67dBm

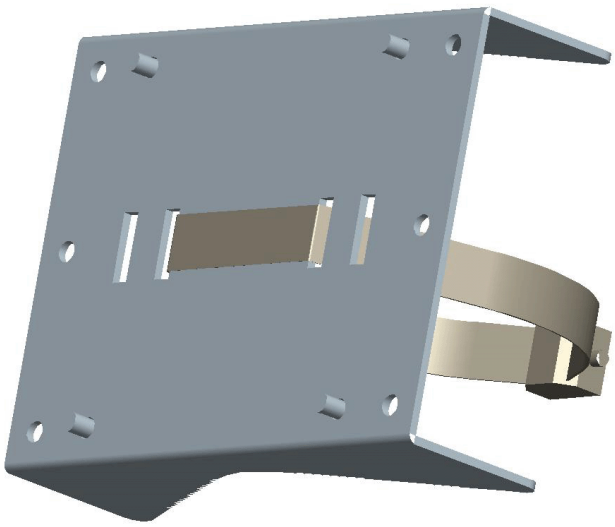
2.4 Mounting the SU-L ODU

The SU-L's pole-mounting bracket has two parts: One rectangular plate with V-shaped edges that attaches directly to the SU-L ODU, and one steel-band clamp that secures the unit to a pole. The rectangular plate connects to the unit using four screws. The steel-band clamp threads through the rectangular plate and around the pole to which it fastens.

Perform the following steps to mount the unit to a 1.5 to 2 inch diameter steel pole or tube using the mounting bracket:

1 Thread the provided steel-band through the rectangular plate.

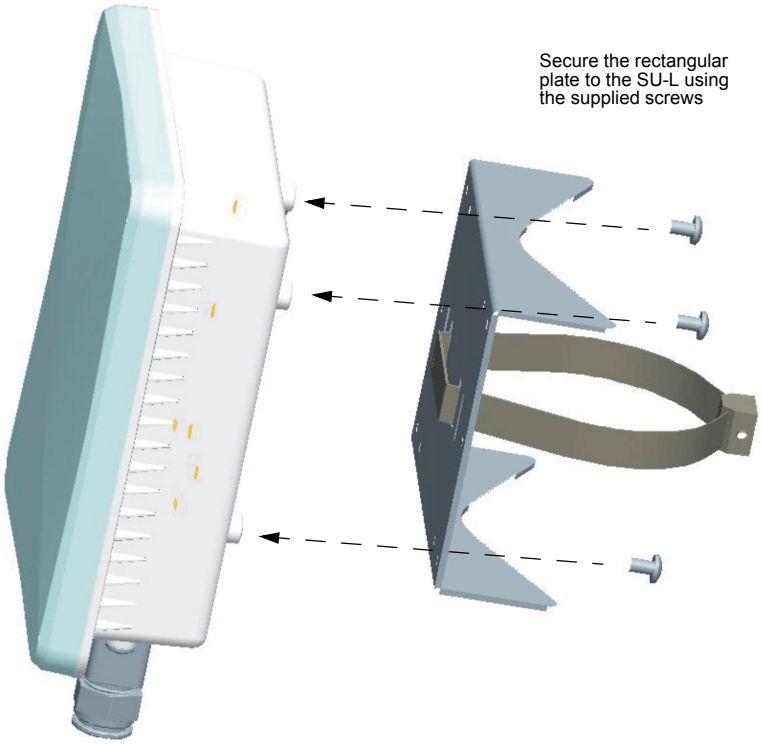




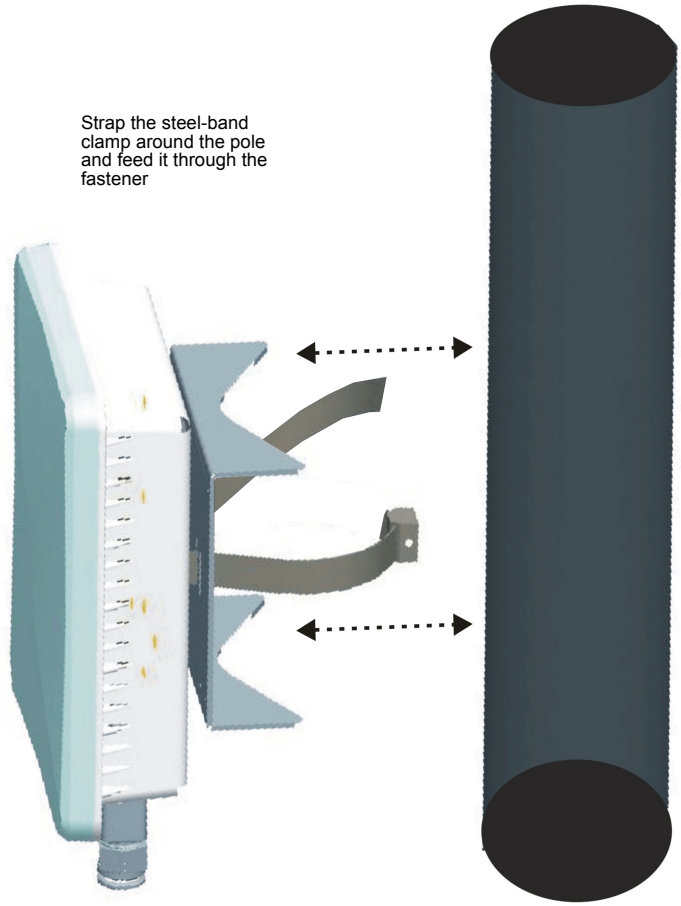
2 Attach the rectangular mounting plate to the SU-L using the supplied four screws.

NOTE

The mounting plate can be attached to the unit in a way that allows it to be mounted vertically or at a 45 degree angle.

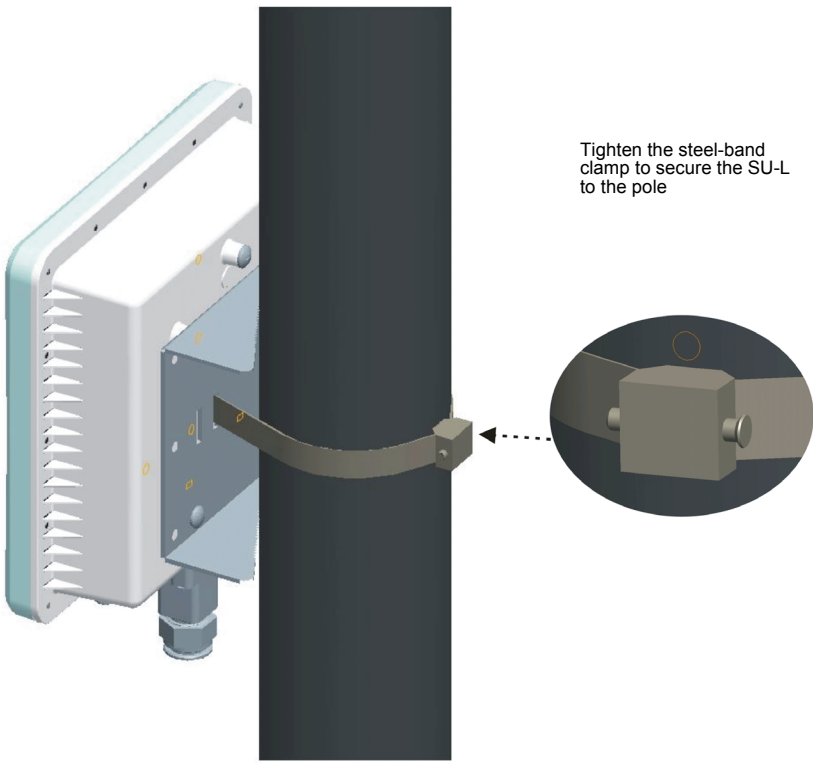


3 Place the SU-L with its attached rectangular plate on one side of the pole and strap the steel-band clamp around the pole. Feed the steel band through its fastener and secure it tightly.



NOTE

Be sure to take account of the antenna polarization direction; antennas in a link must be mounted with the same polarization.


Tighten the steel-band
clamp to secure the SU-L
to the pole

2.5 Connecting Cables to the Outdoor Unit

WARNING

Do not connect or disconnect cables or otherwise work with the SU-L during periods of lightning activity.

2.5.1 IDU-ODU Cables

NOTE

The length of the Indoor-to-Outdoor cable should not exceed 90 meters. The length of the Indoor-to-Outdoor cable, together with the length of the Ethernet cable connecting the IDU to the data equipment, should not exceed 100 meters.

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

Table 2-1: Approved Category 5E Ethernet Cables

Manufacturer	Part Number
Synergy Cables Ltd. www.sinergy-cables.com	612098
HES Cabling Systems www.hescs.com	H5E-00481
Teldor www.teldor.com	8393204101
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
GU-Tech., LLC . - A Member of OVIS GroupTel/Fax : 732 918 8221 Mobile: 718 909 4093 www.OVIS.COM.TW www.GU-TECH.COM	

In case of missing information in the manufacturer's WEB site (product specifications, ordering issues, etc.), it is highly recommended to contact the manufacturer's sales representative directly.

2.5.2 Preparing and Connecting the IDU-ODU Cable

1. Unscrew the top nut from the Service Box.
2. Route a straight-through Cat. 5 Ethernet cable (8-wire, 24 AWG) through both the top nut and the body of the Service Box.
3. Insert and crimp the RJ-45 connector. Refer to the cable preparations instructions described below.
4. Connect the Ethernet cable to the ODU RJ-45 connector.
5. Attach the Service Box to the ODU and tighten the top nut. Make sure that the external jack of the cable is well inside the Service Box to guarantee good sealing.
6. Route the cable to the location selected for the indoor equipment. It is recommended to attach a lightning arrestor to the cable immediately before it enters the building.
7. Assemble an RJ-45 connector on the indoor end of the ODU cable. Refer to the pin assignment and color codes in standard cables described below.

IDU-ODU Cable Preparation:

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

- Remove as small a length as possible of the external jacket. Verify that the external jacket is well inside the sealing cover when connected to the unit, to ensure good sealing.
- Pull 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.

The IDU-ODU cable provides pin-to-pin connection on both ends.

The following figure shows the required wire pair connections.

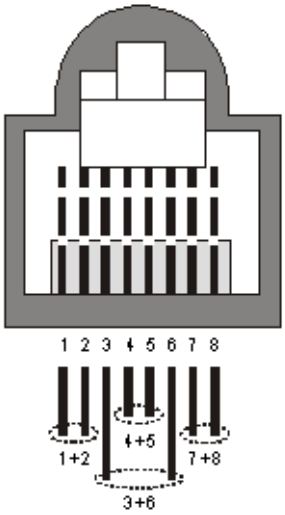


Figure 2-1: Ethernet Connector Pin Assignments

The color codes used in standard cables supplied by Alvarion are as listed in the following table:

Table 2-2: Cable Color Codes

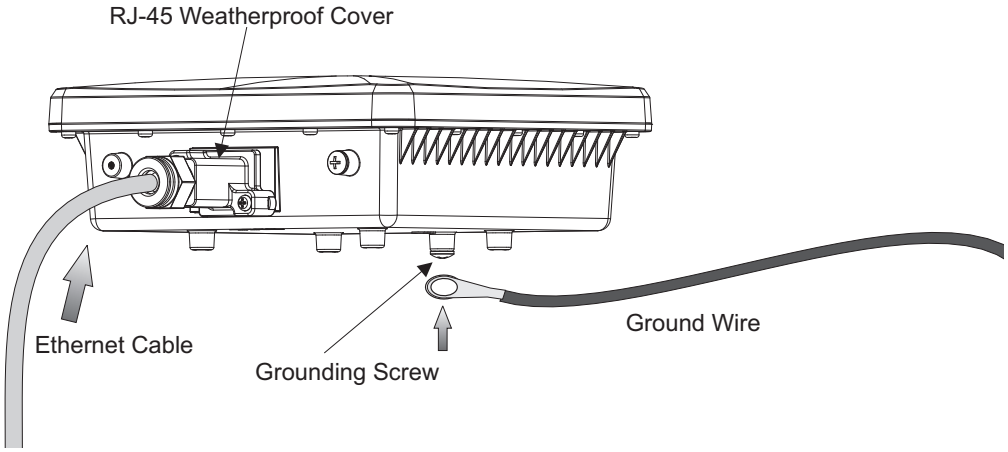
Wire color	Pin
Blue	1
Blue/white	2
Orange	3
Orange/white	6
Brown	4
Brown/white	5
Green	7
Green/white	8

2.5.3 Grounding Wire

Be sure to ground the Outdoor Unit with an appropriate grounding wire (not included) by connecting the grounding point on the base of the unit to a good ground (earth) connection.

CAUTION

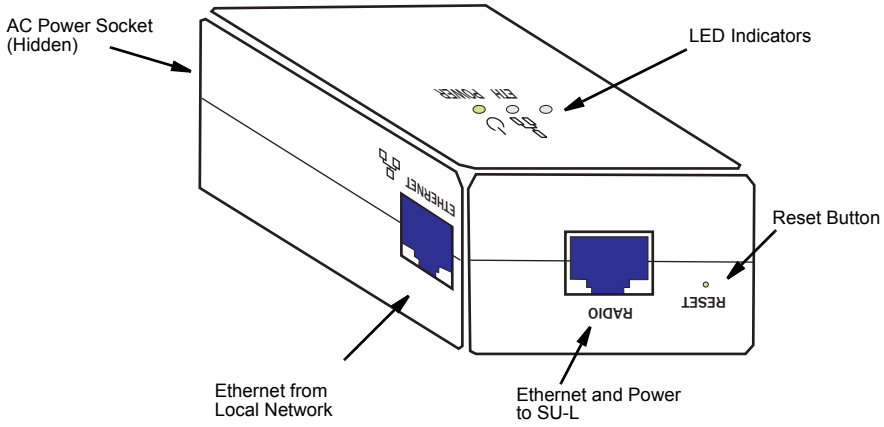
Be sure that grounding is available and that it meets local and national electrical codes. For additional lightning protection, use lightning rods, lightning arrestors, or surge suppressors.



2.6 The Power Injector IDU

The SU-L receives power through its network cable connection using power-over-Ethernet technology. A power injector IDU is included in the SU-L package and provides two RJ-45 Ethernet ports, one for connecting to the SU-L (Radio), and the other for connecting to a local LAN switch (Ethernet).

The Ethernet port uses an MDI (i.e., internal straight-through) pin configuration. You can therefore use straight-through twisted-pair cable to connect this port to most network interconnection devices such as a switch or router that provide MDI-X ports. However, when connecting the SU-L to a workstation or other device that does not have MDI-X ports, you must use a crossover twisted-pair cable.



The SU-L does not have a power switch. It is powered on when its Ethernet port is connected to the power injector module, and the power injector module is connected to an AC power source.

The Power LED indicates whether AC power is applied. The Link LED does not function in current release of SU-L.

In the current release, the Reset button does not function.

The power injector module automatically adjusts to any AC voltage between 100-240 volts at 50 or 60 Hz. No voltage range settings are required.

WARNING

The power injector module is designed for indoor use only. Never mount the power injector outside with the SU-L unit.

2.7 Connecting the Power Injector IDU Cables

The unit can be placed on a desktop or a shelf. Alternatively, it may be wall-mounted using the kit supplied with the unit.

CAUTION

Do not install the power injector outdoors. The unit is for indoor installation only.

CAUTION

Install lightning protection at the power injector end of the Ethernet cable, use a lightning arrestor immediately before the cable enters the building.

NOTE

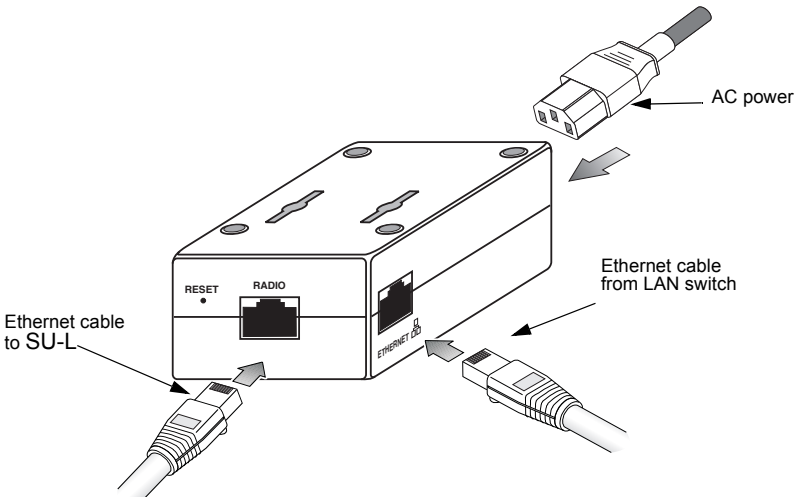
The SU-L's Ethernet port does not support Power over Ethernet (PoE) based on the IEEE 802.3af standard. Do not try to power the unit by connecting it directly to a network switch that provides IEEE 802.3af PoE. Always connect the unit to the included power injector module.

To connect the IDU cables:

1. Connect the Ethernet cable from the SU-L ODU to the RJ-45 port labeled "Radio" on the power injector IDU.
2. Connect a straight-through unshielded twisted-pair (UTP) cable from a local LAN switch/router to the RJ-45 port labeled "Ethernet" on the power injector. If you connect to a workstation, use a crossover cable. Use Category 5E or better UTP cable for 10/100BASE-TX connections.

NOTE

The RJ-45 port on the power injector is an MDI port. If connecting directly to a computer, use a crossover cable



3 Insert the power cable plug directly into the standard AC receptacle on the power injector.

4 Plug the other end of the power cable into a grounded, 3-pin socket, AC power source.

NOTE

For International use, you may need to change the AC line cord. You must use a line cord set that has been approved for the receptacle type in your country.

5 Check the Power LED on top of the power injector IDU to be sure that power is being supplied to it.

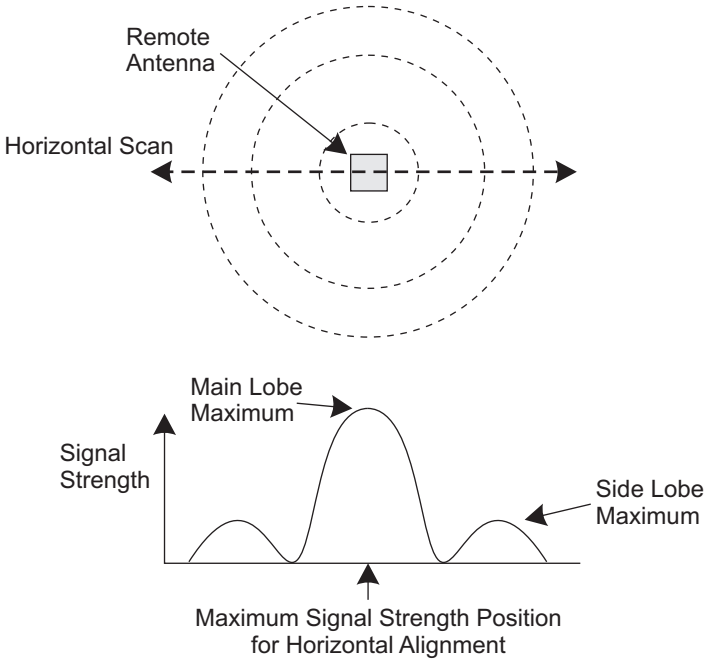
2.8 Align the Antenna

After the SU-L unit has been mounted, connected, and its radio is operating, the antenna must be accurately aligned to ensure optimum performance on the wireless link. This alignment process is particularly important for long-range links.

To start the alignment process, you can just point the antenna in the general direction of the Access Unit's antenna using binoculars or a compass. For accurate alignment, you must monitor the signal strength LEDs as the antenna moves horizontally.

The signal strength LEDs indicate the downlink radio signal strength for the link. The more LEDs that turn on, the stronger the signal.

When you move the antenna during alignment, the radio signal from the remote antenna can be seen to have a strong central main lobe and smaller side lobes. The object of the alignment process is to set the antenna so that it is receiving the strongest signal from the central main lobe.



To align the antennas in the link, monitor the signal strength LEDs. For details see "LED Indicators" on page 16. Perform the following procedure:

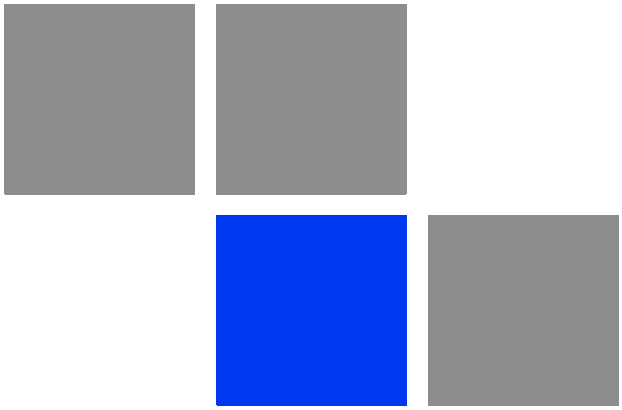
1 Pan the SU-L antenna horizontally back and forth while checking the LEDs by rotating the pole-mounting bracket around the pole.

