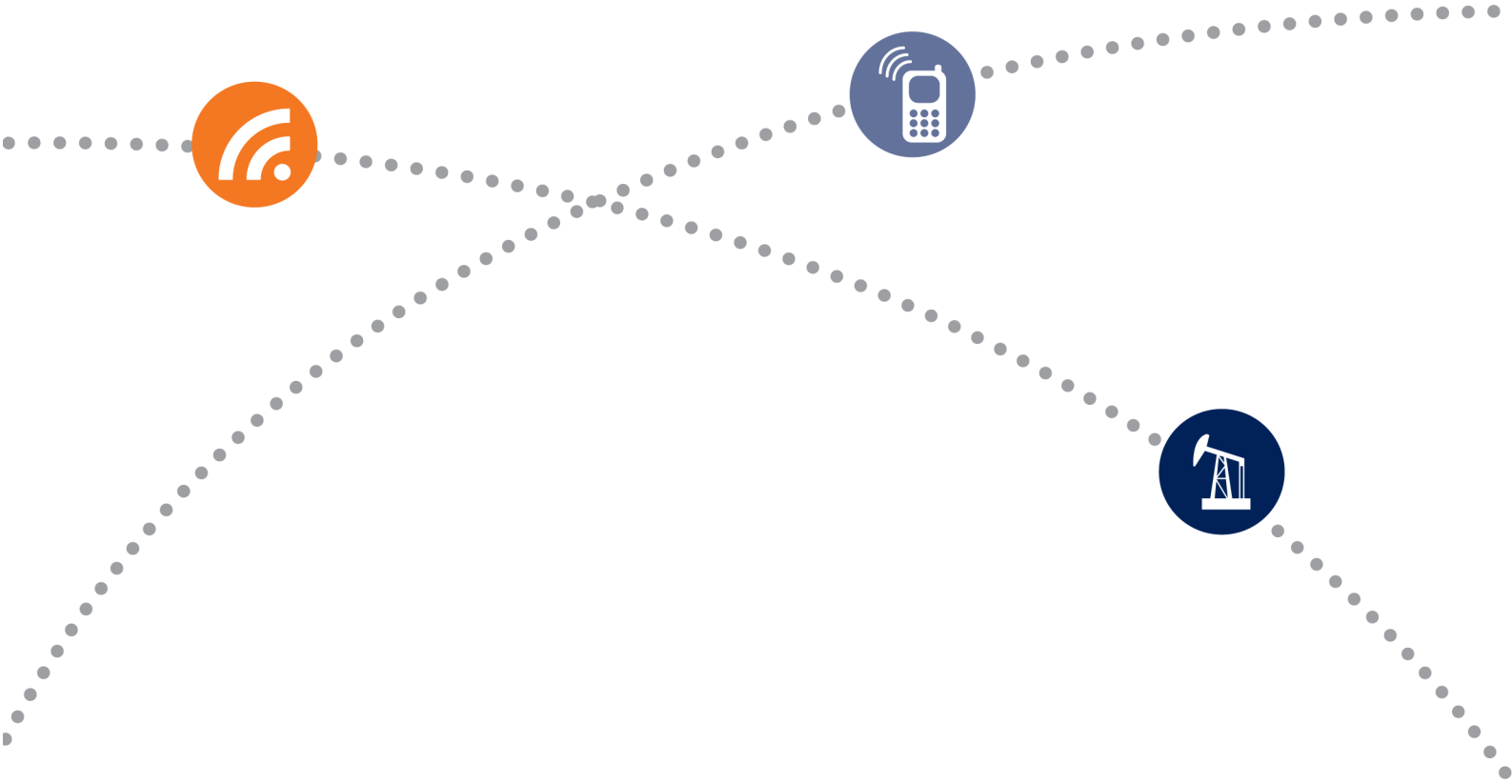


WBSn-2400 and WBSn-2450

System Manual

Software Version 2.0
June 2015
P/N 216066

Front Matter

Trade Names

Alvarion®, Alvarion Technologies®BreezeCOM®, BreezeNET®, BreezeACCESS®, BreezeMAX®, BreezeULTRA™, and/or other products and/or services referenced here in are either registered trademarks, trademarks or service marks of Alvarion.

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. 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 Technologies 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).

FCC Compliance Statement

The Base Station complies with Part 15 of the Federal Communications Commission (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.

CAUTION:

Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the manufacturer's instructions, may cause interference harmful to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio or TV technician for help.

FCC and Industry Canada Radiation Hazard Warning

To comply with Industry Canada exposure requirements, and FCC RF exposure requirements in Section 1.1307 and 2.1091 of FCC Rules, the antenna used for this transmitter must be fixed-mounted on outdoor permanent structures with a separation distance of at least 50 cm from all persons.

R&TTE Compliance Statement

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

Grounding

BS Units are required to be bonded to protective grounding using the bonding stud or screw provided with each unit.

Lithium Battery

The battery is not intended for replacement.

Caution

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

Line Voltage

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

Radio

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

Outdoor Units Installation and Grounding

Ensure that outdoor units and supporting structures are properly installed to eliminate any physical hazard to either people or property. Make sure that the installation of the outdoor units 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 units are grounded and suitable lightning protection devices are used so as to provide protection against voltage surges and static charges. In any event, Alvarion is not liable for any injury, damage or regulation violations associated with or caused by installation, grounding or lightning protection.

Disposal of Electronic and Electrical Waste

Disposal of Electronic and Electrical Waste

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

Important Notice

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

- This manual contains proprietary information belonging to Alvarion Technologies 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 Technologies 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 Technologies 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 Technologies 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 WBSn-2400 and WBSn-2450 solution, and details how to install, operate and manage the system components.

This manual is intended for technicians responsible for installing, setting and operating the WBSn-2400 and WBSn-2450 BS equipment, and for system administrators responsible for managing the system.

This manual contains the following chapters and appendices:

- Chapter 1 - "Introduction": Describes the WBSn-2400 and WBSn-2450 system and its components and provides details on the new features and main modifications introduced in this release.
- Chapter 2 - "Base Station Installation": Describes how to install the base station equipment, complete its' initial configuration and validate proper operational status.
- Chapter 3 - "Base Station Management": Describes how to manage the base station equipment using the web-based management utility.
- Appendix A - "Troubleshooting": Describes the functionality of LEDs and Reset button in the base station, including a description of Rescue mode options.
- Appendix B - "Preparing Ethernet Cables": Describes how to prepare the Ethernet cable for the base station.

Contents

Chapter 1 - Introduction

In This Chapter:

1.1 WBSn System Description

Alvarion's Wi-Fi Base Stations with 802.11n support (WBSn) is a family of advanced Gigabit outdoor Wi-Fi base stations operating in the 2.4 and 5 GHz unlicensed bands. The system combines true two-way Beamforming 802.11n and interference mitigation technologies together with 3x3:3 MIMO (2x2:2 in the WBSn-2450-SHD), delivering best capacity and coverage. The interference immunity suite combines the inherent Beamforming ability to suppress interference, the Dynamic Interference Handling (DIH) algorithm that continuously optimizes receiver's parameters according to noise level, the Automatic Channel Selection (ACS) algorithm for selection of best operating channel, the Wireless Alvarion Rate Adaptation (WARA) mechanism for optimal rate selection in environments with high interference, and the capabilities of the sector antennas and Down Tilted omni Antennas to reject noise out of their field-of-view.

The carrier grade WBSn base stations are designed for high reliability and manageability, including a robust IP-68 certified enclosure for harsh environments, security and QoS features, FCAPS management suite, and simple and easy installation.

WBSn base stations include rich embedded networking capabilities, including Bridging, Routing and a fully integrated Access Controller, for flexible service planning and reduced costs.