2 Find the point where the signal is strongest (refer to "LED Indicators" on page 16) and secure the bracket in that position.



NOTE

Sometimes there may not be a central lobe peak because vertical alignment is too far off; only two similar peaks for the side lobes are detected.



Chapter 3

Initial Configuration

In This Chapter:

- "Introduction" on page 34
- "Setting the Regulatory Domain" on page 35
- "Configuring Basic Parameters" on page 37

3.1 Introduction

The SU-L offers a user-friendly web-based management interface for the configuration of all the unit's features. Any PC directly attached to the unit can access the management interface using a web browser, such as Internet Explorer (version 6.0 or above).

The initial configuration steps can be made through the web-browser interface using the default IP address. You can make the initial changes by connecting a PC directly to the Ethernet port of SU-L's power injector IDU before mounting the unit outdoors in its operating location.

3.2 Setting the Regulatory Domain

Before operating the SU-L it is important to set the regulatory domain in which the unit is to operate. Not doing so can result in breaching local laws. The unit must be installed by a qualified professional.

The SU-L has a default IP address of 10.0.0.1 and a subnet mask of 255.0.0.0. If your PC has an IP address (static or assigned by a DHCP server) on the same subnet then you can connect immediately to the command line interface using Telnet. Otherwise, you must first change your PC's IP address to be on the same subnet as the SU-L.

To set the regulatory domain you must log into Installer mode from the command prompt. Specify "installer" as the operating mode and the default password is also "installer". For more information on using Telnet and the command prompt see "Command Line Interface."

Example.

```
ClientSta login: installer
Password:*********
Installer#
```

Then type "regdomain" followed by the RETURN key. The unit then displays all possible domain settings. The options are:

- **FCC -** Federal Communications Commission.
- **ETSI -** European Telecommunications Standards Institute.
- **UK -** United Kingdom.
- **JAPAN -** Japan. Not applicable for current release.
- **Universal -** This selects all frequencies in the 802.11a radio bands.
- **WLG -** Not applicable for current release.Access restricted.
- **Brazil -** Brazil
- **India -** India



WARNING

You must select the regulatory domain that is legally permissable for the country in which you intend to operate the SU-L.

This example shows how to display all possible regulatory domains by entering the syntax "regdomain" followed by the Enter (Return) key. The FCC domain is then selected by entering the syntax "regdomain FCC".

Example

```
Installer# regdomain
Usage :
        regdomain [FCC | ETSI | UK | JAPAN | Universal | WLG | Brazil | India]
Installer# regdomain FCC
Installer#
```

In order to apply the new selected regulatory domain you need to use the command "set ClientSta status-update yes" to apply them and "save-running" command to save all changes. The unit must be reset to fully apply the changes.

3.3 Configuring Basic Parameters

Several parameters must be configured to ensure that the unit can function properly and connect to the Access Unit. Additional parameters may be configured later, either locally or remotely over the wireless link.

3.3.1 Accessing the Web Management Interface

The SU-L has a default IP address of 10.0.0.1 and a subnet mask of 255.0.0.0. If your PC has an IP address (static or assigned by a DHCP server) on the same subnet then you can connect immediately to the web interface. Otherwise, you must first change your PC's IP address to be on the same subnet as the SU-L.

In the web browser's address bar, type the default IP address: http://10.0.0.1.

The web browser displays the SU-L's login window.



Figure 3-1: Login Window

Logging In – Type the default user name "admin" and password "private", then click OK.

NOTE

The Web Management Interface only supports the "admin" account.

The management interface displays.

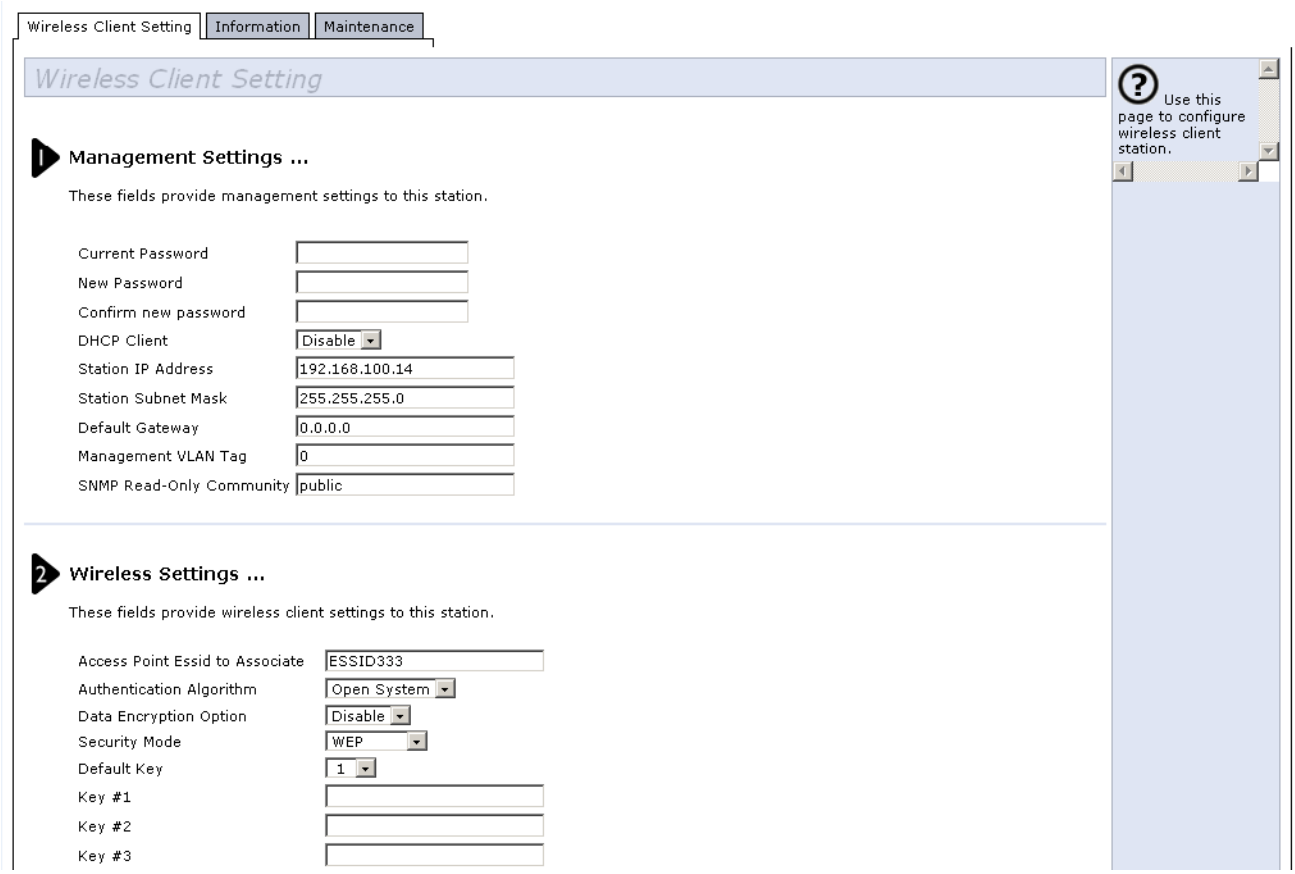


Figure 3-2: The SU-L Management Interface

3.3.2 Basic Parameters

There are only a few basic steps you need to set up the SU-L and provide a connection to your service provider's Access Unit.

Follow these steps:

1 **Set a New Password** – On the Wireless Client Setting page, enter a new password to replace the default "private".



NOTE

It is strongly recommended that you configure your own password. If a password is not configured, the management interface is not protected and anyone that can connect to the SU-L may be able to compromise your network security.

2 **Set the ESSID** (Extended Service Set Identifier) – Enter the ESSID, or wireless network name, of the network you want to connect to. All SU-Ls in the same network must use the same ESSID as the remote access point to associate.

The ESSID is case sensitive and can consist of up to 31 alphanumeric characters.

3 **Enter security Keys** – If the wireless network you are connecting to uses WEP or AES-CCM security, you need to enter the WEP key provided to you by the network operator. Enter "0x" followed by 32 hexadecimal digits (0 to 9 and A to F) for 152 bit keys. Note that Authentication Algorithm, Data encryption, Default key and all 4 keys (or at least the one selected as the default) must be configured with the same values as those configured in the AP in order to ensure proper operation.

4 **Change the SU-L IP Address** – If the SU-L's default IP address is not compatible with the network you want to connect to, enter an appropriate IP address and subnet mask as provided by the network operator.

Save Your Settings – Click the "Update" button to save all your changes.

Chapter 4

Web-managed Configuration

In This Chapter:

- "Introduction" on page 42
- "Management Settings" on page 47
- "Wireless Settings" on page 49
- "Saving Settings" on page 61
- "Status Information" on page 62
- "Site Survey" on page 64
- "Radar Status" on page 64
- "Managing the SU-L Configuration" on page 66
- "Upgrading SU-L Firmware" on page 68
- "Feature Upgrade" on page 69

4.1 Introduction

The SU-L's basic wireless client settings can be configured as described in the previous chapter, "Initial Configuration." This chapter describes all the unit's settings and features in more detail.

4.1.1 Main Menu

The System Configuration pages include the following options.

Menu	Description	Page
Wireless Client Setting		
Management Settings	Configures the access password, IP address, subnet mask, VLAN tag, and SNMP Read-Only Community setting	47
Current Password	Web interface password	47
New Password	Configures a new password	47
Confirm new password	Re-enter the above password for confirmation	47
DHCP Client	Enables / disables the DHCP client	47
Station IP Address	Configures an IP address for the SU	48
Station Subnet Mask	Configures a subnet mask for the SU	48
Default Gateway	Configures a gateway for routing traffic to the SU	48
Management VLAN Tag	Sets the tag for identifying the management VLAN	48
SNMP Read-Only Community	Sets the SNMP Read-only password	48
Wireless Settings	Configures the ESSID, WEP keys, and antenna transmit settings	49
Access Point ESSID to Associate	Configures the Service Set Identifier of the network you want to connect to	49
Authentication Algorithm	Specifies the authentication method	50
Data Encryption Option	Enables / disables data encryption	50
Security Mode	Switches between WEP and AES-CCM	50
Default Key	Configures the key number used for encryption	50
Keys	Configures the keys provided by the network you wish to associate with	50
RTS Threshold	Configures the packet size threshold for using RTS/CTS mechanism	50

Menu	Description	Page
Transmit Power Level	Configures the radio transmit power	51
Modulation Type and Link Rate	Specifies the modulation type and configures the maximum rate for sending data.	51
MIR uplink	Sets the Maximum Information Rate of the uplink from the SU to the AU	51
MIR downlink	Sets the Maximum Information Rate of the downlink from the AU to the SU	51
CIR uplink	Sets the Committed Information Rate of the uplink from the SU to the AU	51
CIR downlink	Sets the Committed Information Rate of the downlink from the AU to the SU	51
CIR delay	Sets the Maximum delay time introduced by the CIR\MIR buffering mechanism	52
Burst duration	Sets the maximum duration for the initial uninterrupted burst of data sent after a period of inactivity	52
Min Contention Window	Sets the initial (lowest) minimal value for the additional timeslots employed by the back-off algorithm	52
Max Contention Window	Sets the final (highest) maximal value for the additional timeslots employed by the back-off algorithm	53
AIFS	Defines the Arbitration Inter-Frame Spacing number of time slots	53
Burst Time (ms)	Defines the burst size	54
Hardware Retries	Sets the maximum number of times that an unacknowledged frame is retransmitted in each Hardware Retrial phase	54
Preferred AU MAC Address	Sets the preferred AU	54
RF Distance (Km)	Configures the maximum distance of the cell	54
VLAN Support Mode (Link Type)	Chooses between Access and Hybrid VLAN link types	55
VLAN Tag For Data Frames	Sets the VLAN ID tag	55
Priority Tagging For Data Frames	Sets the VLAN priority tag	55
VLAN Priority Threshold	Sets up a VLAN based threshold for allocating packets to either the High Priority or the Low Priority queue.	55
ToS Prioritization Option	Sets up the ToS based prioritization for the High/Low priority queues	55
IP ToS Precedence Threshold	Sets up the threshold for IP Precedence based ToS prioritization (RFC791)	56
DSCP Threshold	Sets up the threshold for DSCP based ToS prioritization (RFC2474)	56
UDP/TCP Port Ranges Prioritization	Defines prioritization in accordance with UDP and/or TCP destination port ranges.	56

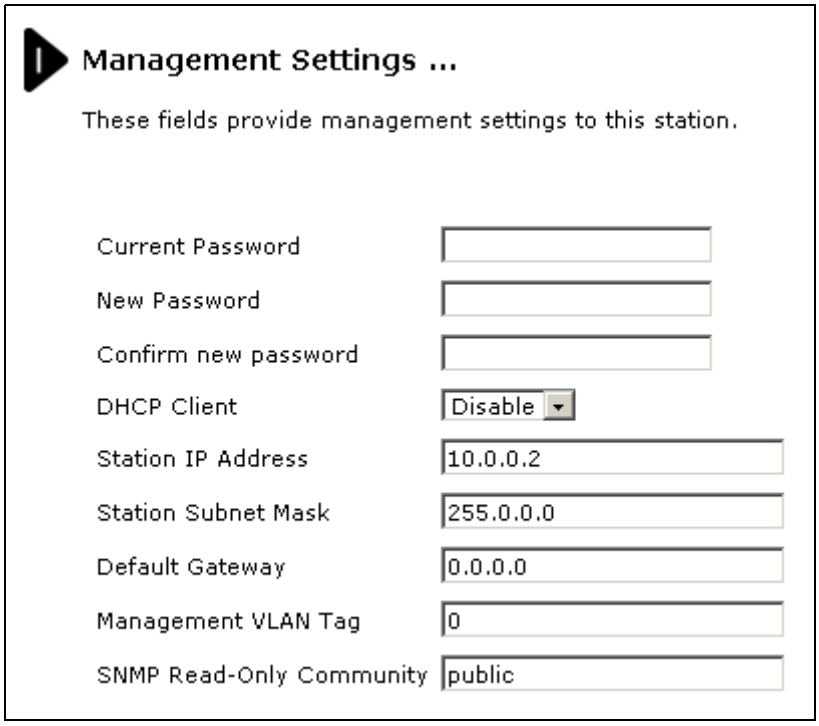
Menu	Description	Page
UDP Port RTP/RTCP Prioritization	Configures whether to prioritize only RTP packets or both RTP and RTCP packets when UDP port prioritization is enabled.	56
TCP Port RTP/RTCP Prioritization	Configures whether to prioritize only RTP packets or both RTP and RTCP packets when TCP port prioritization is enabled.	56
UDP Port Ranges	Defines UDP port ranges to be used as priority classifiers when UDP port range prioritization is enabled	57
TCP Port Ranges	Defines TCP port ranges to be used as priority classifiers when TCP port range prioritization is enabled	57
IP Range Option	Sets up traffic prioritization based on the frame's source/destination IP address	57
IP Range Start Address	Defines the start address for the high priority IP range	57
IP Range Mask	Defines the range mask for the high priority IP range	57
Regulatory Domain	Displays the regulatory domain	57
DFS Required by Regulations	Sets whether DFS is required by local regulations	58
Channel Check Time (seconds)	Sets the duration of the channel radar check	58
Channel Avoidance Period (minutes)	Sets the duration for the persistency of the Radar Detected or Adjacent to Radar tagging applied when radar is detected on a particular channel or adjacent channel respectively	58
Clear Radar Detected Channels	Sets all frequencies to Radar Free after clicking Update	58
Minimum Pulses to Detect	Minimum number of pulses that validate a signal as a radar signal	59
DFS Detection Algorithm	Selects between ETSI and FCC detection algorithms	59
Bandwidth (MHz)	Selects the operating channels' bandwidth	59
LED Operation Mode	Configures the LEDs' behavior	59
Information		
Status Information	Displays wireless client configuration settings for the system	62
Access Point ESSID to Associate	Displays the Service Set Identifier of the network to which you are connected	62
Access Point MAC Address	Displays the MAC address of the AU to which the SU is connected	62
Channel	Displays the radio channel the SU is transmitting through	62
Frequency	Displays the frequency at which the SU is transmitting	63

Menu	Description	Page
Link Quality	Displays the quality of the link between the SU and the AU	63
RSSI	Displays the Receive Signal Strength Indicator	63
Noise Floor	Displays the ambient noise floor	63
Transmit Power Level	Displays the overall power level of the SU in a range of minimum to maximum	63
MIR/CIR uplink/downlink	Displays MIR and CIR transfer rates for both uplink and downlink traffic	63
Rx/Tx Packets/Bytes (Wireless)	Displays traffic statistics for the wireless port	63
Rx/Tx Packets/Bytes (Ethernet)	Displays traffic statistics for the Ethernet port	63
CRC Counter (Wireless)	Displays the number of frames sent over the air that contained CRC errors	63
CRC Percentage (Wireless)	Displays the percentage of frames sent over the air that contained CRC errors	63
Site survey	Displays wireless site survey information	64
Radar Status	Displays the radar detection status for each channel	64
Maintenance		
Configuration	Saves the unit's configuration to a file; restores the configuration from a previously saved file; resets configuration settings to factory defaults; and resets the unit	66
Restore Factory Default	Restores factory default and reboots the SU	66
Save Current Configuration	Saves the current configuration to a backup file; you have the option to save the file in either encrypted or non-encrypted format through the check box	67
Restore Configuration	Restores a previously saved configuration (in either encrypted or non-encrypted format) to the SU	67
Reboot Client Station	Reboots the SU	67
Upgrade	Upgrades software from a local file	68
Model	Displays the SU's model name	68
Platform	Displays the hardware platform number	69
MAC Address	Displays the MAC address of the SU	69
Boot Code Version	Displays the current version of the boot code	69
Firmware Version	Displays the current version of the firmware	69
Upgrade via HTTP	Allows the user to upgrade firmware by HTTP	69

Menu	Description	Page
Upgrade via TFTP/FTP	Allows the user to upgrade firmware by TFTP/FTP	69
Feature Upgrade	Upgrades a particular feature for the unit	69
Model	Displays the SU's model name	70
Licence Number	Displays the unit's current licence number	70
Upgrade via HTTP	Allows the user to upgrade the feature by HTTP	70
Upgrade via TFTP/FTP	Allows the user to upgrade the feature by TFTP/FTP	70

4.2 Management Settings

The SU-L's basic client settings are described in this section.



Current Password – The password used to access the admin account via the web interface. The default name is "private" (Length: 1-32 characters, case sensitive).

Management access to the web interface on the SU-L is controlled through a single user name and password. To protect access to the management interface, you need to configure an Administrator password as soon as possible. If the password is not configured, then anyone having access to the SU-L may be able to compromise the SU-L and network security.

New Password – The new admin password for management access. (Length: 1-32 characters, case sensitive)

Confirm New Password – Enter the password again for verification.

DHCP Client – With DHCP Client enabled, the IP address, subnet mask and default gateway can be dynamically assigned to the SU-L by the network DHCP server. (Default: Disabled). If no DHCP server is found when the unit boots up or the lease of DHCP assignation expires, then the unit will use the configured IP address, subnet mask and default gateway until it can find a proper DHCP server and obtain a valid IP; DHCP server search operation will not stop until the feature is disabled.

Station IP Address – The IP address of the SU-L. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. If the SU-L's default IP address is not compatible with the network you want to connect to, enter an appropriate IP address and subnet mask as provided by the network operator.

Configuring the SU-L with an IP address expands your ability to manage the SU-L. A number of SU-L features depend on IP addressing to operate.

Station Subnet Mask – The mask that identifies the host IP address bits used for routing to specific subnets.

NOTE



You can use the web browser interface to access IP addressing only if the SU-L already has an IP address that is reachable through your network.