WBSn base stations are currently available in the following configurations:

- Single band base stations operating in the 2.4 GHz band:
  - WBSn-2400-O: A base station with 3 omni antennas.
  - WBSn-2400-S: A base station with an integral high gain triple polarization sector antenna.
- Dual band base stations operating in both the 2.4 GHz and 5 GHz bands:
  - WBSn-2450-O: A base station with 3 omni antennas serving both bands.
  - WBSn-2450-S: A base station with an integral high gain triple polarization sector antenna serving both bands.
  - WBSn-2450-OS: A base station with 3 omni antennas serving the 2.4 GHz band and an integral high gain triple polarization sector antenna serving the 5 GHz band.
  - WBSn-2450-SO: A base station with an integral high gain triple polarization sector antenna serving the 2.4 GHz band and 3 omni antennas serving the 5 GHz band.
- WBSn-2450-SHD: A dual band base station with an integral high gain, dual polarization, narrow beam sector antenna serving both the 2.4 GHz and 5 GHz radio bands. The WBSN-2450-SHD is designed for enhanced performance in high density environments such as sport stadiums, music arenas and exhibition halls.

1.2 Specifications

1.2.1 Modem & Radio

Table 1-1: General Modem & Radio Specifications

Item	Description	
	2.4 GHz Band	**5 GHz Band**
Frequency Range*	2.400 - 2.483 GHz, 13 channels	4.900 - 5.900 GHz
Radio Type	IEEE 802.11 b/g/n	IEEE 802.11 a/n
Modulation	802.11n: ■ All models excluding WBSn-2450-SHD: 3x3 MIMO with 3 spatial data streams (3:3:3) ■ WBSn-2450-SHD: 2x2 MIMO with 2 spatial data streams (2:2:2) 802.11g: OFDM 802.11b: DSSS	802.11n: ■ All models excluding WBSn-2450-SHD: 3x3 MIMO with 3 spatial data streams (3:3:3) ■ WBSn-2450-SHD: 2x2 MIMO with 2 spatial data streams (2:2:2) 802.11a: OFDM
Data Rates	802.11n: MCS0 - MCS23 802.11g: 54, 48, 36, 24, 18, 12, 9, 6 Mbps 802.11b: 11, 5.5, 2, 1 Mbps	802.11n: MCS0 - MCS23 802.11a: 54, 48, 36, 24, 18, 12, 9, 6 Mbps
Channel Bandwidth	20 / 40 MHz	20 / 40 MHz
Central Frequency Resolution*	5 MHz	5 MHz
Transmit Power** (at antenna port)	3-26 dBm, 1 dB steps	3-25 dBm, 1 dB steps
Sector Antenna (internal)	■ All models excluding WBSn-2450-SHD: HGDP 12 dBi, 120°H x 16°V, triple polarization (45°-0°--45°) ■ WBSn-2450-SHD: HGDP 15 dBi, 30°H x 20°V, dual polarization (0°-90°)	■ All models excluding WBSn-2450-SHD: HGDP 14 dBi, 120°H x 8°V, triple polarization (45°-0°--45°) ■ WBSn-2450-SHD: HGDP 18 dBi, 30°H x 9°V, dual polarization (0°-90°)
Omni Antennas	3 x 7.5 dBi, 360°H 20°V	3 x 8.5 dBi, 360°H 10°V

* Actually available channels depend on relevant regulations and standards.

** In the 5 GHz band actual operating frequency range and maximum transmit power depend on relevant local regulations.

1.2.2 Mechanical and Electrical

Table 1-2: Base Station Mechanical & Electrical Specifications

Item	Description
Dimensions	WBSn-2400-O: 38 x 13.7 x 7.5 cm (excluding antennas) WBSn-2400-S: 38 x 13.7 x 39 cm WBSn-2450-O: 38 x 13.7 x 12 cm (excluding antennas) WBSn-2450-OS, WBSn-2450-SO: 38 x 13.7 x 43.5 cm (excluding antennas) WBSn-2450-S, WBSn-2450-SHD: 38 x 13.7 x 43.5 cm
Weight	WBSn-2400-O: 1.85 kg (excluding antennas) WBSn-2400-S: 2.5 kg WBSn-2450-O: 2.45 (excluding antennas) WBSn-2450-OS: 3 kg (excluding antennas) WBSn-2450-SO: 3.2 kg (excluding antennas) WBSn-2450-S, WBSn-2450-SHD: 3.2 kg
Input Power	55 VDC Power over Gigabit Ethernet (use only PoE injector supplied by Alvarion).
Power Consumption	Single band: 19 W nominal, 23 W maximum Dual band: 22 W nominal, 30 W maximum *Power consumption will be lower if actual Tx Power is lower than the maximum supported by the unit

1.2.3 Management

Table 1-3: Management Specifications

Item	Description
Management	Type: Web-based management utility Local management: Via Ethernet (LAN) port Remote management: Via Ethernet (LAN) or wireless link
Software Upgrade	Via the web-based management utility, FTP
Configuration upload/download	Via the web-based management utility, FTP)
Management Access Security	Access Protection: user Name and Password. Access via wireless link can be blocked.

1.2.4 Standards Compliance

Table 1-4: Base Station Standards Compliance

Type	Standard
EMC	■ FCC 47 CFR Part 15B Class B ■ EN 301 489 ■ ETSI EN 301 489-1/17
Safety	■ UL 60950-1 ■ UL 60950-22 ■ CAN/CSA-C22.2 No. 60950-1 ■ CAN/CSA-C22.2 No. 60950-22 ■ EN/IEC 60950-1 ■ EN/IEC 60950-22
Environmental	■ ETSI EN 300 019-2-2 ■ ETSI EN 300 019-2-4 V2.1.2 ■ IEC 60068-2-64, 29 ■ IP68 - IEC 60529
Radio	■ FCC 47 CFR part 15C ■ EN 302 502 ■ EN 301 893 ■ EN 300 328
Restriction of Hazardous Substances	RoHS Directive
General	■ 802.11n ■ 802.1x ■ SNMPv2 ■ WMM

1.2.5 Environmental

Table 1-5: Environmental Specifications

Type	Details
Operating Temperature	-40°C to 55°C
Operating Humidity	5%-95% non condensing, weather protected
Ingress Protection Rating	IP-68
Wind Survivability	220 km/h

1.2.6 Power over Ethernet Injectors (optional)

Table 1-6: PoE Injectors Specifications

Type	Details
WPI-AC-1G	Power over 1Gbps Ethernet Injector with TVS (transient voltage suppressing) protection. Input 90-264VAC, output 56VDC, max 60 Watt. Indoor environment only, 0°-40°C operating temperature. Power cable to be ordered separately.
WPI-48DC-1G	Passive Power over 1Gbps Ethernet injector with internal over-current protection. Input -48VDC, output 48VDC, max 48 Watt (1Amp). Indoor environment only, -20°-60°C operating temperature.

Chapter 2 - Base Station Installation

In This Chapter:

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 equipment.

Failure to do so may void the product warranty and may expose the user 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 equipment.

2.1 Installation Requirements

2.1.1 Packing List

Check contents of the package:

- Base Station:
  - » BS Unit
  - » Post clamp
  - » Two steel bands
  - » 2 screws, each with attached spring and flat washers
  - » Extraction Key
  - » Security cable
  - » For WBSn-2400-O, WBSn-2450-O, WBSn-2450-OS and WBSn-2450-SO: Three suitable Omni Antennas
  - » For a unit with Omni antennas (WBSn-2400-O, WBSn-2450-O, WBSn-2450-OS and WBSn-2450-SO: IP68 waterproof sealing tape)

2.1.2 Additional Installation Requirements

The following items are also required to install the BS:

- 1 Gigabit Ethernet PoE Injector and a power cable (for details on PoE Injectors available from Alvarion refer to "Power over Ethernet Injectors (optional)" on page 6).
- Data and Power Ethernet cable: Outdoor Category 5e 4-pair shielded data cable, two shielded RJ45 connectors, and tools required for on-site preparation of the cable if required.