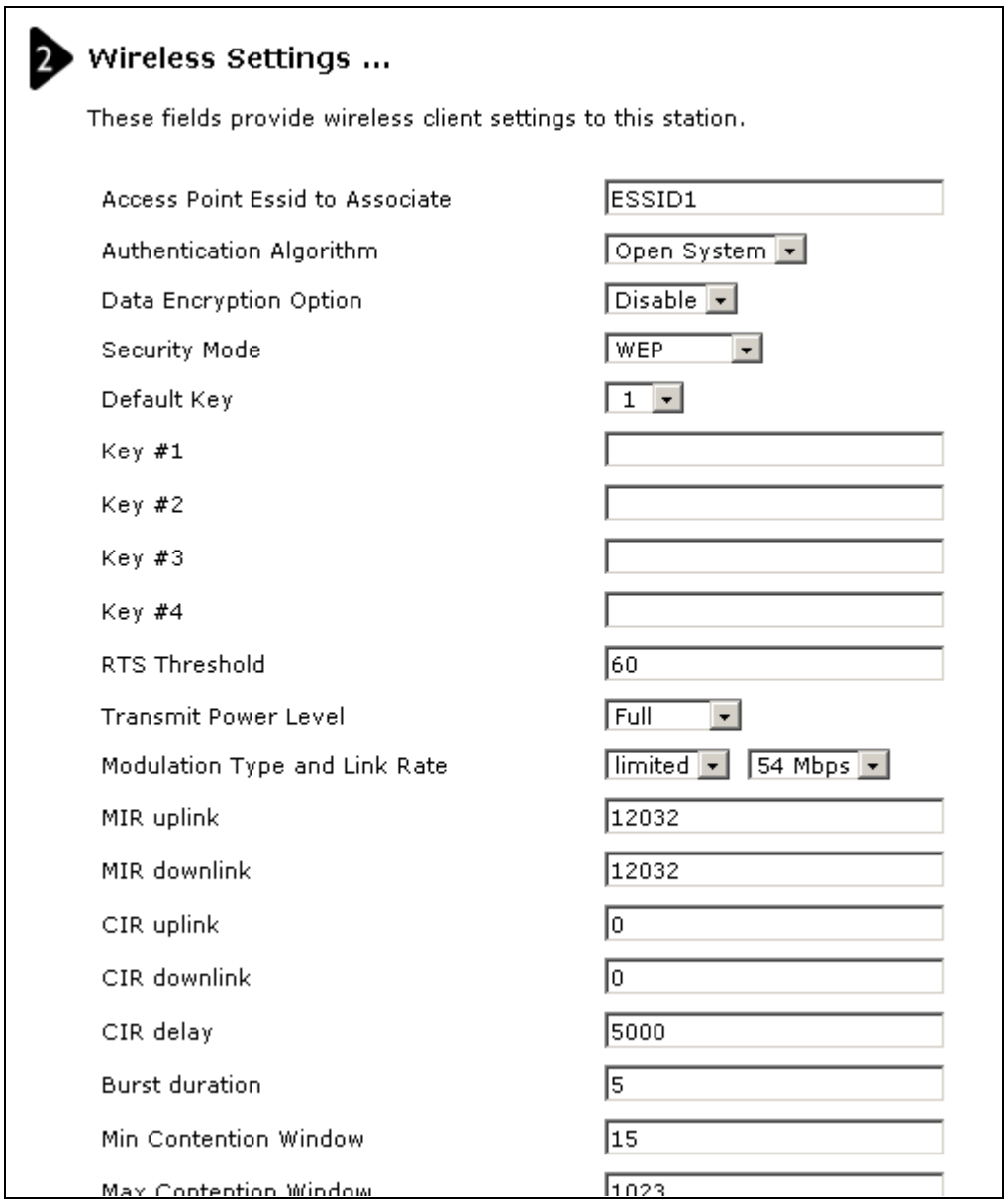
Default Gateway – If a management station exists on another network segment, then you must enter the IP address for a gateway that can route traffic between these segments.

Management VLAN Tag – Sets the tag of the management VLAN. (Default: 0, meaning no VLAN tag)

SNMP Read-Only Community – Sets SNMP Read-only password for SNMP. The default password is "public" (Length: 1~32 characters, case sensitive).

4.3 Wireless Settings

The SU-L's wireless settings, ESSID, security, regulatory domain, frequencies and other radio parameters are described in this section.



Access Point ESSID to Associate – The ESSID, or wireless network name, of the network you want to connect to. All wireless clients and Access Units in the same network must use the same ESSID to associate. The ESSID is case sensitive and can consist of up to 31 alphanumeric characters.

Authentication Algorithm – Sets the SU-L to communicate with an AU configured as an open system, or as a pre-configured system using static shared keys. (Default: Open System)

- Open System: If you don't set up any other security mechanism on the SU-L, the network has no protection. This is the default setting.
- Shared Key: Sets the SU-L to use shared keys. If this option is selected, you must configure at least one key on the SU-L and AU.

Data Encryption Option – Enable or disable the SU-L to use data encryption (WEP or AES-CCM). If this option is selected, you must configure at least one key on the SU-L and the AU. (Default: Disable)

NOTE



Selecting a data encryption option (WEP or AES-CCM) without specifying any encryption key will determine SU to use the 00000000000000000000000000000000 key (32 times 0).

Security Mode – Allows you to select the encryption algorithm employed when enabling the Data Encryption Option. You can choose between Advanced Encryption Standard in Counter with CBC-MAC mode (AES-CCM) and Wired Equivalent Privacy (WEP).

It is possible to associate an SU using the AES-CCM with an AU employing FIPS 197.

Default Key – Selects the key number to use for encryption. The key indicated by the default key selection must be configured with the same value in the AU and in the SU-L in order for the link to work (Default: Key 1.)

Keys – If the wireless network you are connecting to uses data encryption, you need to enter the keys provided to you by the network operator.

Enter "0x" followed by 32 hexadecimal digits (0 to 9 and A to F) for 152 bit keys.

RTS Threshold – Sets the packet size threshold at which a Request to Send (RTS) signal must be sent to a receiving station prior to the sending station starting communications. The SU-L sends RTS frames to a receiving station to negotiate the sending of a data frame. After receiving an RTS frame, the station sends a CTS (clear to send) frame to notify the sending station that it can start sending data.

NOTE



All wireless devices must be configured with the same Key values to communicate with an AU.

If the RTS threshold is set to 20, the SU-L always sends RTS signals. If set to 2347, the SU-L never sends RTS signals. If set to any other value, and the packet size equals or exceeds the RTS threshold, the RTS/CTS (Request to Send / Clear to Send) mechanism will be enabled.

The SU-Ls contending for the medium may not be aware of each other. The RTS/CTS mechanism can solve this "Hidden Node Problem." (Range: 20-2347 bytes: Default: 60 bytes)

Transmit Power Level – Adjusts the power of the radio signals transmitted from the SU-L. The higher the transmission power, the farther the transmission range. Power selection is not just a trade off between coverage area and maximum supported clients. You also have to ensure that high-power signals do not interfere with the operation of other radio devices in the service area. (Options: Full, Half, Quarter, Eighth, Min (0 dBm); Default: Full

Modulation Type and Link Rate – Sets the modulation type to limited or fixed. (Default: limited). It also sets the maximum data rate at which the SU-L transmits unicast packets on the wireless interface. The maximum transmission distance is affected by the data rate. The lower the data rate, the longer the transmission distance. (Default: 54 Mbps)

MIR uplink – Sets the Maximum Information Rate of the uplink from the SU to the AU. The MIR value cannot be lower than the corresponding CIR value.

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

MIR downlink – Sets the Maximum Information Rate of the downlink from the AU to the SU. The MIR value cannot be lower than the corresponding CIR value.

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

CIR uplink – Sets the Committed Information Rate of the uplink from the SU to the AU. The CIR value cannot be higher than the corresponding MIR value.

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

CIR downlink – Sets the Committed Information Rate of the downlink from the AU to the SU. The CIR value cannot be higher than the corresponding MIR value.

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

CIR delay – The maximum time packets may be delayed by the CIR\MIR buffering mechanism. Packets which are delayed longer than this period will be discarded. This decreases the MIR/CIR queues by limiting the number of available buffers. If the SU supports applications that are sensitive to delays, such as VoIP, this value should be decreased.

The CIR Delay setting only applies to downlink communications. (Range: 300-10000 ms; Default: 5000 ms)

Burst duration – This is the maximum duration of the initial burst of data sent after an equivalent or longer period of inactivity.

The MIR/CIR 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 intended for the AU has been received from the Ethernet port during the last N seconds, the unit is allowed to transmit to this destination N times its allowed CIR value without any delay.

For instance, the default value of 5 ms enables a maximum burst of (0.005 X CIR) Kbps after a period of inactivity of at least 5 milliseconds (provided overall conditions in the wireless link allow this burst).

The Burst Duration should be set to a lower value for delay sensitive traffic. Typically, the Burst Duration of the SUs should be set to lower values than that of the AU, because of the higher number of packets that should be transmitted by the AU. (Range: 0-2000 ms; Default: 5ms)

Min Contention Window – The Minimum Contention Window parameter determines how long after a unit concludes that there are no detectable transmissions by other units it will attempt to transmit its own data. The system uses a special mechanism based on detecting the presence of a carrier signal and analyzing the information contained in the transmissions of the AU to estimate the activity of other SUs served by the same AU. The target is to minimize collisions in the wireless medium resulting from multiple units attempting to transmit at the same time.

The system uses an exponential back-off algorithm to resolve contention between units accessing the wireless medium. The method requires each station to choose a random number N between 0 and a given number C each time it accesses the medium. The unit will attempt to access the medium only after a time interval equal to DIFS plus N time slots (see the AIFS description below for more details on DIFS), always checking if a different unit has already accessed the medium. 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 Minimum Contention Window parameter is the initial maximal value C used in the back-off algorithm. The higher the number of SUs served by the same AU, the higher the Minimum Contention Window for each SU should be.

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

NOTE



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 interval equal to DIFS. It should only be used in point-to-point applications

Max 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.

AIFS – The time interval between two consecutive frame transmissions is called Inter-Frame Spacing (IFS). This is the time during which the unit determines whether the medium is idle by using the carrier sense mechanism. The IFS varies depending 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 the Min Contention Window and Max Contention Window descriptions above) after reaching a decision that the medium has become free.

The Arbitration Inter-Frame Spacing (AIFS) is the difference between DIFS and SIFS. It is used to define the DIFS based on the SIFS using the following formula: DIFS = SIFS + AIFS. It can be configured to a value between 1 and 50 time slots. A unit with a lower AIFS has an advantage over units with higher AIFS values, 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 engaged in a point-to-point link, while in the other unit the AIFS remains configured to two time slots. The unit with AIFS configured to one will have an advantage over the other unit, provided that the Minimum Contention Window parameter in both units is configured to 0 to disable the contention window back-off algorithm.

(Range: 1-50 time slots; Default: 2 time slots)

Burst Time (ms) – The Burst Time (ms) option defines the time in which data frames are sent immediately without contending for the wireless medium.

The range is between 1 and 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).

Hardware retries – The Number of HW Retries parameter defines the maximum number of times that an unacknowledged frame is retransmitted in each Hardware Retrial phase. When the Adaptive Modulation Algorithm is disabled, a frame will be dropped when the number of unsuccessful retransmissions reaches this value. (Range: 1-14; Default: 10)

Preferred AU MAC Address – The Preferred AU MAC Address parameter defines a specific AU with which the SU should associate when it is set up. Once the SU has identified the preferred AU based on its MAC address, it will associate with it and terminate the scanning process. Setting up the 00:00:00:00:00:00 MAC address (12 zeros) means there is no preferred AU.

If there is no preferred AU MAC Address or if the preferred AU is unreachable after three scanning attempts, the SU-L will automatically employ the Best AU support mechanism. When the Best AU feature is used, each of the detected AUs is given a quality mark based on the signal received at the SU during the three successive scans. At the end of the scanning period, the SU reaches a Best AU decision according to the information gathered. The AU with the highest quality mark is selected as the Best AU, and the SU will immediately try to associate with it.

After a successful setup, if the connection between the SU and the preferred/best AU is lost, the SU will automatically reiterate the connection process described above. (Valid values: A MAC address string. The default value for the Preferred AU MAC Address is 00:00:00:00:00:00 (12 zeros), meaning that there is no preferred AU.)

RF Distance (Km) – The maximum data transmission distance. The maximum data rate for a link decreases as the operating range increases. (Default: 1km). The RF Distance should be set to the distance from the access unit of the furthest SU in the cell (up-rounded). Since this parameter affects the time the unit waits

for acknowledgement, wrong configuration of its value (too low or too high) may have a very strong negative effect on performance.

VLAN Support Mode (Link Type) – The SU-L is a VLAN aware equipment. This means it is able to handle VLAN ID and priority tag headers inside the transmitted frames. SU-L supports two types of links:

- **Access** - This type of link is applicable when the devices connected to the unit are VLAN unaware. The SU behaves as follows:
  - When receiving frames from the wireless port, only the ones with matching VLAN tag headers (see the **VLAN Tag For Data Frames** option below for details) will be forwarded to the Ethernet port. In the process, the SU will remove the VLAN tag headers.
  - When receiving frames from the Ethernet port, only the ones without VLAN tags will be forwarded to the wireless port. In the process, the SU will add the VLAN tag and VLAN priority headers defined below (see the **VLAN Tag For Data Frames** and **Priority Tagging For Data Frames** options below for details).
- **Hybrid** - This type of link supports both VLAN aware and VLAN unaware devices. The SU is VLAN transparent, transferring all tagged and untagged frames as they are.

VLAN Tag For Data Frames – VLAN ID that identifies the VLAN to which the unit belongs. It is inserted/removed when the unit is working in Access Mode. (Range: 1-4049; Default: 1)

Priority Tagging For Data Frames – VLAN priority tagging for data frames. Lower values indicate higher priorities. The priority tags are only inserted when working with Access link types. (Range:0-7; Default: 0).

VLAN Priority Threshold – Sets a threshold for the VLAN priority tag above which frames are routed via the High priority queue. It is only applicable for Hybrid links. (Range:0-7; Default:7 (all frames are routed via the Low priority queue)).

ToS Prioritization Option – Switches between prioritization based on either the 3 IP Precedence bits in the IP header (RFC 791) or the 6 Differentiated Services Code Point bits (RFC 2474). The following options are available:

- **Disable** - Disables ToS prioritization

- **IP Precedence (RFC 791)** - Enables precedence based on the IP Precedence bits in the IP header

- **DSCP (RFC 2474)** - Enables precedence based on the Differentiated Services Code Point bits in the IP header

The default value is Disable.

IP ToS Precedence Threshold – Sets a threshold for the IP Precedence bits' value above which frames are routed via the High priority queue. It is only applicable when IP Precedence ToS Prioritization (RFC 791) is enabled. (Range:0-7; Default:4).

DSCP Threshold – Sets a threshold for the Differentiated Services Code Point bits' value above which frames are routed via the High priority queue. It is only applicable when DSCP ToS Prioritization (RFC 2474) is enabled. (Range:0-63; Default:32).

UDP/TCP Port Ranges Prioritization – Sets up prioritization based on the destination UDP/TCP port ranges. The following settings are available:

- **Disable** - UDP/TCP Port Ranges Prioritization is disabled.

- **UDP only** - UDP Port Ranges Prioritization is enabled.

- **TCP only** - TCP Port Ranges Prioritization is enabled.

- **UDP and TCP** - Both UDP and TCP Port Ranges Prioritization is enabled.

The default value is Disable.

UDP Port RTP/RTCP Prioritization – Sets up prioritization for Voice over IP traffic over UDP ports depending on the protocol:

- **All Ports (RTP and RTCP)** - Both RTP (Real Time Protocol) and RTCP (Real Time Control Protocol) traffic is prioritized.

- **Even Ports (RTP only)** - Only RTP (Real Time Protocol) traffic is prioritized.

The default value is All Ports (RTP and RTCP).

TCP Port RTP/RTCP Prioritization – Sets up prioritization for Voice over IP traffic over TCP ports depending on the protocol:

- **All Ports (RTP and RTCP)** - Both RTP (Real Time Protocol) and RTCP (Real Time Control Protocol) traffic is prioritized.
- **Even Ports (RTP only)** - Only RTP (Real Time Protocol) traffic is prioritized.

The default value is All Ports (RTP and RTCP).

UDP Port Ranges – Defines priority port ranges for UDP traffic. You can enter a list of up to 64 port numbers and/or ranges. Use hyphens to separate start/end port numbers within a range. Use commas to separate entries.

Example: 9800,9000-9007,9010,9022-9036

TCP Port Ranges – Defines priority port ranges for TCP traffic. You can enter a list of up to 64 port numbers and/or ranges. Use hyphens to separate start/end port numbers within a range. Use commas to separate entries.

Example: 9800,9000-9007,9010,9022-9036

IP Range Option – This option prioritizes frames with source/destination IP address matching the predefined IP range. The available settings are:

- **Disable** - IP Range Prioritization is disabled.
- **Source IP** - Frames with matching source IP addresses are prioritized.
- **Destination IP** - Frames with matching destination IP addresses are prioritized.
- **Source or Destination IP** - Frames with matching source or destination IP address are prioritized.

The default value is Disable.

IP Range Start Address – IP address which, in conjunction with the IP range mask, defines the IP Range used for prioritization (Range: 4 groups of up to 3 digits separated by dots, Default: 0.0.0.0).

IP Range Mask – IP mask which, in conjunction with the IP range start address, defines the IP Range used for prioritization (Range: 4 groups of up to 3 digits separated by dots, Default: 255.0.0.0).

Regulatory Domain – The regulatory domain for the SU-L is preset for the country of intended operation and may only be configured through the CLI, (see “Regulatory Domain Commands” on page 85.) Within the allowed domain for your country of operation you may limit transmission on certain band frequencies by

deselecting the frequency on the grid and updating your settings. For example, deselecting 5.2 GHz 60 MHz, disables the 5.260 GHz frequency.

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).

Channel Check Time (seconds) - 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 overlappling partially or totally with frequency range 5600 - 5650 MHz, the Channel Check Time is forced to minimum 600 seconds (10 minutes).

Channel Avoidance Period (minutes) - 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's frequency marking will change to Radar Free.

The range is 1 to 60 minutes.

The default is 30 minutes.

Clear Radar Detected Channels - When the Clear Radar Detected Channels is enabled, after the next update 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 unit will start operation using its default frequency.

The default is Disable.

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

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.

Bandwidth (MHz) – Sets the channel bandwidth:

- **10** - 10 MHz channels
- **20** - 20 MHz channels
- **10-20** - Either 10 or 20 MHz channels

The default value is 10-20.

Select All – Selects all available frequencies in the regulatory domain.

Clear All – De-selects all available frequencies in the regulatory domain (at least one frequency will be retained for security purposes).

LED Operation Mode – Allows users to customize the operation mode for the 7 SNR leds. The leds are numbered as follows: from 1 to 3 the first 3 LEDs from left to right on the upper row, and from 4 to 7 the LEDs on the second row from left to right. The Power LED's behavior is not affected by these settings:

- **Normal** - This is the default mode of operation where the LEDs indicate the SNR level (see "LED Indicators" on page 16 for more information).
- **Threshold** - Allows customization for each LED behavior by setting a Modulation, SNR, CRC or RSSI threshold in respect to which the LED will light

up. When the Threshold mode is enabled, a table is displayed, allowing users to set thresholds for each LED:

- **Type** - Indicates 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
  - **Modulation** - Sets up a threshold for the average modulation
- **Mode** - Defines how the threshold parameter relates to the threshold target
  - **lower than or equal to** - The threshold parameter must be lower than or equal to the threshold target value for the LED to light up.
  - **greater than or equal to** - The threshold parameter must be greater 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.
- **Target** - Defines the threshold target values. Depending on the threshold type, the following value ranges apply:

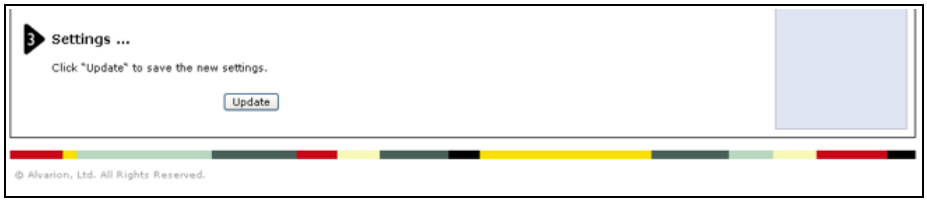
Table 4-1: Threshold Target Value Ranges

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

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.

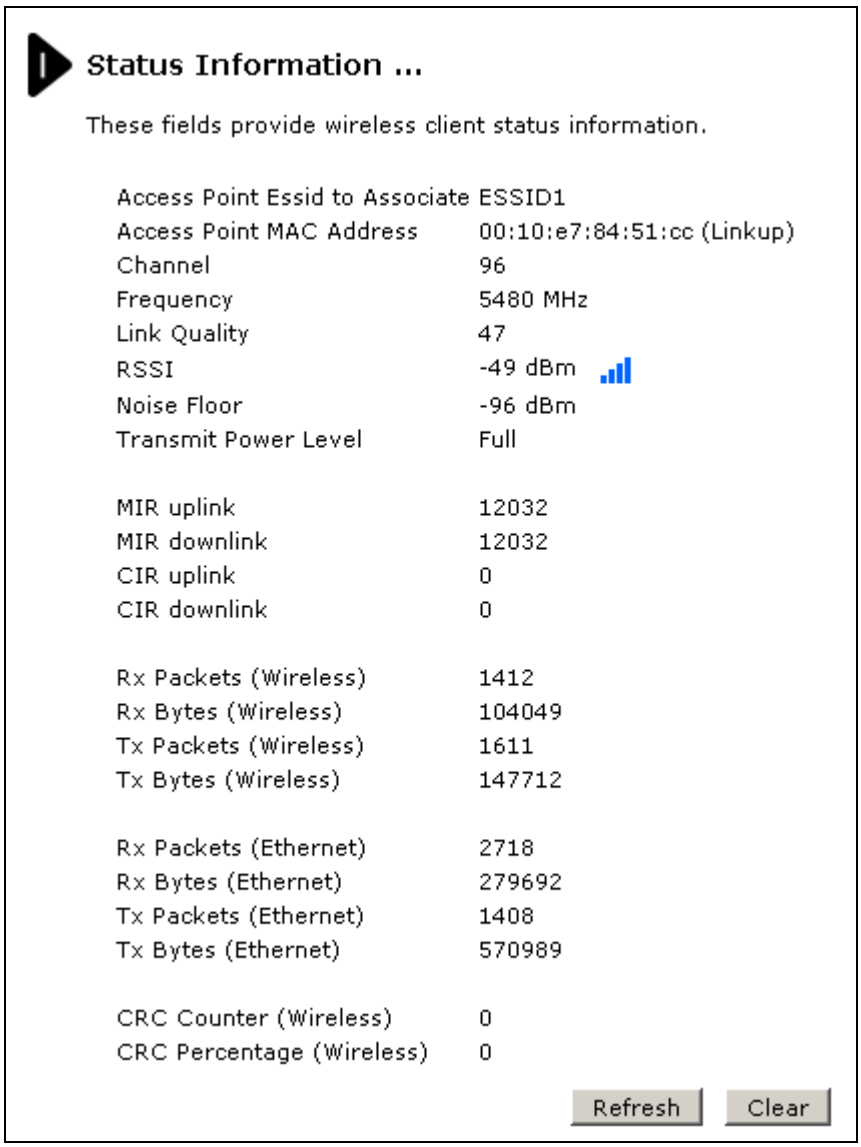
4.4 Saving Settings

To save any new settings, click “Update”.



4.5 Status Information

The “Review description of this client station” displays basic system configuration settings and traffic counters for the SU-L.



Access Point ESSID to Associate – The service set identifier of the network to which the client wants to associate.

Access Point MAC Address – The physical layer address of the AU. Specified in the form of six pairs of hexadecimal digits separated by colons; for example, 00:10:E7:01:02:03.

Channel – Displays the radio channel through which the SU-L communicates with the AU.

Frequency – Displays the frequency at which the SU-L is transmitting.

Link Quality – Displays the quality of the signal received at the SU-L.

RSSI – Receive Signal Strength Indicator (RSSI) displays the strength of the received signal, measured in dBm.

Noise Floor – Indicates the level of interference noise above which the received signal must be for successful reception, measured in dBm.

Transmit Power Level – Indicates the power of the radio signals transmitted from the SU-L.

MIR/CIR uplink/downlink – Indicates the values in Kbps for the Maximum Information Rated and Committed Information Rate for both SU to AU and AU to SU communication.

Rx/Tx Packets/Bytes (Wireless) – The number of successfully received (Rx) and transmitted (Tx) data packets/bytes via the wireless port since the unit was last reset or since the counters were cleared.

Rx/Tx Packets/Bytes (Ethernet) – The number of successfully received (Rx) and transmitted (Tx) data packets/bytes via Ethernet since the unit was last reset or since the counters were cleared.

CRC Counter (Wireless) – The number of Cyclic Redundancy Check errored packets received over the air link.

CRC Percentage (Wireless) – The percentage of Cyclic Redundancy Check errored packets received over the air link. The exact formula is the following:

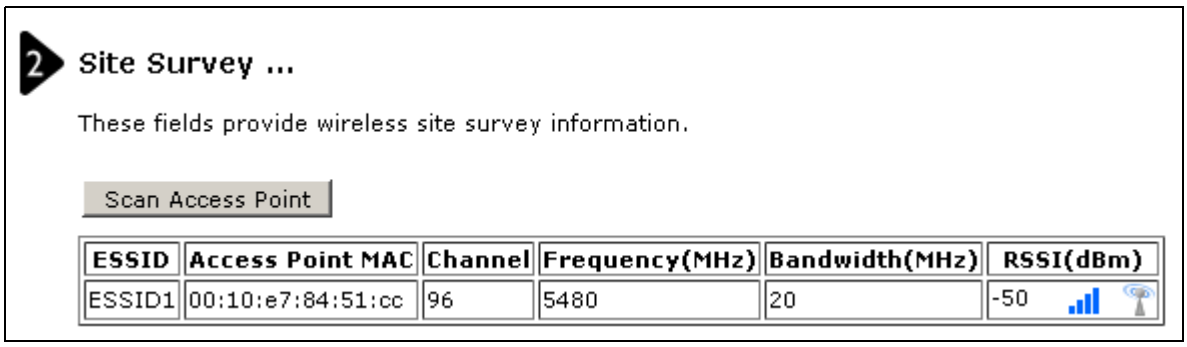
$$CRCpercentage(Wireless) = \frac{CRCcounter(Wireless) \times 100}{CRCcounter(Wireless) + RXpackets(Wireless)}$$

Refresh – Updates the statistics to the most recent data.

Clear – Resets the Rx/Tx counters to a null value.

4.6 Site Survey

The Site Survey scans the available frequencies for neighboring wireless devices that act as APs (that generate beacons).

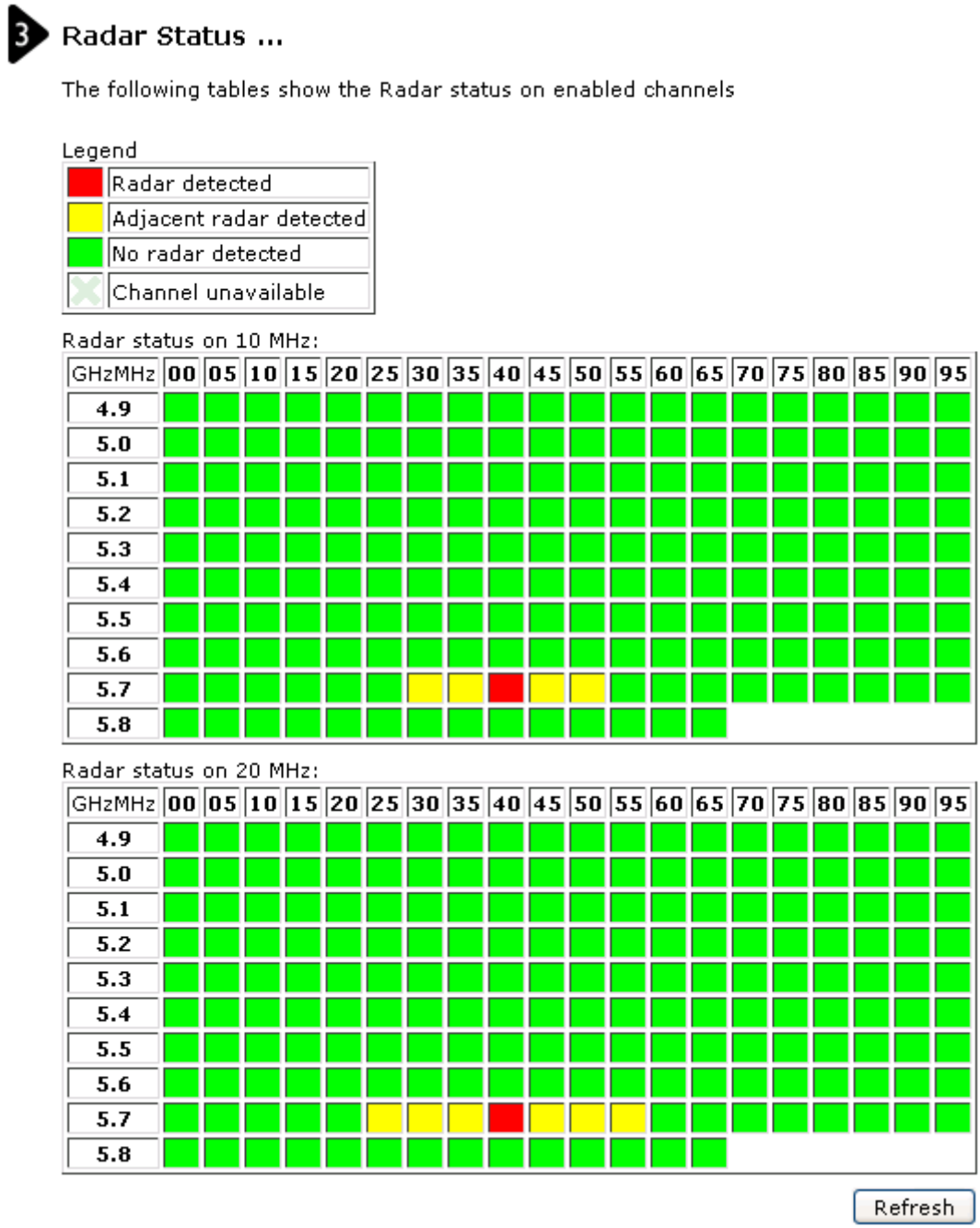


Scan Access Point – Click this to perform a scan for neighboring wireless devices.

4.7 Radar Status

The Radar Status section displays the radar detection status for each available channel. Each channel is color coded as follows:

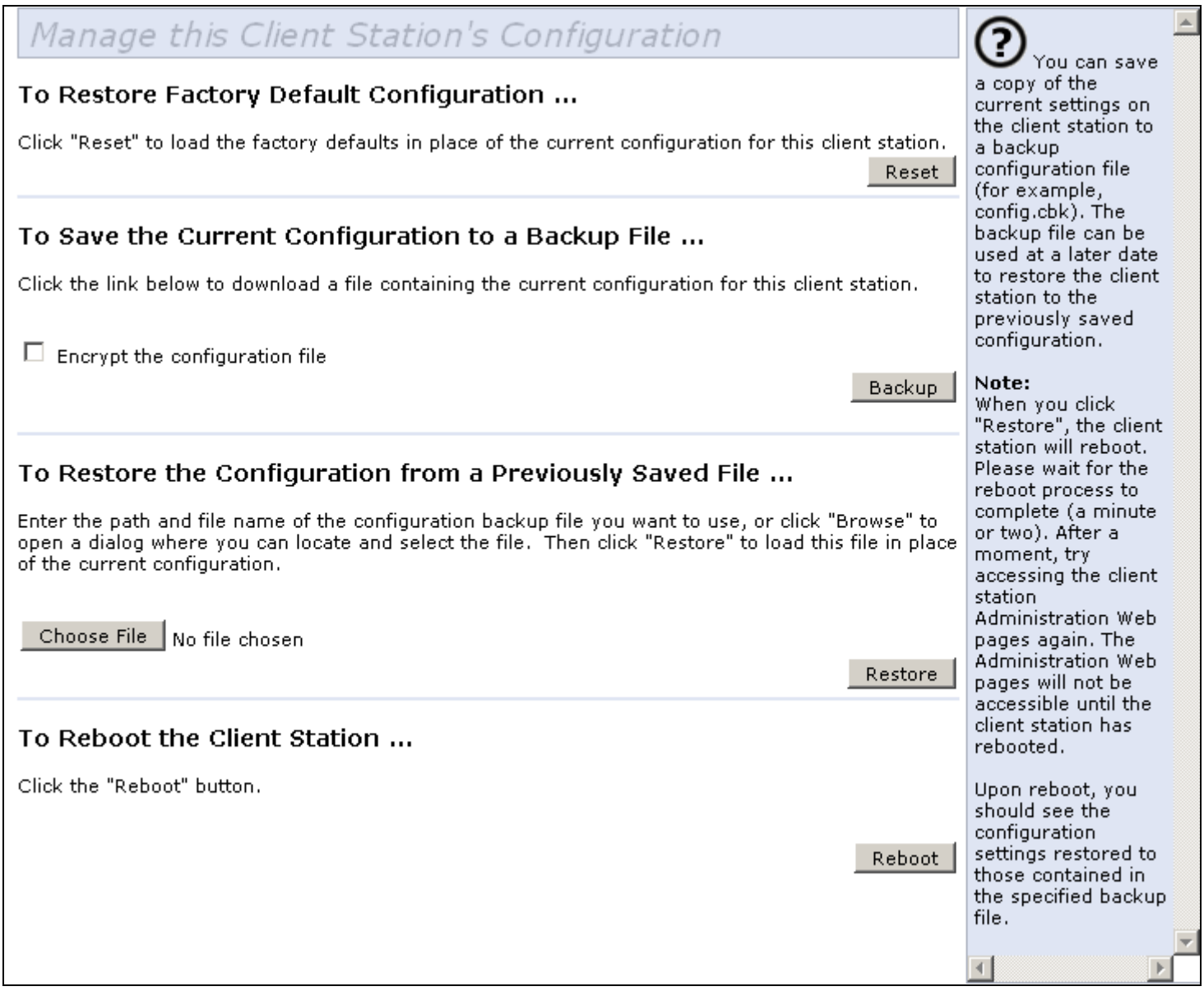
- Radar free channels are colored in green
- Channels adjacent to radar are colored in yellow
- Channels that are occupied by radar are colored in red
- Unavailable channels are crossed out



Click the Refresh button to update the Radar Status table

4.8 Managing the SU-L Configuration

The Maintenance/Configuration page allows you to save and restore the unit's configuration settings, restore factory defaults, and to reset the unit.



To Restore Factory Default Configuration – Click the Reset button to set the configuration settings for the SU-L to the factory defaults and reboot the system. Note that all user configured information will be lost. You will have to re-enter the default user name (admin) and password (private) to re-gain management access to this device.

To Save the Current Configuration to a Backup File – Click the Backup button to download the current SU-L configuration file to the web management station. Check the Encrypt the configuration file check-box to store the backup configuration file in an encrypted format.

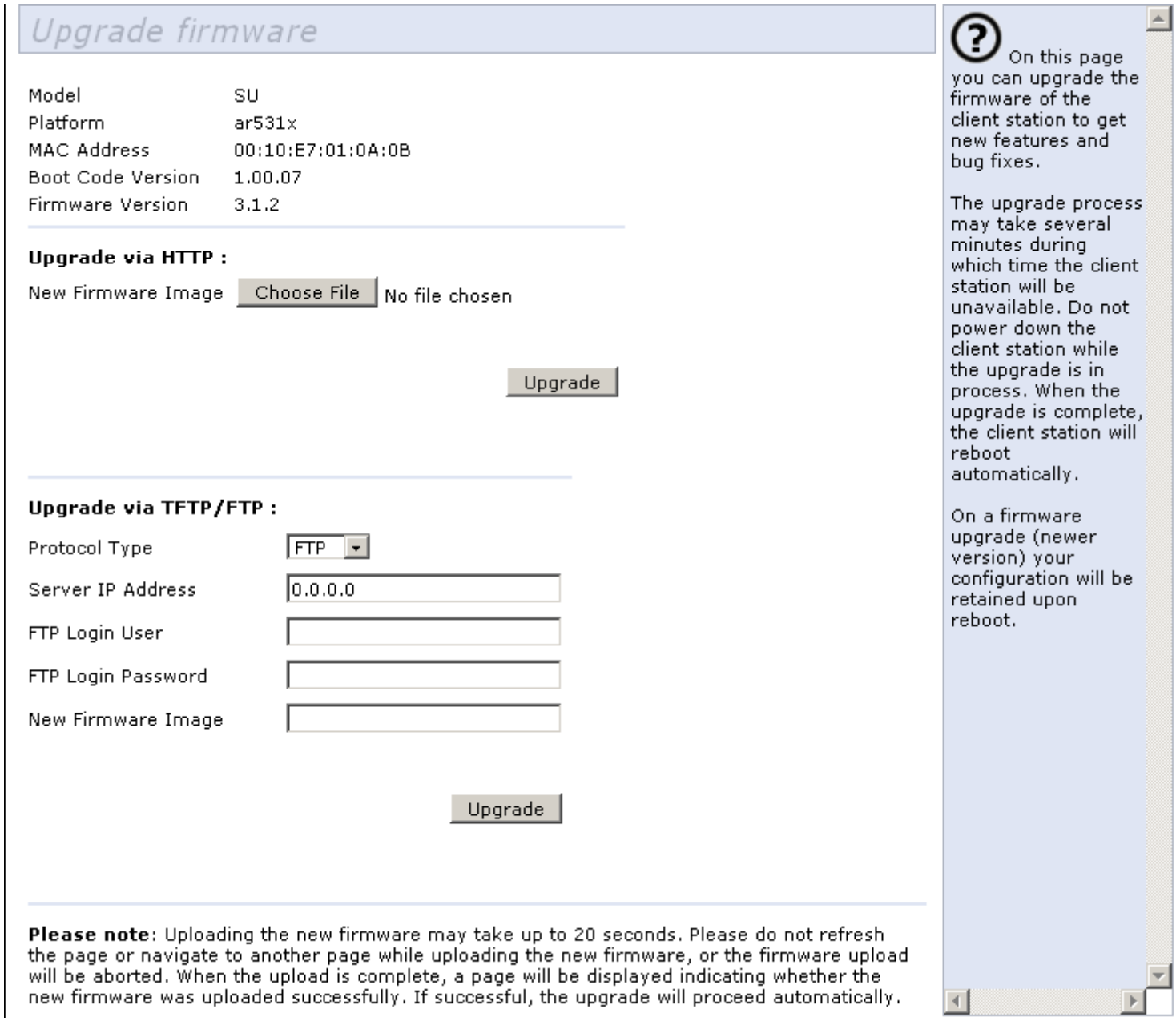
To Restore the Configuration From a Previously Saved File – Sends a saved configuration file on the web management station to the SU-L to restore a specific configuration. You can use the Choose File button to find the configuration file on the local PC. Click the Restore button to replace the current SU-L configuration.

To Reboot the Client Station – Click the Reboot button to reset the system.

4.9 Upgrading SU-L Firmware

You can upgrade new SU-L firmware (often called system software) from a local file on the management workstation.

After upgrading new software, the SU-L will automatically reboot itself and load the new code.



Model – Shows the model number of the SU-L.

Platform – Shows the platform number of the hardware.

MAC Address – Shows the physical address of the SU-L.

Boot Code Version – Shows the current version number of the boot code.

Firmware Version – Shows the current version number of the runtime code.

Upgrade via HTTP – Upload a new software version to the unit using HTTP. Use the Choose File button to locate the image file locally on the management station and click the Upgrade button to proceed.

Upgrade via TFTP/FTP – Upload a new software version to the unit using TFTP or FTP.

Protocol Type – Selects either the TFTP or FTP protocol for the upgrade process.

Server IP Address – IP address of FTP / TFTP server. This is the server that is hosting the new software version.

FTP Login User – Applicable only for FTP. Username for logging in to the FTP server

FTP Login Password – Applicable only for FTP. Password for logging in to the FTP server

New Firmware Image – Name of the new software version. Please enter a valid file-name that is present on FTP / TFTP server. Select “Upgrade” to start the download process.



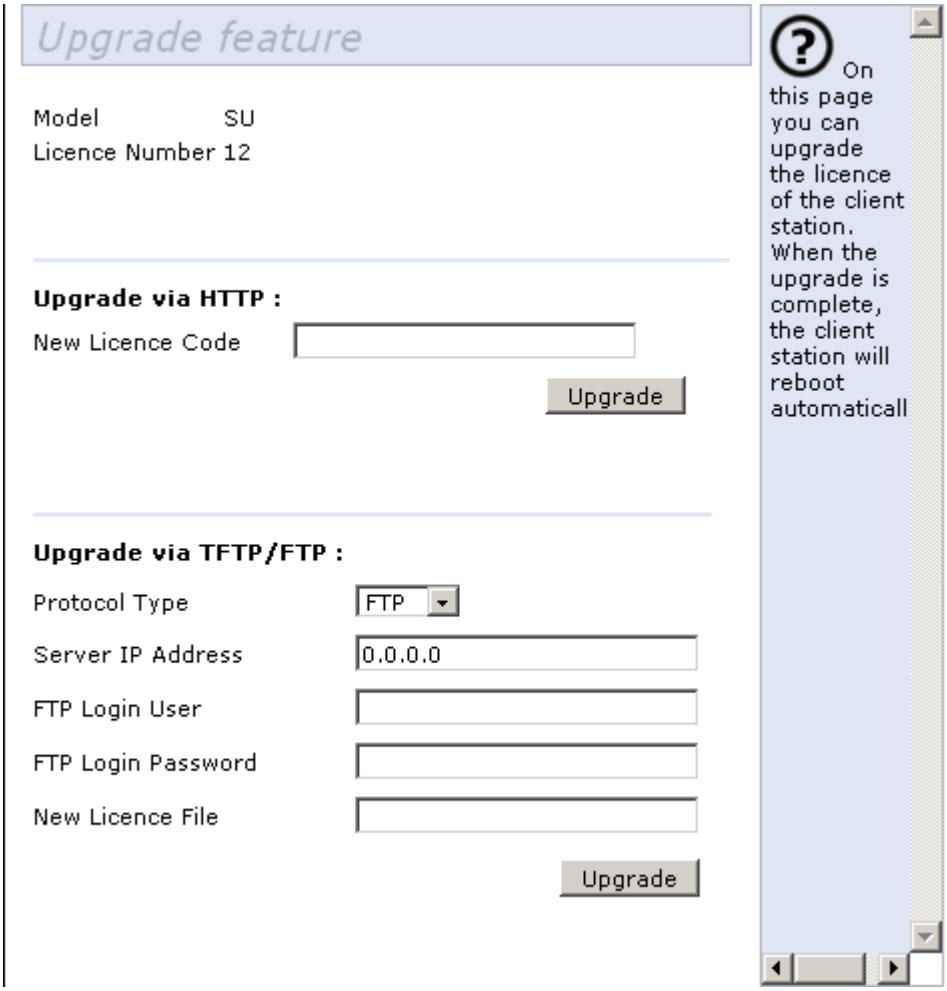
NOTE

Be sure to allow enough time for the firmware download to complete and the unit automatically reboot itself. Typical download time is 5 minutes when the unit is not handling heavy traffic.