NOTE!

The combined length of the outdoor Ethernet cable (from the PoE Injector to the BS) and the Ethernet cable connecting to the data networking equipment should not exceed 100 meters.

- Grounding cable (10 AWG or thicker) with an M6 terminal ring for connecting to the BS grounding terminal and an appropriate termination for connecting to protective grounding.
- For pole installation: 1"-6" diameter pole (or a suitable tower structure) should be available.
- For wall installation: Depending on type of surface - 4 suitable screws or 4 sets of suitable screws and anchors.
- Portable PC and a straight Ethernet cable (for configuration purposes).
- Ethernet cable for connecting to the data networking equipment.

- Installation tools and materials.

INFORMATION

Even where grounding and lightning protection is not mandatory according to applicable regulation and national codes, it is highly recommended to ensure that the outdoor units are grounded and suitable lightning protection devices are used so as to provide protection against voltage surges and static charges.

It is recommended to install a well grounded lightning rod above the BS and a suitable lightning protection device at the point of entry to the indoor structure. In a lightning prone area it is recommended to install another lightning protection device close to the Ethernet port of the base station. Only Gigabit PoE lightning protection devices should be used with this equipment.

For more information on lightning protection techniques you may consult with Alvarion's technical experts.

The following sections describe an installation without any lightning protection devices. For installations with lightning protection device(s), additional cable segments prepared following relevant instructions will be required.

2.1.3 Optional Accessories

Extender kit (for details see "Attaching an Extender to the Post Clamp (optional)" on page 13).

2.2 Location Selection Guidelines

NOTE!

For specific information about selecting the locations for WBSn-2450-SHD units in high density environments refer to the High Density Wi-Fi Solution Guidelines document.

Prior to installation of the Base Station equipment, select a suitable installation site. Choose a site that supports the physical characteristics of the unit and is in accordance with the unit's environmental and power requirements.

Consider the following when planning the installation:

- The location of the indoor PoE Injector should take into account its connection to the power source and to the data networking equipment.
- When selecting the location intended for the outdoor BS equipment make sure to allow easy access for installation, replacement or maintenance purposes.
- Consider the maximum cable length specified for the units. Make sure that the length of the cables is sufficient to reach their destination connection.
- The base stations are pole or wall mounted. For pole mounted units, ascertain the existence of potential posts or poles to which the base station could be attached. Consider the axis of the post, its placement, and whether extenders are required.
- The front panel of a base station with sector antenna(s) (WBSn-2400-S, WBSn-2450-S, WBSn-2450-OS, WBSn-2450-SO and WBSn-2450-SHD) should be directed towards the area intended to be covered, with maximum possible lines of sight for client locations.

- A unit with Omni antennas should be installed at the highest of point the pole. This is to ensure that there is no interference caused by the close proximity of the antenna to other metal objects. Where this is not possible, the unit should be installed at a distance of at least 1 meter from the pole, using a horizontal bar.
- Generally, the higher the placement of the base station, the better the link quality achievable. However, the higher the installation the greater the interference from other sources of radiation that the base station is exposed to. Consider best installation spot that maximizes coverage and minimizes interference. Typically, the ideal height at which a base station should be installed is at least 3 meters above the rooftops of the buildings within the coverage zone. Keep the maximum distance possible from other RF radiating sources, power lines and metal objects.
- The minimum vertical separation distance between two base stations is 2 meters. The minimum horizontal separation distance between two base stations (back-to-back) with sector antennas is 2 meters. For units with Omni antennas he minimum horizontal separation distance between two base stations (back-to-back) is 10 meters.

2.3 Safety Instructions and Information

Please ensure that you read and understand the following safety information. Ensure that you carefully read and follow all instructions in this manual, and heed all warnings.