Rebooting the unit before completion of the download may damage the software and cause the unit to be inoperative..

4.10 Feature Upgrade

It is possible to load new license code to the unit to support new features. When you click the "Upgrade" button, the unit will automatically update its configuration making the new feature available. There is no need to reset the unit.



Model – Shows the unit type

Licence Number – Shows the model type

Upgrade via HTTP – Insert the new license code provided by Alvarion. Each license code is associated with a unique MAC Address and one feature/option. If the inserted encrypted string does not match, the code will be rejected by the unit. After inserting the license code, click the "Upgrade" button to proceed. The unit will automatically update its configuration making the new feature available. There is no need to reset the unit.

Upgrade via TFTP/FTP – Download a license file image using TFTP or FTP protocol.

Protocol Type – Selects either TFTP or FTP.

Server IP Address – IP address of FTP/TFTP server. This is the server that is hosting the new license code file.

FTP Login User – Applicable only for FTP. Username for logging in to the FTP server

FTP Login Password – Applicable only for FTP. Password for logging in to the FTP server

New Firmware Image – Name of the license code file. Please enter a valid file-name that is present on FTP / TFTP server.

Select “Upgrade” to start the download process.

Chapter 5

Command Line Interface

In This Chapter:

- "Using the Command Line Interface" on page 74
- "Entering Commands" on page 76
- "General Commands" on page 79
- "LED Operation Mode Commands" on page 82
- "Regulatory Domain Commands" on page 85
- "Password Commands" on page 90
- "File Commands" on page 92
- "SNMP Commands" on page 105
- "Ethernet Interface Commands" on page 106
- "Wireless Commands" on page 109
- "VLAN Commands" on page 121
- "Contention Commands" on page 123
- "MIR/CIR Commands" on page 126
- "DFS Commands" on page 129
- "Traffic Prioritization Commands" on page 133

5.1 Using the Command Line Interface

5.1.1 Accessing the CLI

When accessing the management interface via a Telnet connection, the SU-L (CPE) unit can be managed by entering command keywords and parameters at the prompt. Using the SU-L's command-line interface (CLI) is very similar to entering commands on a UNIX system.

5.1.2 Telnet Connection

Telnet operates over the IP transport protocol. In this environment, your management station and any network device you want to manage over the network must have a valid IP address. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Each address consists of a network portion and host portion.

To access the SU-L through a Telnet session, you must first use the default IP address 10.0.0.1.



To open a Telnet session:

1. From the remote host, enter the Telnet command and the IP address of the device you want to access.
2. At the prompt, enter the user name and system password for the command mode that you wish to enter. There are two command modes: admin mode and installer mode. Admin mode allows you to configure most settings with the exception of the regulatory domain. The regulatory domain may be configured through the installer mode only.
3. The CLI will display the prompt for the mode you enter, for example Installer# to show that you are using the Installer user account and ClientSta# for priviledged access mode.
4. Enter the necessary commands to complete your desired tasks.
5. When finished, exit the session with the "exit" command.

After entering the Telnet command, the login screen is displayed:

```
ClientSta login: installer
Password: *********
Installer#
```



CAUTION

You can open up to four sessions to the device via Telnet.

5.2 Entering Commands

This section describes how to enter CLI commands.

5.2.1 Minimum Abbreviation

The CLI does not accept incomplete commands. For example, the command "addfreq" can not be entered as **add**. In exchange, you can get hints from the CLI by entering "add" followed by TAB key. If an entry is ambiguous or incorrect, the system will not prompt for further input, nor inform you if you have entered incorrect syntax.

5.2.2 Command Completion

If you terminate input with a Tab key, the CLI will print the remaining characters of a partial keyword up to the point of ambiguity. In the “configure” example, typing **ex** followed by a tab will result in printing the command up to “**exit**.”

5.2.3 Getting Help on Commands

You can display a brief description of the help system by pressing the tab key twice at the command prompt.

Example

```
ClientSta#
addfreq         Add Frequency
delfreq         Delete Frequency
dynamicfreq     Set Exactly Frequency
exit            Logout the system
get             Get property values of the running configuration
getfreq         Get Current Frequency
ping
reboot          Reboot the system
save-running    Save the running configuration
set             Set property values of the running configuration
```

The help system may show additional detail by adding a term to query and then pressing the tab key twice, for example “set” followed by a double tab displays all parameters associated with this command set only.

Example

```
Installer# set
CStatus      status class
ClientSta    client station
config       Configuration settings
system       System settings
tftpftp      tftpftp class
Installer# set
```

Furthermore, adding an additional term displays more help system results, for example entering “set ClientSta” followed by a double tab displays all parameters associated with this command subset only.

Example

```
Installer# set ClientSta
authentication           authentication algorithm
bridge-mip               bridge ip mask
bridge-static-ip         bridge ip
data-encryption-option   data encryption option
default-gw               default gateway
default-key              default key
dhcpc                    DHCP client
distance                 wireless RF distance
key-1                    wep key string #1
key-2                    wep key string #2
key-3                    wep key string #3
key-4                    wep key string #4
linkrate                 link rate
mangVLAN                 management VLAN
modulation               modulation type
rtsthreshold             RTS threshold
snmp-rocommunity         SNMP read-only community
status-update            status of station
txpowerlevel             TxPower Level
wireless-essid           essid
Installer#
```

5.2.4 Partial Keyword Lookup

If you terminate a partial keyword with pressing the tab key twice, alternatives that match the initial letters are provided. (Remember not to leave a space between the command and tab keys.) For example "**s<Tab><Tab>**" shows all the keywords starting with “s.”

```
Installer# s
save-running   Save the running configuration
set            Set property values of the running configuration
Installer# s
```

5.2.5 Command Line Processing

Commands are case sensitive. You can abbreviate commands and parameters as long as they contain enough letters to differentiate them from any other currently available commands or parameters. You can use the Tab key to complete partial commands.

5.3 General Commands

Table 5-1: General Commands

Command	Function	Mode	Page
exit	Logs out of the current session.	Installer; Admin	79
ping	Sends a ping signal to test for connectivity.	Installer; Admin	79
reboot	Reboots the unit.	Installer; Admin	81

5.3.1 exit

The "exit" command allows you to log out of the current session.

Syntax

exit

Default Setting

None

Command Mode

Installer, Admin

Example

This example shows how to logout of the current session:

```
Installer#exit
ClientSta login:
```

5.3.2 ping

This command sends ICMP echo request packets to another node on the network.

Syntax

ping <*ip_address*>

- *ip_address* - IP address of the host.

Default Setting

None

Command Mode

Installer, Admin

Command Usage

- Use the ping command to see if another site on the network can be reached.

- The following are some results of the ping command:
  - It details how many bytes were received, and the time taken from sending the request to the response.
  - If the host does not respond the screen returns a blank and continues sending a ping request until it is manually stopped by the user with the CTRL+C command. After typing this command a summary is displayed describing packets transmitted, packets received and percentage of packet loss.
- Press <Ctrl-C> to stop pinging.

Example 1

```
Installer# ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1): 56 data bytes
64 bytes from 10.0.0.1: icmp_seq=0 ttl=64 time=0.4 ms
64 bytes from 10.0.0.1: icmp_seq=1 ttl=64 time=0.3 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=64 time=0.3 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=64 time=0.3 ms
64 bytes from 10.0.0.1: icmp_seq=4 ttl=64 time=0.3 ms
64 bytes from 10.0.0.1: icmp_seq=5 ttl=64 time=0.3 ms

--- 10.0.0.1 ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 0.3/0.3/0.4 ms
Installer#
```

Example 2

```
Installer# ping 10.0.0.23

--- 10.0.0.23 ping statistics ---
78 packets transmitted, 0 packets received, 100% packet loss
Installer#
```

Example 3

```
Installer# ping 192.168.2.1
PING 192.168.2.1 (192.168.2.1): 56 data bytes
ping: sendto: Network is unreachable
Installer#
```

5.3.3 reboot

This command restarts the system.

Syntax

reboot

Default Setting

None

Command Mode

Installer, Admin

Command Usage

Used for troubleshooting. If you perform a reboot without prior using the “save-running” command, your parameter changes will be lost.

Example

This example shows how to reset the system:

```
Installer#reboot
```

5.4 LED Operation Mode Commands

The following commands configure the SNR LEDs' behavior.

Table 5-2: LED Operation Mode Commands

Command	Function	Mode	Page
set ClientSta ledMode	Sets the SNR LEDs into the Normal or Threshold mode.	Installer; Admin	82
set ClientSta led1Type ~ led7Type	In Threshold mode, this option sets the threshold parameter that is monitored for the respective LED.	Installer; Admin	82
set ClientSta led1Mode ~ led7Mode	In Threshold mode, this option sets the relational operator that is applied to the threshold target to determine whether the LED will light up.	Installer; Admin	83
set ClientSta led1Target ~ led7Target	In Threshold mode, this option sets the threshold target that is monitored for the respective LED.	Installer; Admin	84

5.4.1 set ClientSta ledMode

Sets the SNR LEDs behavior

Syntax

set ClientSta ledMode <normal | threshold>

- **normal -** LEDs indicate the SNR level
- **threshold -** Each LED indicates whether a specific threshold is reached. If all the thresholds that were set up are reached, the entire SNR bar will light up, irrespective of the number of thresholds that were set.

Default Setting

normal

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta ledMode threshold
Installer#
```

5.4.2 set ClientSta led1Type ~ led7Type

When the SNR LEDs are in threshold mode, this command sets the type of parameter that is monitored for the respective LED and that the threshold is set for.

Syntax

set ClientSta led#Type <disabled | rssi | crc | snr | modulation>

- **disabled -** The LED is disabled
- **rssi -** The LED is monitoring the Received Signal Strength Indicator level.
- **crc -** The LED is monitoring the Cyclic Redundancy Check percentage.
- **snr -** The LED is monitoring the Signal-to-Noise Ratio.
- **modulation -** The LED is monitoring the average modulation level.

Default Setting

disabled

Command Mode

Installer, Admin

Example 1:

```
Installer# set ClientSta led2Type rssi
Installer#
```

Example 2:

```
Installer# set ClientSta led5Type modulation
Installer#
```

5.4.3 set ClientSta led1Mode ~ led7Mode

When the SNR LEDs are in threshold mode, this command sets how the threshold parameter relates to the threshold target value for the LED that the threshold is set for.

Syntax

set ClientSta led#Mode <eq | ge | le>

- **le -** The threshold parameter must be lower than or equal to the threshold target value for the LED to light up.
- **ge -** The threshold parameter must be greater than or equal to the threshold target value for the LED to light up.
- **eq -** The threshold parameter must be equal to the threshold target value for the LED to light up.

Default Setting

le

Command Mode

Installer, Admin

Example 1:

```
Installer# set ClientSta led2Mode ge
Installer#
```

Example 2:

```
Installer# set ClientSta led5Mode eg
Installer#
```

5.4.4 set ClientSta led1Target ~ led7Target

When the SNR LEDs are in threshold mode, this command sets the threshold target value for the LED that the threshold is set for.

Syntax

set ClientSta led#Target <*target value*>

- *target value* **-** Numeric string. Range: -108...0 for RSSI, 0...100 for CRC, 0...80 for SNR, 1...8 for modulation

Command Mode

Installer, Admin

Example 1:

```
Installer# set ClientSta led2Target -50
Installer#
```

Example 2:

```
Installer# set ClientSta led5Target 7
Installer#
```

5.5 Regulatory Domain Commands

Before transmitting wireless data from the unit, you should determine the correct regulatory domain setting for the country in which you are operating the SU-L. The selected regulatory domain must comply with applicable local radio regulations.

Table 5-3: Regulatory Domain Commands

Command	Function	Mode	Page
regdomain	Allows you to select what regional domain to set.	Installer	85
addfreq	Adds one or more individual frequencies or a range of frequencies within the band allowed by the chosen regulatory domain.	Installer; Admin	86
dynamicfreq	Configures one or more frequencies or a range of frequencies within the band allowed by the chosen regulatory domain (old setting are overwriten).	Installer, Admin	87
delfreq	Deletes one or more individual frequencies or a range of frequencies.	Installer; Admin	88
getfreq	Displays the currently used frequencies.	Installer; Admin	88

5.5.1 regdomain

This command allows you to set the regulatory domain in which the SU-L will be used. After selecting the required domain, the unit must be rebooted for changes to take effect.



WARNING

It is the responsibility of the wireless system operator to verify that use of the selected regulatory domain does not result in violation of the relevant local radio regulations!

Syntax

regdomain <**FCC** | **ETSI** | **UK** | **JAPAN** | **Universal** | **WLG** | **India** | **Brazil**>

- **FCC -** Federal Communications Commission.
- **ETSI -** European Telecommunications Standards Institute.
- **UK -** United Kingdom.
- **JAPAN -** Japan (Disabled in this version).
- **Universal -** For a testing environment only. Do not select for wireless transmission of data outside of a test environment. This selects all frequencies in the 802.11a bandwidth.
- **WLG -** White Logo: may be customized to a domain other than those stated above. Access restricted.

- **India -** India
- **Brazil -** Brazil

Default Setting

Universal

Command Mode

Installer

Example

This example shows how to display all possible regulatory domains by entering the syntax “regdomain” followed by the RETURN key, followed by selecting the ‘FCC’ domain by entering the syntax “regdomain FCC”.

```
Installer# regdomain
Usage :
        regdomain [FCC | ETSI | UK | JAPAN | Universal | WLG | India | Brazil]
Installer# regdomain FCC
Installer# reboot
....
```

5.5.2 addfreq

This command allows you to add individual frequencies and/or frequency ranges within the band allowed by the chosen regulatory domain.

Syntax

addfreq <*f1* | *f2* | *f3-f4*>

- *f1*, *f2* - Specify the frequencies you wish to add to the regulatory domain, in MHz, i.e. for the frequency 5.500 GHz type 5500
- *f3-f4* - A frequency range may be entered by separating two frequencies with a “-”, for example type ‘5500-5560’, to select the range from 5.500GHz to 5.560GHz.

Default Setting

None

Command Mode

Installer, Admin

Example

In this example the command is entered and the following help is displayed by pressing the ‘enter’ key. The frequency 5.520GHz is then added to the regulatory domain. Use the getfreq command to display all selected frequencies.

```
Installer# addfreq
Usage :
        addfreq [f1,f2,f3-f4...]
Installer#
Installer# addfreq 5520
Installer#
```

5.5.3 dynamicfreq

This command allows you to set one or more individual frequencies and a range of frequencies, allowed by the chosen regulatory domain.

Syntax

dynamicfreq <*f1,f2,f3-f4*>

- *f1,f2,f3-f4* - Specify the individual frequencies and/or frequency ranges that you wish to replace the already configured scanning frequency list, in MHz, separated by comas and no spaces. For a frequency range, separate the beginning and ending frequencies with a "-", i.e. for the frequencies 5.26GHz, 5.54GHz, and the range 5.7~5.785 type '5260,5540,5700-5785'

Default Setting

None

Command Mode

Installer, Admin

Example

In this example the frequencies 5.260GHz, 5.540GHz, and 5.700GHz to 5.785GHz are added within the band allowed by the chosen regulatory domain FCC. The getfreq command is then used to display all selected frequencies.

```
Installer# dynamicfreq 5260,5540,5700-5785
...
Installer# getfreq
...
5260,5540,5700,5745,5765,5785
Installer#
```

5.5.4 delfreq

This command allows you to delete one or more individual frequencies and/or ranges of frequencies within a band allowed by the chosen regulatory domain.

Syntax

delfreq <*f1* | *f2* | *f3-f4*>

- *f1, f2* - Specify the frequencies you wish to remove within a band allowed by the chosen regulatory domain, in MHz, i.e. for the frequency 5.5GHz type 5500
- *f3-f4* - A frequency range may be entered by separating two frequencies with a "-", for example type '5500-5560', to select the range from 5.5GHz to 5.56GHz.

Default Setting

None

Command Mode

Installer, Admin

Example

In this example the frequency 5.500GHz is deleted from the frequency range.

```
Installer# delfreq 5500
Installer#
```

5.5.5 getfreq

This command allows you to display the available frequencies that the unit is using.

Syntax

getfreq

Default Setting

None

Command Mode

Installer, Admin

Example 1

This example shows how to display all selected frequencies in the regulatory domain ETSI:

```
Installer# getfreq
5300,5700-5735
Installer#
```

Example 2

This example shows how to use the addfreq command to add a frequency, the delfreq command to remove another frequency, and the getfreq command to display the updated list of frequencies:

```
Installer# getfreq
5520,5540,5600,5580,5620,5640,5660,5680,5700
Installer# addfreq 5500
Installer# delfreq 5600
Installer# getfreq
5500,5520,5540,5560,5580,5620,5640,5660,5680,5700
Installer#
```

NOTE



Be aware that the new range or frequency will be applied after reset or after running the "set ClientSta status-update yes" command.

5.6 Password Commands

After initially logging onto the system, you should set a new password for both Admin and Installer modes. Remember to record your passwords in a safe place.

Table 5-4: Password Commands

Command	Function	Mode	Page
set system password	Specifies the password for management access to the Admin account.	Admin	90
passwd	Specifies the password for management access to the Installer account.	Installer	91

5.6.1 set system password

This command changes the password for Admin mode.

Syntax

set system password <*password*>

- *password* - A string (Range:1~32 printable characters).

Default Setting

"private"

Command Mode

Admin

Example

```
Admin# set system password a-good-secret
Admin#
```

5.6.2 passwd

This command changes the password for Installer mode. After entering the command you will be prompted to enter the new password twice. The password may be 5~8 characters, using upper and lower case letters and numbers, with no spaces, nor comas.

Syntax

passwd

Default Setting

"installer"

Command Mode

Installer

Example

```
Installer# passwd
Changing password for installer
Enter the new password (minimum of 5, maximum of 8 characters)
Please use a combination of upper and lower case letters and numbers.
Enter new password:*********
Re-enter new password:*********
Password changed.
Write Config Area ...Finished!
Installer#
```

5.7 File Commands

Table 5-5: File Commands

Command	Function	Mode	Page
save-running	Saves the current running configuration.	Installer; Admin	93
set config default	Reboots the system and restores factory default settings.	Installer, Admin	93
set ClientSta status-update	Applies all parameters that are currently set in the unit.	Installer, Admin	93
set tftpftp ftppass	Sets the FTP password.	Installer, Admin	94
set tftpftp ftpuser	Sets the FTP user name.	Installer, Admin	94
set tftpftp ptype	Selects the method used for file transfer.	Installer, Admin	95
set tftpftp rfile	Sets the name of the file for upgrade.	Installer, Admin	95
set tftpftp sip	Sets the IP address of the FTP or TFTP server.	Installer, Admin	95
set tftpftp start	Starts the file upgrade process.	Installer, Admin	96
get tftpftp	Displays detailed information about FTP or TFTP settings.	Installer, Admin	96
get config	Displays whether the default configuration for the unit's specific version will be in use after reset.	Installer, Admin	97
get interface	Displays interface information.	Installer, Admin	98
get system	Displays information regarding the SU's hardware and software.	Installer, Admin	98
get ClientSta	Displays detailed system information about the SU.	Installer, Admin	100

5.7.1 save-running

This command allows you to save the running configuration to flash memory, so that after a reboot the current configuration will be restored.

Syntax

save-running

Default Setting

No

Command Mode

Installer, Admin

```
Installer# save-running
Installer#
```

5.7.2 set config default

This command restores the factory default settings and restarts the system.

Syntax

set config default <**yes** | **no**>

- **yes** - Resets settings to the factory default and reboots the system.
- **no** - Takes no action.

Default Setting

no

Command Mode

Installer, Admin

Example

```
Installer# set config default yes
Installer#
```

5.7.3 set ClientSta status-update

This command will apply all parameters that are currently set in the unit. Please be aware that after this command is issued, the unit will disassociate and perform a new association process.

Syntax

set ClientSta status-update <**yes** | **no**>

- **yes** - Enables configuration update.
- **no** - No action.

Default Setting

no

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta status-update yes
Installer#
```

5.7.4 set tftpftp ftppass

Sets the password for the FTP connection.

Syntax

set tftpftp ftppass <*password*>

- *password* - Alphanumeric string (Range: up to 36 characters).

Default Setting

Blank

Command Mode

Installer, Admin

Example

```
Installer# set tftpftp ftppass unforgetable
Installer#
```

5.7.5 set tftpftp ftpuser

Sets the user name for the FTP connection.

Syntax

set tftpftp ftpuser <*username*>

- *username* - Alphanumeric string (Range: up to 36 characters).

Default Setting

Blank

Command Mode

Installer, Admin

Example

```
Installer# set tftpftp ftpuser David
Installer#
```

5.7.6 set tftpftp ptype

Selects FTP or TFTP for file transfer.

Syntax

set tftpftp ptype <**ftp** | **tftp**>

- **ftp** - Selects FTP.
- **tftp** - Selects TFTP.

Default Setting

tftp

Command Mode

Installer, Admin

Example

```
Installer# set tftpftp ptype ftp
Installer#
```

5.7.7 set tftpftp rfile

Set the name of the file that will be downloaded from FTP server (rfile = remote file). The new firmware file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.). (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")

Syntax

set tftpftp rfile <*file*>

- *file* - The name of the file for transfer.

Default Setting

upgrade.tar

Command Mode

Installer, Admin

Example

```
Installer# set tftpftp rfile 1.00.14.tar
Installer#
```

5.7.8 set tftpftp sip

IP address of FTP or TFTP server.

Syntax

set tftpftp sip <*IP address*>

- *IP address* - IP address specified in the form xxx.xxx.xxx.xxx.

Default Setting

0.0.0.0

Command Mode

Installer, Admin

Example

```
Installer# set tftpftp sip 192.168.0.0
Installer#
```

5.7.9 set tftpftp start

Commences the FTP or TFTP file transfer process.

Syntax

set tftpftp start <**yes** | **no**>

- **yes** - Commences the file transfer process.
- **no** - Takes no action.

Default Setting

Disabled

Command Mode

Installer, Admin

Example

```
Installer# set tftpftp start yes
Installer#
```

5.7.10 get tftpftp

This command displays detailed TFTP or FTP configuration information.

In addition, instead of listing all display parameters, a specific parameter relative to the configuration may be specified by adding syntax after the command, i.e. get tftpftp ptype.

Syntax

get tftpftp <**detail** | *parameter*>

- **detail** - Use to display all parameters for this command.
- *parameter* - Optional parameter used to narrow the query result (see example below).

Default Setting

None

Command Mode

Installer, Admin

Example 1

```
Installer# get tftpftp detail
Property  Value
--------------------
ptype     tftp
rfile     upgrade.tar
sip       0.0.0.0
ftpuser
ftppass
start     no
Installer#
```

Example 2

```
Installer# get tftpftp ptype
tftp
Installer#
```

5.7.11 get config

This command displays the system configuration that will be employed after the unit is reset.

Syntax

get config

get config <**default** | **startup**| **version**>

- **default** - Displays if the configuration will reset to the default setting after the next reboot.
- **version** - Displays the current configuration version file number.

Default Setting

None

Command Mode

Installer, Admin

Example 1

```
Installer# get config
Property  Value
---------------
default   no
version   1.02
Installer#
```

Example 2

```
Installer# get config default
no
Installer#
```

5.7.12 get interface

This command displays the interface information for all connections.

Syntax

get interface <**all** | **br0** | **lo**>

- **all** - Use to display all parameters for this command.
- **br0** - Displays interface information about the SU-L.
- **lo** - Displays loopback interface information.

Default Setting

None

Command Mode

Installer, Admin

Example 1

```
Installer# get interface all
name  type      status  mac                ip         mask
-------------------------------------------------------------
br0   bridge    up      00:10:E7:02:15:5D  10.0.0.1   255.0.0.0
lo    loopback  up      00:00:00:00:00:00  127.0.0.1  255.0.0.0
Installer#
```

Example 2

```
Installer# get interface lo
Property  Value
--------------------------
type      loopback
status    up
mac       00:00:00:00:00:00
ip        127.0.0.1
mask      255.0.0.0
Installer#
```

5.7.13 get system

This command displays detailed hardware and software information for the system.

Syntax

get system <**detail** | **model** | **bversion** | **version** | **platform**>

- **detail** - Use to display all parameters for this command.
- **model -** The SU-L model number.
- **bversion -** The boot code version number.
- **version -** The software version number.
- **platform -** The design version for integrating software and hardware.
- **When no parameter is specified, the default admin password will be displayed (if it is still in use). If the admin password is to be changed after reboot, this command will not display anything.**

Default Setting

None

Command Mode

Installer, Admin

Example 1

```
Installer# get system detail
Property  Value
------------------
model     SU
bversion  1.00.07
version   1.00.14
platform  ar531x
Installer#
```

Example 2

```
Installer# get system platform
ar531x
Installer#
```

Example 3

```
Installer# get system
private
Installer#
```

5.7.14 get ClientSta

This command allows you to display detailed information about the SU-L.

Syntax

get ClientSta <**detail** | **status-update** | **wireless-essid** | **authentication** | **security-mode** | **data-encryption-option** | **wep-key-input** | **wep-key-type** | **default-key** | **key-1** | **key-2** | **key-3** | **key-4** | **rtsthreshold** | **modulation** | **linkrate** | **bridge-static-ip** | **bridge-mip** | **default-gw** | **regdomain** | **total-channel** | **dfs-radar-status** | **mangVLAN** | **txpowerlevel** | **MirDownlink** | **MirUplink** | **CirDownlink** | **CirUplink** | **CirDelay** | **BurstDuration** | **MinContentionWindow** | **MaxContentionWindow** | **AIFS** | **burstTime** | **HardwareRetries** | **PreferredAuMacAddress** | **distance** | **dhcp** | **dhcpc** | **snmp-rocommunity** | **EthernetLinkType** | **VlanDataID** | **VlanDataPriority** | **VlanPriorityThreshold** | **ToSPrioritizationOption** | **IPToSPrecedenceThreshold** | **DSCPThreshold** | **UdpTcpPortRangesPrioOpt** | **UdpPortPriRtpRtcp** | **TcpPortPriRtpRtcp** | **UdpPortRanges** | **TcpPortRanges** | **IpRangeOption** | **IpRangeAddress** | **IpRangeMask** | **SuName** | **bandwidth** | **dfsOption** | **dfsChannelCheckTime** | **dfsChannelAvoidancePeriod** | **dfsClearRadarDetectedChannels** | **dfsMinimumPulseToDetect** | **dfsDetectionAlgorithm** | **led1Type** | **led1Mode** | **led1Target** | **led2Type** | **led2Mode** | **led2Target** | **led3Type** | **led3Mode** | **led3Target** | **led4Type** | **led4Mode** | **led4Target** | **led5Type** | **led5Mode** | **led5Target** | **led6Type** | **led6Mode** | **led6Target** | **led7Type** | **led7Mode** | **led7Target**>

- **detail** - Use to display all parameters for this command.
- **status-update** - Notifies the user if a system status update has been recorded.
- **wireless-essid** - Displays the service set identifier used to identify wireless traffic.
- **authentication** - Displays the type of authentication used.
- **security-mode** - Displays the encryption algorithm used when the data-encryption-option is activated
- **data-encryption-option** - Notifies the user if data encryption is being used on transmitting data.
- **wep-key-input** - Displays if WEP security is being used.
- **wep-key-type** - Displays the type of WEP security being used, if any.
- **default-key** - Displays the default WEP key.
- **key-1~key-4** - Displays the WEP key value.
- **rtsthreshold** - Displays the set packet size threshold after which an RTS packet must be sent.
- **modulation** - Displays the method at which data is being transferred in relation to the linkrate, fixed or dynamic (limited).
- **linkrate** - Displays the maximum data rate at which the SU-L can transmit data.
- **bridge-static-ip** - Displays the IP address of the SU-L.
- **bridge-mip** - Displays the subnet mask for the Ethernet connection.
- **default-gw** - Displays the default gateway for the Ethernet connection.
- **regdomain** - Displays the chosen regulatory domain. (Only in installer mode)
- **total-channel** - Displays the number of channels of bandwidth enabled within the chosen regulatory domain.
- **dfs-radar-status** - Displays a table indicating the radar detection status for each channel
- **mangVLAN** - Displays the ID of the management VLAN.
- **txpowerlevel** - Displays the transmission power level in relation to maximum capabilities.
- **MirDownlink** - Displays the Maximum Information Rate of the downlink from the AU to the SU

- **MirUplink** - Displays the Maximum Information Rate of the uplink from the SU to the AU
- **CirDownlink** - Displays the Committed Information Rate of the downlink from the AU to the SU
- **CirUplink** - Displays the Committed Information Rate of the uplink from the SU to the AU
- **CirDelay** - Displays the Maximum delay time introduced by the CIR\MIR buffering mechanism
- **BurstDuration** - Displays the maximum duration for the initial burst after a period of inactivity
- **MinContentionWindow** - Displays the initial (lowest) maximal value for the additional timeslots employed by the back-off algorithm
- **MaxContentionWindow** - Displays the final (highest) maximal value for the additional timeslots employed by the back-off algorithm
- **AIFS** - Displays the Arbitration Inter-Frame Spacing number of time slots
- **burstTime** - Displays the time (in ms) in which multiple data frames are sent in succession, without contention in between
- **HardwareRetries** - Displays the maximum number of times that an unacknowledged frame is retransmitted in each Hardware Retrial phase
- **PreferredAuMacAddress** - Displays the preferred AU
- **distance** - Displays the configured distance between the SU-L's antenna and the AP.
- **dhcp** - Displays if DHCP has been enabled.
- **snmp-rocommunity** - Displays the SNMP read-only community access string.
- **EhernetLinkType** - Displays the VLAN link type
- **VlanDataID** - Displays the VLAN ID tag
- **VlanDataPriority** - Displays the Vlan priority tag
- **VlanPriorityThreshold** - Displays the threshold value for the VLAN priority tag over which packets are routed via the High priority queue
- **ToSPrioritizationOption** - Displays the current state of the ToS prioritization
- **IPToSPrecedenceThreshold** - Displays the threshold value for the 3 IP precedence bits over which packets are routed via the High priority queue
- **DSCPThreshold** - Displays the threshold value for the 6 DSCP bits over which packets are routed via the High priority queue
- **UdpTcpPortRangesPrioOpt** - Displays the types of destination ports used as priority classifiers for port range prioritization
- **UdpPortPriRtpRtcp** - Displays prioritization that is applied for VoIP protocols (RTP and RTCP) when UDP port prioritization is used
- **TcpPortPriRtpRtcp** - Displays prioritization that is applied for VoIP protocols (RTP and RTCP) when TCP port prioritization is used
- **IpRangeOption** - Displays the type of IP based prioritization applied
- **IpRangeIpAddress** - Displays the base IP address for the IP range used for prioritization
- **IpRangeMask** - Displays the IP mask for the IP range used for prioritization
- **SuName** - Dispalys the name of the subscriber unit
- **bandwidth** - Displays the channel bandwidth(s) used for the airlink
- **dfsOption** - Displays whether the Dynamic Frequency Selection is enabled
- **dfsChannelCheckTime** - Displays the duration of the channel radar check (in seconds)
- **dfsChannelAvoidancePeriod** - Displays for how long (in minutes) to avoid channels where radar was detected or that are adjacent to radar
- **dfsClearRadarDetectedChannels** - Displays whether frequencies are reset to Radar Free status after the next status-update
- **dfsMinimumPulseToDetect** - The minimum number of pulses that validates a signal as belonging to a radar
- **dfsDetectionAlgorithm** - Displays whether the DFS uses the ETSI or FCC detection algorithm
- **ledMode** - Displays the SNR LEDs' behavior

- **led1Type** ~ **led8Type** - Displays the corresponding SNR LED's threshold parameter
- **led1Mode** ~ **led8Mode** - Displays the corresponding SNR LED's threshold relational operator
- **led1Target** ~ **led8Target** - Displays the corresponding SNR LED's threshold target value

Default Setting

Normal Mode

Command Mode

Installer, Admin

Example 1

```
Installer# get ClientSta detail
Property                        Value
-------------------------------------------------
status-update                   no
wireless-essid                  ESSID1
authentication                  OpenSystem
security-mode                   WEP
data-encryption-option          no
wep-key-input                   NONE WEP
wep-key-type                    NONE WEP
default-key                     1
key-1
key-2
key-3
key-4
rtsthreshold                    60
modulation                      limited
linkrate                        54
bridge-static-ip                10.0.0.1
bridge-mip                      255.0.0.0
default-gw                      0.0.0.0
regdomain                       ETSI
total-channel                   10
dfs-radar-status
mangVLAN                        0
txpowerlevel                    Full
MirDownlink                     12032
MirUplink                       12032
CirDownlink                     0
CirUplink                       0
CirDelay                        5000
BurstDuration                   5
MinContentionWindow             15
MaxContentionWindow             1023
AIFS                            2
burstTime                       10
HardwareRetries                 10
PreferredAuMacAddress           00:00:00:00:00:00
distance                        20
dhcpc                           no
snmp-rocommunity                public
EthernetLinkType                Hybrid
VlanDataID                      1
VlanDataPriority                0
VlanPriorityThreshold           7
ToSPrioritizationOption         Disable
IPToSPrecedenceThreshold        4
DSCPThreshold                   32
UdpTcpPortRangesPrioOpt         Disable
UdpPortPriRtpRtcp               RTPRTCP
TcpPortPriRtpRtcp               RTPRTCP
UdpPortRanges
TcpPortRanges
```

```
IpRangeOption                   Disable
IpRangeIpAddress                0.0.0.0
IpRangeMask                     0.0.0.0
SuName                          3
bandwidth                       10-20
dfsOption                       enabled
dfsChannelAvoidancePeriod       30
dfsClearRadarDetectedChannels   no
dfsMinimumPulseToDetect         4
dfsDetectionAlgorithm           etsi
ledMode                         normal
led1Type                        disabled
led1Mode                        le
led1Target                      0
led2Type                        disabled
led2Mode                        le
led2Target                      0
led3Type                        disabled
led3Mode                        le
led3Target                      0
led4Type                        disabled
led4Mode                        le
led4Target                      0
led5Type                        disabled
led5Mode                        le
led5Target                      0
led6Type                        disabled
led6Mode                        le
led6Target                      0
led7Type                        disabled
led7Mode                        le
led7Target                      0
Installer#
```

Example 2

```
Installer# get ClientSta modulation
limited
Installer#
```

5.8 SNMP Commands

Table 5-6: SNMP Commands

Command	Function	Mode	Page
set ClientSta snmp -rocommunity	Defines the SNMP read-only access string.	Installer, Admin	105

5.8.1 set ClientSta snmp-rocommunity

This command defines the SNMP community access string that has read-only access. Authorized management stations are only able to retrieve MIB objects.

Syntax

set ClientSta snmp-rocommunity <*string*>

- *string* - 1~32 alphanumeric characters.

Default Setting

"public"

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta snmp-rocommunity monkeys
Installer#
```

5.9 Ethernet Interface Commands

The commands described in this section configure connection parameters used for unit management.

Table 5-7: Ethernet Interface Commands

Command	Function	Mode	Page
set ClientSta bridge-mip	Sets the subnet mask for the unit.	Installer, Admin	106
set ClientSta bridge-static-ip	Sets the IP address for the unit.	Installer, Admin	106
set ClientSta default-gw	Sets the default gateway for passing traffic to the unit.	Installer, Admin	107
set ClientSta dhcpc	Enables/disables DHCP on the unit.	Instaler, Admin	107

5.9.1 set ClientSta bridge-mip

This command sets the subnet mask for the interface.

Syntax

set ClientSta bridge-mip <*subnet mask*>

- *subnet mask* - The mask that identifies the host address bits used for routing to specific subnets. Specified as four decimal numbers, 0 to 255, separated by periods

Default Setting

255.0.0.0

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta bridge-mip 255.255.255.0
Installer#
```

5.9.2 set ClientSta bridge-static-ip

This command sets the IP address for the interface.

Syntax

set ClientSta bridge-static-ip <*IP address*>

- *IP address* - The IP address of the unit. Specified as four decimal numbers, 0 to 255, separated by periods

Default Setting

10.0.0.1

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta bridge-static-ip 192.168.1.1
Installer#
```

5.9.3 set ClientSta default-gw

This command sets the IP address of the gateway router between this device and management stations that exist on other network segments.

Syntax

set ClientSta default-gw <*gateway IP address*>

- *gateway IP address* - The IP address of the gateway router. Specified as four decimal numbers, 0 to 255, separated by periods

Default Setting

0.0.0.0

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta default-gw 192.168.0.0
Installer#
```

5.9.4 set ClientSta dhcpc

Enables or disables the DHCP client. If enabled, the unit searches for a DHCP server and acquires its IP parameters from the server. If a DHCP server is not located within approximately 60 seconds, the currently configured parameters are used. Every minute the unit will search for a DHCP server to acquire an IP address. To set a new IP address you must first either enable DHCP, or enter it manually using the “set ClientSta bridge-static-ip” command.

Syntax

set ClientSta dhcpc <**yes** | **no**>

- **yes** - Enables DHCP.
- **no** - Disables DHCP.

Default Setting

Disabled

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta dhcpc yes
Installer#
```

5.10 Wireless Commands

The commands described in this section configure connection parameters for the wireless interfaces.

Table 5-8: Wireless Commands

Command	Function	Mode	Page
set ClientSta authentication	Defines the 802.11 authentication type allowed by the SU.	Installer, Admin	110
set ClientSta security-mode	Switches between WEP and AES-CCM	Installer, Admin	110
set ClientSta data-encryption-option	Enables/disables data encryption.	Installer, Admin	111
set ClientSta default-key	Sets the key number for transmission.	Installer, Admin	111
set ClientSta distance	Sets the estimated distance between the farthest SU in the cell and the serving AU.	Installer, Admin	112
set ClientSta key-1~4	Allows the user to set up to 4 152-bit hexadecimal keys.	Installer, Admin	112
set ClientSta linkrate	Sets the maximum data rate for transmission of wireless packets.	Installer, Admin	113
set ClientSta mangVLAN	Sets the management VLAN ID.	Installer, Admin	113
set ClientSta modulation	Sets a fixed or dynamic data transmission rate.	Installer, Admin	114
set ClientSta rtsthreshold	Sets the packet size threshold at which an RTS must be sent to the receiving station prior to the sending station starting communications.	Installer, Admin	114
set ClientSta txpowerlevel	Adjusts the power of the radio signals from the SU.	Installer, Admin	115
set ClientSta wireless-essid	Allows the user to specify an ESSID for the SU.	Installer, Admin	116
set ClientSta HardwareRetries	Sets the maximum number of times that an unacknowledged frame is retransmitted in each Hardware Retrial pahse	Installer, Admin	116
set ClientSta PreferredAuMacAddress	Sets the preferred AU	Installer, Admin	116
set ClientSta bandwidth	Sets the channel bandwidth(s) enabled for the unit	Installer, Admin	117

Table 5-8: Wireless Commands

Command	Function	Mode	Page
get BSSList	Shows the wireless APs available in the neighborhood.	Installer; Admin	117
set CStatus clear-cnt yes	Sets all Rx/Tx display statistics to a null value.	Installer, Admin	118
get CStatus	Shows the status for the wireless interface.	Installer, Admin	118

5.10.1 set ClientSta authentication

This command defines the 802.11 authentication type allowed by the SU-L.

Syntax

set ClientSta authentication <OpenSystem | SharedKey>

- **OpenSystem** - Can associate to an AU without verifying its identity using a shared key. “Open” authentication means either there is no encryption (if encryption is disabled) or WEP-only encryption is used (if encryption is enabled).
- **SharedKey** - Authentication is based on a shared key that has been distributed to all stations.

Default Setting

OpenSystem

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta authentication SharedKey
Installer#
```

5.10.2 set ClientSta security-mode

This command defines the encryption algorithm employed when enabling the data-encryption-option. You can choose either Advanced Encryption Standard in Counter with CBC-MAC mode (AES-CCM) or Wired Equivalent Privacy (WEP).