- Do not modify the construction of this product.
- There is a risk of personal injury or death if the unit is close to electric power lines.
- By nature of the outdoor installation, you may be exposed to hazardous environments and high voltage. Use extreme caution when installing the system.
- Servicing may be required when the equipment has been damaged in any way. All servicing should be referred to qualified service personnel only.
- The base station must be properly grounded.
- Do not open the unit - risk of electric shock.
- Any change or modification not expressly described in this manual or approved by the manufacturer could void your authority to operate this equipment.
- It is recommended to install a suitable surge suppressor device to protect against overvoltage on mains input to the equipment.

2.4 The Installation Process

	IMPORTANT
NOTE!	Before starting the installation process note down the MAC address of the unit printed on the label. Availability of this information is mandatory when IP parameters of the management interface are obtained using DHCP.

The typical installation process comprises the following steps:

1. Choose the locations for the outdoor and indoor equipment (refer to "Location Selection Guidelines" on page 9).
2. Verify the existence of a good protective grounding (earth) connection near the location intended for the base station.
3. Prepare the outdoor Ethernet cable and connect it to the base station (refer to "Preparing and Connecting the Outdoors Ethernet Cable" on page 12).
4. Prepare the grounding cable and connect it to the base station (refer to "Preparing and Connecting the Grounding Cable" on page 13).
5. If an extender is required, attach it to the post clamp (refer to "Attaching an Extender to the Post Clamp (optional)" on page 13).
6. Attach the post clamp (with the extender if applicable) to the pole/wall and attach to it the base station. Verify that it is properly directed towards the required coverage area (refer to "Mounting the Base Station" on page 15).
7. For units with Omni antennas: Connect and seal the three antennas (refer to "Connecting and Sealing Omni Antennas (if applicable)" on page 17).
8. Complete the outdoor installation (refer to "Completing the Outdoor Installation" on page 17).
9. Install and connect the indoor equipment (refer to "Connecting the Indoor Equipment" on page 18).
10. Verify that the unit can be remotely managed (refer to "Verification" on page 19).

2.5 Base Station Connectors and LEDs

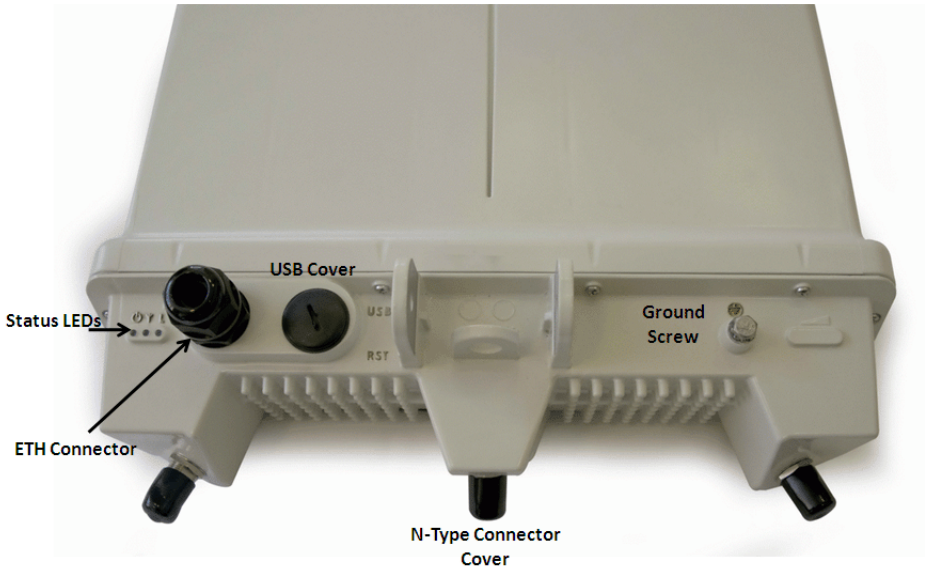


Figure 2-1: Base Station Connectors and LEDs (a unit with both omni and sector antennas)

IMPORTANT

NOTE!

The USB connector does not function as a standard USB port and is intended for special engineering purposes only. Ensure that the USB connector and RST button are properly sealed with the plastic cap.