Syntax

set ClientSta security-mode <AES-CCM | WEP>

- **AES-CCM** - Selects the Advanced Encryption Standard in Counter with CBC-MAC mode standard
- **WEP** - Selects.Wired Equivalent Privacy standard

Default Setting

WEP

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta security-mode AES-CCM
Installer#
```

5.10.3 set ClientSta data-encryption-option

This command enables or disables the SU-L to use data encryption (WEP). If this option is selected when using static WEP keys, you must configure at least one key on the SU-L.

Syntax

set ClientSta data-encryption-option <**yes** | **no**>

- **yes** - Enables data encryption.
- **no** - Disables data encryption.

Default Setting

Disabled

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta data-encryption-option yes
Installer#
```

5.10.4 set ClientSta default-key

This command selects the key number to use for encryption. The key indicated by the default key selection must be configured with the same value in the AP and in the SU-L in order for the link to work.

Syntax

set ClientSta default-key <**1** | **2** | **3** | **4**>

- The key may be a number between 1 and 4.

Default Setting

1

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta default-key 2
Installer#
```

5.10.5 set ClientSta distance

This command allows the user to configure the estimated distance between the AP and the farthest SU-L in the cell.

Syntax

set ClientSta distance <*distance*>

- *distance* - The distance between antennas in the range 1~50 km.

Default Setting

1 km

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta distance 25
Installer#
```

5.10.6 set ClientSta key

This command defines hexadecimal WEP encryption keys on the SU-L. Up to four keys may be entered.

Syntax

set ClientSta <**key-1** | **key-2** | **key-3** | **key-4**> <*hex*>

- **key-1 ~ key-4** - Selects the key number to use for encryption.
- *hex* - Enter keys as "0x" followed by 32 hexadecimal digits (0-9 and A-F) for 152 bit keys.

Default Setting

Null

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta key-1  0x12345678901234567890123456789012
Installer#
```

5.10.7 set ClientSta linkrate

This command sets the maximum data rate at which the SU-L transmits unicast packets on the wireless interface. The maximum transmission distance is affected by the data rate. The lower the data rate, the longer the transmission distance.

Syntax

set ClientSta linkrate <*linkrate*>

- *linkrate* - May be set to 6, 9, 12, 18, 24, 36, 48 or 54 Mbps.

Default Setting

54 Mbps

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta linkrate 6
Installer#
```

5.10.8 set ClientSta mangVLAN

This command configures the management VLAN ID. The management VLAN is for managing the SU-L. The data traffic is bridged transparently regardless of this setting.

Syntax

set ClientSta mangVLAN <*VLAN ID*>

- *VLAN ID* - Range 0, or 1~4094. 0 implies that the management VLAN is disabled.

Default Setting

Disabled

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta mangVLAN 4094
Installer#
```

5.10.9 set ClientSta modulation

This command allows you to set fixed or dynamic (limited) transmission rate. If the modulation is set to fixed, the data transmission rate will be set by the link rate. However if the modulation is set to dynamic, the transmission rate may be less than or equal to, but not greater than the link rate.

Syntax

set ClientSta modulation <**fixed** | **limited**>

- **fixed** - Data transmission will be set by the linkrate.
- **limited** - Modulation will be dynamic according to requirements, i.e. if the linkrate is set to 24 Mbps, and the modulation is set to limited, then the data transmission rate could be 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, or 24 Mbps.

Default Setting

Limited

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta modulation fixed
Installer#
```

5.10.10 set ClientSta rtsthreshold

This command sets the packet size threshold at which a Request to Send (RTS) signal must be sent to the receiving station prior to the sending station starting communications.

Syntax

set ClientSta rtsthreshold <*threshold*>

- *threshold* - Threshold packet size for which to send an RTS. (Range: 20-2347 bytes)

Default Setting

60

Command Mode

Installer, Admin

Command Usage

If the threshold is set to 20, the SU-L always sends RTS signals. If set to 2347, the SU-L never sends RTS signals. If set to any other value, and the packet size equals or exceeds the RTS threshold, the RTS/CTS (Request to Send / Clear to Send) mechanism will be enabled.

The SU-L sends RTS frames to a receiving station to negotiate the sending of a data frame. After receiving an RTS frame, the station sends a CTS frame to notify the SU-L that it can start sending data.

SU-A-EZs contending for the wireless medium may not be aware of each other.

Example

```
Installer# set ClientSta rtsthreshold 20
Installer#
```

5.10.11 set ClientSta txpowerlevel

This command adjusts the power of the radio signals transmitted from the SU-L. The higher the transmission power, the farther the transmission range. Power selection is not just a trade off between coverage area and maximum supported clients. You also have to ensure that high-power signals do not interfere with the operation of other radio devices in the service area. The “full” transmission power level corresponds to the maximum power level allowed for the currently used regdomain setting.

Syntax

set ClientSta txpowerlevel <**Full** | **Half** | **Quarter** | **Eighth** | **Min**>

- **Full** - 100% of maximum transmission power level.
- **Half** - 50% of maximum transmission power level.
- **Quarter** - 25% of maximum transmission power level.
- **Eighth** - 12.5% of maximum transmission power level.
- **Min** - Minimum transmission power level (0 dBm).

Default Setting

Full

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta txpowerlevel Min
Installer#
```

5.10.12 set ClientSta wireless-essid

This command allows the user to set the name of the wireless network.

Syntax

set ClientSta wireless-essid <*ESSID string*>

- *ESSID string* - 1~31 alphanumeric characters.

Default Setting

ESSID1

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta wireless-essid essid123
Installer#
```

5.10.13 set ClientSta HardwareRetries

This command sets the maximum number of times that an unacknowledged frame is retransmitted in each Hardware Retrial phase. When the Adaptive Modulation Algorithm is disabled, a frame will be dropped when the number of unsuccessful retransmissions reaches this value.

Syntax

set ClientSta HardwareRetries <*no. of retries*>

- *no. of retries* - No. of hardware retries (Range: 1-14).

Default Setting

10

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta HardwareRetries 3
Installer#
```

5.10.14 set ClientSta PreferredAuMacAddress

This command sets the MAC address for a specific AU the SU-L will attempt to connect to when it starts. Setting this value to 00:00:00:00:00:00 disables the feature and sets the SU to choose its AU on the Best AU selection process.

Syntax

set ClientSta PreferredAuMacAddress <*AU MAC address*>

- *AU MAC address* - MAC address for the preferred AU (Format: xx:xx:xx:xx:xx:xx).

Default Setting

00:00:00:00:00:00

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta PreferredAuMacAddress 24:13:96:74:88:50
Installer#
```

5.10.15 set ClientSta bandwidth

This command sets the channel banwidth(s) that the unit may use to associate to an AU.

Syntax

set ClientSta bandwidth <**10** | **20** | **10-20** >

- **10** - The unit can use 10 MHz channels.
- **20** - The unit can use 20 MHz channels.
- **10-20** - The unit can use either 10 or 20 MHz channels.

Default Setting

10-20

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta bandwidth 10
Installer#
```

5.10.16 get BSSList

This command shows all 802.11a wireless devices that act as AP's (transmit beacons) within the proximity of the SU-L.

Syntax

get BSSList

get BSSList <**essid** | **apmac** | **channel** | **freq** | **rssi** >

- **essid** - The service set identifier that is attached to packets sent from neighboring devices.
- **apmac** - The physical layer address used to uniquely identify the APs.
- **channel** - The radio channel through which neighboring devices communicate with the SU-L.
- **freq** - The frequency on which neighboring devices are transmitting (this applies only for 20MHz bandwidth OFDM signals.)
- **rssi** - A measure of the signal strength received from neighboring devices.

Default Setting

None

Command Mode

Installer, Admin

Example 1

```
Installer# get BSSList
essid    apmac              channel  freq  rssi
-----------------------------------------------
linkutil  00:10:e7:c4:00:ab  148      5740  -73
linkutil  00:10:e7:e4:0c:6b  166      5830  -58
Installer#
```

Example 2

```
Installer# get BSSList apmac
apmac     00:10:e7:24:0d:9a
Installer#
```

5.10.17 set CStatus clear-cnt yes

This command sets all Rx/Tx statistics to a null value.

Syntax

set CStatus clear-cnt yes

Default Setting

None

Command Mode

Installer, Admin

Example

```
Installer# set CStatus clear-cnt yes
Installer#
```

5.10.18 get CStatus

This command displays the status of the wireless interface, as well as some Ethernet statistics.

Syntax

get CStatus

get CStatus <essid | apmac | channel | freq | linkquality | rssi | noisefloor | txpower | linkstatus | rxpkt-wlan | rxbyte-wlan | txpkt-wlan | txbyte-wlan | rxpkt-eth | rxbyte-eth | txpkt-eth | txbyte-eth | mir_up | mir_down | cir_up | cir_down | bandwidth>

- **essid** - The service set identifier that is attached to packets sent from the SU-L.
- **apmac** - The physical layer address used to uniquely identify the AP.
- **channel** - The radio channel through which the SU-L communicates with the AP.

- **freq** - The portion of the 802.11a frequency band the SU-L is using.
- **linkquality** - A measurement of the quality of the signal received by the SU-L.
- **rssi** - A measure of the received signal strength indicator for the AP.
- **noisefloor** - A level of interference below which signals to and from the SU-L cannot be detected.
- **txpower** - A measure of the transmission signal power.
- **linkstatus** - A measure of activity on the link between the SU-L and associated AP.
- **rxpkt-wlan** - A measurement of the number of wireless packets received by the SU-L.
- **rxbyte-wlan** - A measurement of the number of wireless bytes received by the SU-L.
- **txpkt-wlan** - A measurement of the number of wireless packets transmitted by the SU-L.
- **txbyte-wlan** - A measurement of the number of wireless bytes transmitted by the SU-L.
- **rxpkt-eth** - A measurement of the number of packets received by the SU-L over the Ethernet port.
- **rxbyte-eth** - A measurement of the number of bytes received by the SU-L over the Ethernet port.
- **txpkt-eth** - A measurement of the number of packets transmitted by the SU-L over the Ethernet port.
- **txbyte-eth** - A measurement of the number of bytes transmitted by the SU-L over the Ethernet port.
- **mir_up** - A measurement of the uplink MIR
- **mir_down** - A measurement of the downlink MIR
- **cir_up** - A measurement of the uplink CIR
- **cir_down** - A measurement of the downlink CIR
- **bandwidth** - A measurement of the channel bandwidth(s) employed
- **crc_percentage_wlan** - A measurement of the percentage of frames sent over the air that contained CRC errors
- **crc_count_wlan** - A measurement of the number of frames sent over the air that contained CRC errors

Default Setting

None

Command Mode

Installer, Admin

Example 1

```
Installer# get CStatus
Property     Value
------------------------------
essid                ESSID1
apmac                00:00:00:00:00:00
channel              108
freq                 5540
linkquality          0
rssi                 -256
noisefloor           -256
txpower               Full
linkstatus            0
rxpkt-wlan            0
rxbyte-wlan           0
txpkt-wlan            0
txbyte-wlan           0
rxpkt-eth             1041
rxbyte-eth            105870
txpkt-eth             734
txbyte-eth            209723
mir_up                12032
cir_up                12032
bandwidth             10-20
crc_count_wlan        0
crc_percentage_wlan   0
iface                 wlan0
Installer#
```

Example 2

```
Installer# get CStatus noisefloor
-96
Installer#
```

5.11 VLAN Commands

The commands described in this section configure networking parameters for VLAN communications.

Table 5-9: VLAN Commands

Command	Function	Mode	Page
set ClientSta EthernetLinkType	Chooses between Access and Hybrid VLAN link types	Installer, Admin	121
set ClientSta VlanDataID	Sets the VLAN ID tag	Installer, Admin	121
set ClientSta VlanDataPriority	Sets the VLAN priority tag	Installer, Admin	122

5.11.1 set ClientSta EthernetLinkType

This command sets the VLAN link type:

Syntax

set ClientSta EthernetLinkType <**Hybrid** | **Access**>

- **Access** - Link type for networks with VLAN unaware devices which enables the frame filtering and VLAN tagging/untagging at the SU level
- **Hybrid** - Determines the SU to behave as a VLAN transparent unit

Default Setting

Hybrid

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta EthernetLinkType Access
Installer#
```

5.11.2 set ClientSta VlanDataID

This command sets the VLAN ID tag used by the SU when working in Access Mode

Syntax

set ClientSta VlanDataID <*VLAN ID*>

- *VLAN ID* - Common ID for all the devices that are part of the same VLAN (Range: 1-4049).

Default Setting

1

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta VlanDataID 14
Installer#
```

5.11.3 set ClientSta VlanDataPriority

This command sets the VLAN priority tag used by the SU when working in Access Mode

Syntax

set ClientSta VlanDataPriority <*priority*>

- *priority* - Sets the priority of the uplink frames relative to the other frames transferred inside the VLAN. Lower values indicate higher priorities (Range: 0-7).

Default Setting

0

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta VlanDataPriority 3
Installer#
```

5.12 Contention Commands

The commands described in this section configure parameters that handle the SU's concurrent frame transmissions inside the wireless cell.

Table 5-10: Contention Commands

Command	Function	Mode	Page
set ClientSta AIFS	Defines the Arbitration Inter-Frame Spacing number of time slots	Installer, Admin	123
set ClientSta burstTime	Defines the burst size emplyed when burst mode is enabled.	Installer, Admin	123
set ClientSta MinContentionWindow	Sets the initial (lowest) maximal value for the additional timeslots employed by the back-off algorithm	Installer, Admin	124
set ClientSta MaxContentionWindow	Sets the final (highest) maximal value for the additional timeslots employed by the back-off algorithm	Installer, Admin	124

5.12.1 set ClientSta AIFS

This command sets the Arbitration Inter-Frame Spacing which is the difference in number of time slots between the DIFS and SIFS.

Syntax

set ClientSta AIFS <*no. of timeslots*>

- *no. of timeslots* - The number of timeslots additional to the SIFS that determine the DIFS (Range: 1-50)

Default Setting

2

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta AIFS 3
Installer#
```

5.12.2 set ClientSta burstTime

This command sets the duration (in milliseconds) of a burst interval. During this time, inter-frame spacing between consecutive frames does not include contention time intervals. The burst time can not exceed the Maximum Burst Duration set for the sub-band.

Syntax

set ClientSta burstTime <*time interval*>

- *time interval* - The duration of a burst in milliseconds. (Range: 1-Maximum Burst Duration defined for the sub-band)

Default Setting

5 or Maximum Burst Duration (the lower of the two)

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta burstTime 10
Installer#
```

5.12.3 set ClientSta MinContentionWindow

This command sets the initial (lowest) maximal value for the additional timeslots employed by the back-off algorithm.

Syntax

set ClientSta MinContentionWindow <*no. of timeslots*>

- *no. of timeslots* - The initial (lowest) maximal value for the number of timeslots additional to the DIFS employed by the back-off algorithm (Range: 7, 15, 31, 63, 127, 255, 511, 1023)

Default Setting

15

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta MinContentionWindow 31
Installer#
```

5.12.4 set ClientSta MaxContentionWindow

This command sets the final (highest) maximal value for the additional timeslots employed by the back-off algorithm.

Syntax

set ClientSta MinContentionWindow <*no. of timeslots*>

- *no. of timeslots* - The final (highest) maximal value for the number of timeslots additional to the DIFS employed by the back-off algorithm (Range: 7, 15, 31, 63, 127, 255, 511, 1023)

Default Setting

1023

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta MaxContentionWindow 255
Installer#
```

5.13 MIR/CIR Commands

The commands described in this section configure parameters that handle the SU's throughput settings.

Table 5-11: MIR/CIR Commands

Command	Function	Mode	Page
set ClientSta MirDownlink	Sets the Maximum Information Rate of the downlink from the AU to the SU	Installer, Admin	126
set ClientSta MirUplink	Sets the Maximum Information Rate of the uplink from the SU to the AU	Installer, Admin	126
set ClientSta CirDownlink	Sets the Committed Information Rate of the downlink from the AU to the SU	Installer, Admin	127
set ClientSta CirUplink	Sets the Committed Information Rate of the uplink from the SU to the AU	Installer, Admin	127
set ClientSta BurstDuration	Sets the maximum duration for the initial uninterrupted burst of data sent after a period of inactivity	Installer, Admin	128

5.13.1 set ClientSta MirDownlink

This command sets the Maximum Information Rate of the downlink from the AU to the SU.

Syntax

set ClientSta MirDownlink <*MIR downlink*>

- *MIR downlink* - The MIR in Kbps of the downlink from the AU to the SU. (Range: multiples of 128 up to 12032)

Default Setting

Maximum downlink rate supported by the unit's license.

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta MirDownlink 1920
Installer#
```

5.13.2 set ClientSta MirUplink

This command sets the Maximum Information Rate of the uplink from the SU to the AU

Syntax

set ClientSta MirDownlink <*MIR uplink*>

- *MIR uplink* - The MIR in Kbps of the uplink from the SU to the AU. (Range: multiples of 128 up to 12032)

Default Setting

Maximum uplink rate supported by the unit's license.

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta MirUplink 2560
Installer#
```

5.13.3 set ClientSta CirDownlink

This command sets the Committed Information Rate of the downlink from the AU to the SU

Syntax

set ClientSta CirDownlink <*CIR downlink*>

- *CIR downlink* - The CIR in Kbps of the downlink from the AU to the SU. (Range: multiples of 128 up to 12032)

Default Setting

0

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta CirDownlink 2176
Installer#
```

5.13.4 set ClientSta CirUplink

This command sets the Committed Information Rate of the uplink from the SU to the AU

Syntax

set ClientSta CirDownlink <*CIR uplink*>

- *CIR uplink* - The CIR in Kbps of the uplink from the SU to the AU. (Range: multiples of 128 up to 12032)

Default Setting

0

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta CirUplink 1280
Installer#
```

5.13.5 set ClientSta BurstDuration

This command sets the maximum duration for the initial uninterrupted burst after a period of inactivity

Syntax

set ClientSta BurstDuration <*burst duration*>

- *burst duration* - The duration in ms of the initial uninterrupted burst of data sent after a period of inactivity. (Range: 0-2000)

Default Setting

5

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta BurstDuration 25
Installer#
```

5.14 DFS Commands

Starting with software version 2.1, subscriber units have the ability to scan the air and detect radar signals. The commands described in this section configure the Dynamic Frequency Selection parameters for the SU.

Table 5-12: DFS Commands

Command	Function	Mode	Page
set ClientSta dfsOption	Enables or disables DFS	Installer, Admin	129
set ClientSta dfsChannelCheckTime	Sets the duration of the radar check for a channel	Installer, Admin	130
set ClientSta dfsChannelAvoidancePeriod	Set the persistence of the Radar Detected or Adjacent to Radar status for a the corresponding frequencies	Installer, Admin	130
set ClientSta dfsClearRadarDetectedChannels	Sets weather all frequencies are set as Radar Free after the next status update	Installer, Admin	130
set ClientSta dfsMinimumPulseToDetect	Sets the minimum number of pulses that identify a signal as generated by radar	Installer, Admin	131
set ClientSta dfsDetectionAlgorithm	Selects between the ETSI and FCC based radar detection mechanisms	Installer, Admin	131

5.14.1 set ClientSta dfsOption

This command enables or disables the DFS function on the SU.

Syntax

set ClientSta dfsOption <enabled | disabled>

- **enabled** - Enables the DFS functionality
- **disabled** - Disabled the DFS functionality

Default Setting

enabled

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta dfsOption disabled
Installer#
```

5.14.2 set ClientSta dfsChannelCheckTime

This command sets the number of minutes the unit will check a frequency for radar signals in order to validate it as either a Radar Free or Radar Detected.

Syntax

set ClientSta dfsChannelCheckTime <*no. of minutes*>

- *no. of minutes* - The number of minutes the unit will check the channel. (Range: 1-60)

Default Setting

60

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta dfsChannelCheckTime 25
Installer#
```

5.14.3 set ClientSta dfsChannelAvoidancePeriod

This command sets the number of minutes the channel will be unavailable for usage after radar signals are detected on it or on an adjacent channel.

Syntax

set ClientSta dfsChannelAvoidancePeriod <*no. of minutes*>

- *no. of minutes* - The number of minutes to keep the frequency tagged as Radar Detected or Adjacent to Radar. (Range: 1-60)

Default Setting

30

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta dfsChannelAvoidancePeriod 12
Installer#
```

5.14.4 set ClientSta dfsClearRadarDetectedChannels

This command sets whether after a status update command, the unit tags all frequencies as Radar Free or reverts them to their previous status.

Syntax

set ClientSta dfsClearRadarDetectedChannels <**yes** | **no**>

- **yes** - Sets all frequencies to Radar Free after the next status update

- **no** - All frequencies keep their current status after the next status update

Default Setting

no

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta dfsClearRadarDetectedChannels yes
Installer#
```

5.14.5 set ClientSta dfsMinimumPulseToDetect

This command sets the number of consecutive pulses that need to be detected by the DFS mechanism for the signal to be considered as radar originated.

Syntax

set ClientSta dfsMinimumPulseToDetect <*no. of pulses*>

- *no. of pulses* - The minimum number of pulses that make up the radar signal. (Range: 1 - 100)

Default Setting

4

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta dfsMinimumPulseToDetect 6
Installer#
```

5.14.6 set ClientSta dfsDetectionAlgorithm

This command defines the type of radar detection algorithm employed by the DFS mechanism

Syntax

set ClientSta dfsDetectionAlgorithm <**etsi** | **fcc**>

- **etsi** - Sets a detection algorithm based on the ETSI standards
- **fcc** - Sets a detection algorithm based on the FCC standards

Default Setting

etsi

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta dfsDetectionAlgorithm fcc
Installer#
```

5.15 Traffic Prioritization Commands

These commands configure the traffic prioritization options for the SU. Frames can be routed via the High Priority queue or the Low Priority queue based on various classifiers: VLAN priority, ToS priority, UDP/TCP port ranges or IP address. When multiple classifiers are enabled, the frame will be routed through the High priority queue if it meets the conditions set by at least one classifier.

Table 5-13: Traffic Prioritization Commands

Command	Function	Mode	Page
set ClientSta VlanPriorityThreshold	Sets frame prioritization based on the VLAN priority tag inside the frame	Installer, Admin	133
set ClientSta ToSPrioritizationOption	Sets the type of ToS prioritization applied	Installer, Admin	134
set ClientSta IPToSPrecedenceThreshold	Sets the threshold value used when the IP precedence mechanim is enabled	Installer, Admin	134
set ClientSta DSCPThreshold	Sets the threshold value used when the DSCP precedence mechanim is enabled	Installer, Admin	135
set ClientSta UdpTcpPortRangesPrioOpt	Sets the UDP/TCP implementation of the destination port range based prioritization	Installer, Admin	135
set ClientSta UdpPortPriRtpRtcp	Sets the RTP/RTCP implementation of the UDP destination port range based prioritization	Installer, Admin	136
set ClientSta TcpPortPriRtpRtcp	Sets the RTP/RTCP implementation of the TCP destination port range based prioritization	Installer, Admin	136
set ClientSta UdpPortRanges	Sets the destination UDP port ranges used for traffic prioritization	Installer, Admin	137
set ClientSta TcpPortRanges	Sets the destination TCP port ranges used for traffic prioritization	Installer, Admin	137
set ClientSta IpRangeOption	Sets source/destination IP address range traffic prioritization	Installer, Admin	138
set ClientSta IpRangeIpAddress	Sets the base IP address for the IP range used for traffic prioritization	Installer, Admin	138
set ClientSta IpRangeMask	Sets the subnet mask for the IP range used for traffic prioritization	Installer, Admin	138

5.15.1 set ClientSta VlanPriorityThreshold

This command sets a threshold for the VLAN priority tag above which frames are routed via the High Priority queue. Frames with VLAN priority tags lower than or

equal to this threshold will be routed through the Low Priority queue. VLAN prioritization is available only for Hybrid links.

Syntax

set ClientSta VlanPriorityThreshold <*threshold value*>

threshold value - When the frame contains a VLAN priority tags higher than this value, it will be routed through the High Priority queue. (Range: 0-7)

Default Setting

7 (All packets go through the Low Priority Queue. VLAN prioritization disabled)

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta VlanPriorityThreshold 4
Installer#
```

5.15.2 set ClientSta ToSPrioritizationOption

This command allows setting a ToS prioritization based on IP precedence or DSCP (Differentiated Services Code Point).

Syntax

set ClientSta ToSPrioritizationOption <**Disable** | **IP** | **DSCP**>

- **Disable** - Disables ToS prioritization.
- **IP** - Enables IP precedence based prioritization (RFC 791).
- **DSCP** - Enables DSCP based prioritization (RFC 2474).

Default Setting

Disable

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta ToSPrioritizationOption DSCP
Installer#
```

5.15.3 set ClientSta IPToSPrecedenceThreshold

This command sets a threshold value for the 3 IP precedence bits inside the IP header above which frames are routed via the High Priority queue. Frames with IP precedence values lower than or equal to this threshold will be routed through the Low Priority queue.

Syntax

set ClientSta IPToSPrecedenceThreshold <*threshold value*>

threshold value - When the frame contains an IP precedence tag higher than this value, it will be routed through the High Priority queue. (Range: 0-7)

Default Setting

4

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta IPToSPrecedenceThreshold 5
Installer#
```

5.15.4 set ClientSta DSCPThreshold

This command sets a threshold value for the 6 DSCP bits inside the IP header above which frames are routed via the High Priority queue. Frames with DSCP values lower than or equal to this threshold will be routed through the Low Priority queue.

Syntax

set ClientSta DSCPThreshold <*threshold value*>

threshold value - When the frame contains a DSCP tag higher than this value, it will be routed through the High Priority queue. (Range: 0-36)

Default Setting

32

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta DSCPThreshold 20
Installer#
```

5.15.5 set ClientSta UdpTcpPortRangesPrioOpt

This command configures the UDP/TCP port ranges based prioritization.

Syntax

set ClientSta UdpTcpPortRangesPrioOpt <**Disable** | **UDP** | **TCP** | **UDPTCP**>

- **Disable** - Disables port range prioritization.
- **UDP** - Enables port range prioritization only for UDP.
- **TCP** - Enables port range prioritization only for TCP.
- **UDPTCP** - Enables port range prioritization for both UDP and TCP.

Default Setting

Disable

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta UdpTcpPortRangesPrioOpt UDPTCP
Installer#
```

5.15.6 set ClientSta UdpPortPriRtpRtcp

This command configures whether UDP port range prioritization differentiates between RTP (odd ports) and RTCP (even ports) traffic.

Syntax

set ClientSta UdpPortPrioRtpRtcp <RTPRTCP | RTP>

- **RTPRTCP** - Enables UDP port range prioritization for both RTP and RTCP ports.
- **RTP** - Enables UDP port range prioritization only for RTP ports.

Default Setting

RTPRTCP

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta UdpPortPriRtpRtcp RTP
Installer#
```

5.15.7 set ClientSta TcpPortPriRtpRtcp

This command configures whether TCP port range prioritization differentiates between RTP (odd ports) and RTCP (even ports) traffic.

Syntax

set ClientSta TcpPortPrioRtpRtcp <RTPRTCP | RTP>

- **RTPRTCP** - Enables TCP port range prioritization for both RTP and RTCP ports.
- **RTP** - Enables TCP port range prioritization only for RTP ports.

Default Setting

RTPRTCP

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta TcpPortPriRtpRtcp RTP
Installer#
```

5.15.8 set ClientSta UdpPortRanges

This command defines the UDP port ranges used for prioritization. If a frame's destination UDP port matches this setting, it will be routed via the High Priority queue. Otherwise, it will be routed through the Low Priority queue.

Syntax

set ClientSta UdpPortRanges <*port ranges*>

port ranges - A list of up to 64 UDP priority port numbers or port ranges. Entries are separated by commas. In ranges, a hyphen is used to separate the start port number from the end port number. Setting an empty port range string will remove all currently enabled ranges.

Default Setting

empty

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta UdpPortRanges 8900,9000-9005,9010,9016-9017
Installer#
```

5.15.9 set ClientSta TcpPortRanges

This command defines the TCP port ranges used for prioritization. If a frame's destination TCP port matches this setting, it will be routed via the High Priority queue. Otherwise, it will be routed through the Low Priority queue.

Syntax

set ClientSta TcpPortRanges <*port ranges*>

port ranges - A list of up to 64 TCP priority port numbers or port ranges. Entries are separated by commas. In ranges, a hyphen is used to separate the start port number from the end port number. Setting an empty port range string will remove all currently enabled ranges.

Default Setting

empty

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta TcpPortRanges 8900,9000-9005,9010,9016-9017
Installer#
```

5.15.10 set ClientSta IpRangeOption

This command configures prioritization based on the source/destination IP address. If the frame's source/destination IP address belongs to a predefined IP address range, the frame will be routed via the High Priority queue. Otherwise, it will be routed through the Low Priority queue.

Syntax

set ClientSta IpRangeOption <**Disable** | **SrcIP** | **DstIP** | **SrcOrDstIP**>

- **Disable** - Disables IP range prioritization.
- **SrcIP** - Enables IP range prioritization for the source IP address.
- **DstIP** - Enables IP range prioritization for the destination IP address.
- **SrcOrDstIP** - Enables IP range prioritization for both the source and destination IP addresses.

Default Setting

Disable

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta IpRangeOption SrcOrDstIp
Installer#
```

5.15.11 set ClientSta IpRangeIpAddress

This command configures the base IP address for the IP range based prioritization.

Syntax

set ClientSta IpRangeIpAddress <*IP address*>

IP address - The base IP address which, along with the IP mask, determines the IP range used for prioritization. (Range: 4 groups of up to 3 digits separated by dots)

Default Setting

0.0.0.0

Command Mode

Installer, Admin

Example

```
Installer# set ClientSta IpRangeIpAddress 172.16.0.0
Installer#
```

5.15.12 set ClientSta IpRangeMask

This command configures the IP mask for the IP range based prioritization.

Syntax

set ClientSta IpRangeMask <*IP mask*>

IP mask - The IP mask which, along with the base IP address, determines the IP range used for prioritization. (Range: 4 groups of up to 3 digits separated by dots)

Default Setting

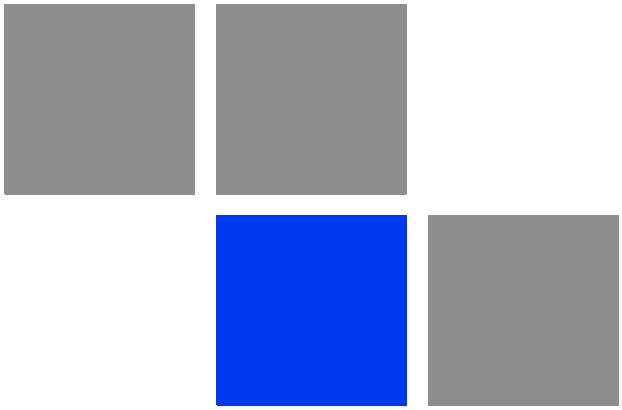
255.0.0.0

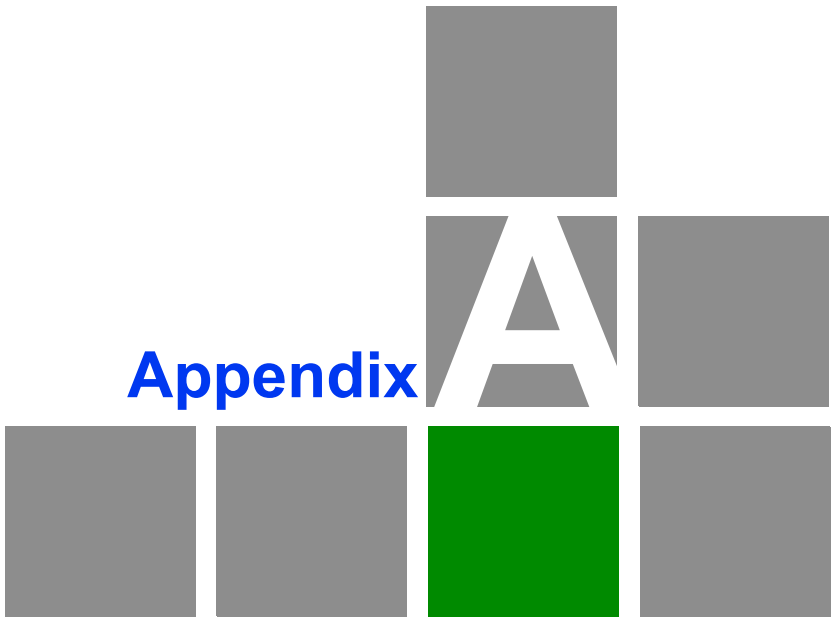
Command Mode

Installer, Admin

Example

```
Installer# set ClientSta IpRangeMask 255.255.0.0
Installer#
```





Appendix A

Troubleshooting

In This Appendix:

This appendix provides a lists of things to check in case of problems before contacting local Technical Support.

Check the following before you contact local Technical Support.

1. If the unit cannot access the network, check the following:
   - Be sure the SU-L is configured with the correct Extended Service Set ID (ESSID) for the network to which it is trying to connect.
   - If authentication or encryption are enabled, ensure that the SU-L is properly configured with the appropriate authentication or encryption keys.
2. If the SU-L cannot be configured using the Telnet, a web browser, or SNMP software:
   - Be sure that the SU-L has been configured with a valid IP address, subnet mask and default gateway.
   - If VLANs are enabled on the wired network, the VLAN tag on the SU-L should be set to the same tag as the management VLAN (default: no tag).
   - Check that you have a valid network connection to the SU-L.
   - If you are connecting to the SU-L through the wired Ethernet interface, check the network cabling between the management station and the SU-L. If you are connecting to SU-L from the wireless interface, ensure that you have a valid connection to the SU-L.
   - If you cannot connect using Telnet, you may have exceeded the maximum number of concurrent Telnet sessions permitted (i.e, four sessions). Try connecting again at a later time, or reboot the unit.
3. If you forgot or lost the password:
   - Use the "restore factory defaults" or "restore password" mechanism, then set the SU-L to its default configuration by powering off the device and rebooting. Then use the default user name and password for the mode you wish to access, admin or installer.
   - Otherwise, contact technical support.
4. If all other recovery measures fail, and the SU-L is still not functioning properly, reset the SU-L's hardware using the web interface, command line, or through a power reset.

Appendix B

Using the Set Factory Defaults Utility

In This Appendix:

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.

NOTE



In order to use the application on SU-L, WinPcap needs to be installed on the host PC.

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 available via both the Ethernet and Wireless ports.

To set factory defaults:

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

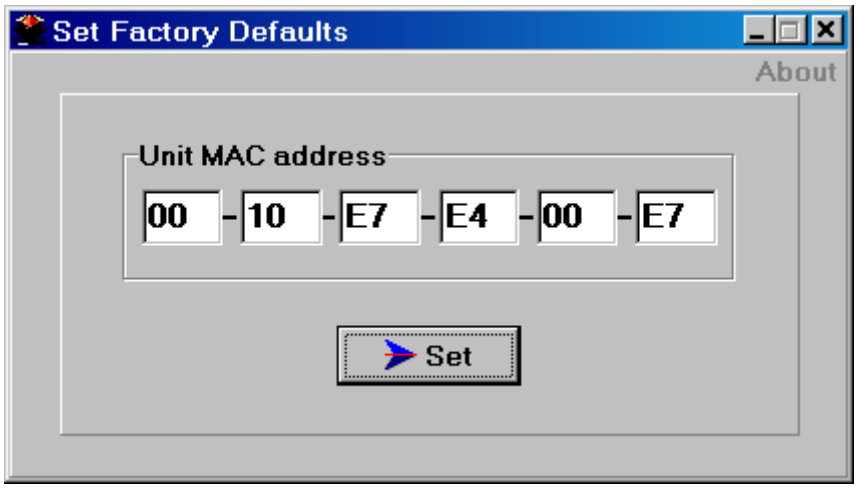
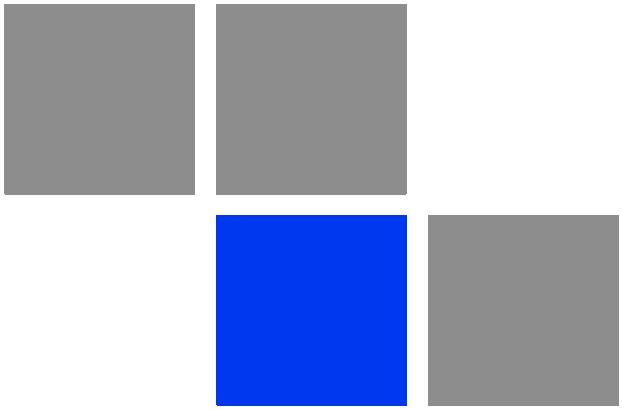


Figure B-1: The Set Factory Defaults Utility

2 Enter the unit's MAC address.

3 Click on the **Set** button.

This utility performs the same operation as **Restore Factory Default Configuration** from Web management or **set config default** Telnet command, restoring the default factory configuration of all parameters.





Glossary

100BASE-TX	IEEE 802.3u specification for 100 Mbps Fast Ethernet over two pairs of Category 5 or better UTP cable.
10BASE-T	IEEE 802.3 specification for 10 Mbps Ethernet over two pairs of Category 3 or better UTP cable
AES-CCM	Deployment of the Advanced Encryption Standard block cipher which uses the Counter with CBC-MAC authenticate-and encrypt mode
AIFS	Arbitration Inter-Frame Spacing: Additional number of timeslots added to the SIFS in order to determine the DIFS
Authentication	The process to verify the identity of a client requesting network access. IEEE 802.11 specifies two forms of authentication: open system and shared key.
Beacon	A signal periodically transmitted from the SU-L that is used to identify the service set, and to maintain contact with wireless clients.
CIR	Committed Information Rate: Minimum trasfer rate ensured for the connection
Customer Premise Equipment (CPE)	Customer Premise Equipment: Communications equipment that resides on the customer's premises.
Dynamic Host Control Protocol (DHCP)	Dynamic Host Configuration Protocol: Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.
Ethernet	A popular local area data communications network, which accepts transmission from computers and terminals.
Encryption	Data passing between the SU-L and clients can use encryption to protect from interception and evesdropping.
Extended Service Set (ESS)	Extended Service Set: More than one wireless cell can be configured with the same Service Set Identifier to allow mobile users can roam between different cells with the Extended Service Set.
File Transfer Protocol (FTP)	File Transfer Protocol: A TCP/IP protocol used for file transfer.
Hypertext Transfer Protocol (HTTP)	Hypertext Transfer Protocol: HTTP is a standard used to transmit and receive all data over the World Wide Web.
IEEE 802.11a	A wireless standard that supports high-speed communications in the 5 GHz band using Orthogonal Frequency Division Multiplexing (OFDM). The standard supports data rates of 6, 12, 24, and 54 Mbps.
Infrastructure	An integrated wireless and wired LAN is called an infrastructure configuration.
Local Area Network (LAN)	Local Area Network: A group of interconnected computer and support devices.

MAC	Media Access Control: The lower of the two sub-layers of the data link layer defined by the IEEE. The MAC sub-layer handles access to shared media, such as whether token passing or contention will be used.
MAC Address	Standardized data link layer address that is required for every port or device that connects to a LAN. Other devices in the network use these addresses to locate specific ports in the network and to create and update routing tables and data structures. MAC addresses are 6bytes long and are controlled by the IEEE.
MIR	Maximum Information Rate: Maximum trasfer rate susceptible for the connection
Orthogonal Frequency Division Multiplexing (OFDM)	Orthogonal Frequency Division Multiplexing: OFDM allows multiple users to transmit in an allocated band by dividing the bandwidth into many narrow bandwidth carriers.
Open System	A security option for the SU-L which broadcasts a beacon signal including the configured ESSID. Wireless clients can read the ESSID from the beacon, and automatically reset their ESSID to allow immediate connection to the nearest SU-L.
Power Over Ethernet (PoE)	Power over Ethernet: A specification for providing both power and data to low-power network devices using a single Category 5 Ethernet cable. PoE provides greater flexibility in the locating of Wi²s and network devices, and significantly decreased installation costs.
RTS Threshold	Transmitters contending for the medium may not be aware of each other. RTS/CTS mechanism can solve this “Hidden Node Problem.” If the packet size is smaller than the preset RTS Threshold size, the RTS/CTS mechanism will NOT be enabled.
Service Set Identifier (SSID)	An identifier that is attached to packets sent over the wireless LAN and functions as a password for joining a particular radio cell; i.e., Basic Service Set (BSS).
Session Key	Session keys are unique to each client, and are used to authenticate a client connection, and correlate traffic passing between a specific client and the AU.
Shared Key	A shared key can be used to authenticate each client attached to a wireless network. Shared Key authentication must be used along with the 802.11 Wireless Equivalent Privacy algorithm.
Simple Network Management Protocol (SNMP)	Simple Network Management Protocol: The application protocol in the Internet suite of protocols which offers network management services.
Trivial File Transfer Protocol (TFTP)	Trivial File Transfer Protocol: A TCP/IP protocol commonly used for software downloads.

Virtual LAN (VLAN)	A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, and allows users to share information and resources as though located on the same LAN.
Wired Equivalent Privacy (WEP)	Wired Equivalent Privacy: WEP is based on the use of security keys and the popular RC4 encryption algorithm. Wireless devices without a valid WEP key will be excluded from network traffic.
Wireless Client (SU-L)	A wireless client is a computer system that accesses a remote service on another computer (AP) by means of a wireless transmission signal.