For details on using the RST (Reset) button refer to "Using the Reset Button of the Base Station" on page 112.

For details on the functionality of the Status LEDs refer to "Base Station LEDs Description" on page 111.

2.6 Preparing and Connecting the Outdoors Ethernet Cable

It is recommended to attach the Ethernet connector to the cable and connect it to the base station prior to mounting the outdoor unit. Typically the connector on the other side will be attached only after completing the outdoor installation and routing the open-ended cable to the location intended for the PoE Injector.

For detailed instructions on how to prepare the Ethernet cable refer to "Preparing the Base Station's Ethernet Cable" on page 116.

NOTE!

Make sure that the length of the Ethernet cable is sufficient for reaching from the intended location of the base station to the intended location of the indoor equipment.

The combined length of the outdoor Ethernet cable (from the base station to the PoE Injector) and the Ethernet cable connecting the PoE Injector to the data networking equipment should not exceed 100 meters.

2.7 Preparing and Connecting the Grounding Cable

To prepare and connect the grounding cable:

1. Prepare a 10 AWG (or thicker) grounding cable with an M6 terminal ring on one end (for connecting to the base station) and a suitable termination on the other end according to the intended protective ground connection. The length of the cable should be sufficient for conveniently reaching from the base station's grounding screw to the protective ground connection.
2. Remove the nut and one of the star washers from the grounding screw.
3. Attach the M6 terminal ring to the grounding screw.
4. Attach the second star washer and firmly tighten the nut.

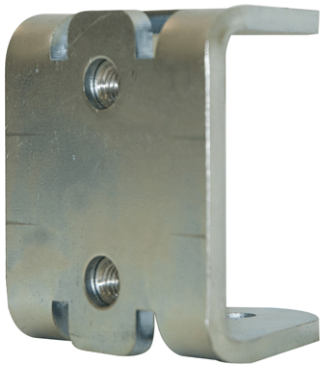
2.8 Attaching an Extender to the Post Clamp (optional)

An extender (ordered separately) may be needed in the following cases:

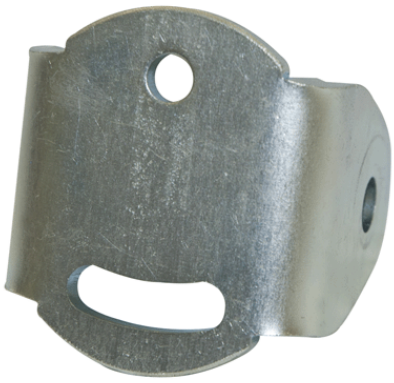
- A wall or horizontal pole installation where adjustment of the direction in the horizontal plan is required for directing the base station towards the required coverage area. The extender may also be used in vertical pole installations for simpler adjustment of the direction in the horizontal plan.
- Installation on a post that deviates from the vertical or horizontal plane by up to +/- 15 degrees.

The extender comprises two parts:

1. A part that enables adjustment of the direction in the horizontal plane (left/right) when attached to the post clamp
2. A part with a circular slot that enables adjustment of the direction in the vertical plane (up/down) when attached to the first part.



Horizontal Plane Adjustment



Vertical Plane Adjustment

Figure 2-2: Extender Parts

The extender kit includes also 4 screws with attached spring and flat washers.

To attach the extender to the post-clamp:

1. Attach the horizontal adjustment part of the extender to the post clamp with 2 screws and washers using a 13 mm ratchet key with a torque of 18.4 lb-ft (25 Nm).
2. Attach the vertical adjustment part to the horizontal adjustment part with 2 screws and washers using a 13 mm ratchet key with a torque of 18.4 lb-ft (25 Nm).

Figure 2-3: Extender and Post-Clamp Attached

2.9 Mounting the Base Station

NOTE!

For specific information about mounting the WBSn-2450-SHD in high density environments refer to the High Density Wi-Fi Solution Guidelines document.

2.9.1 Using the Post-Clamp

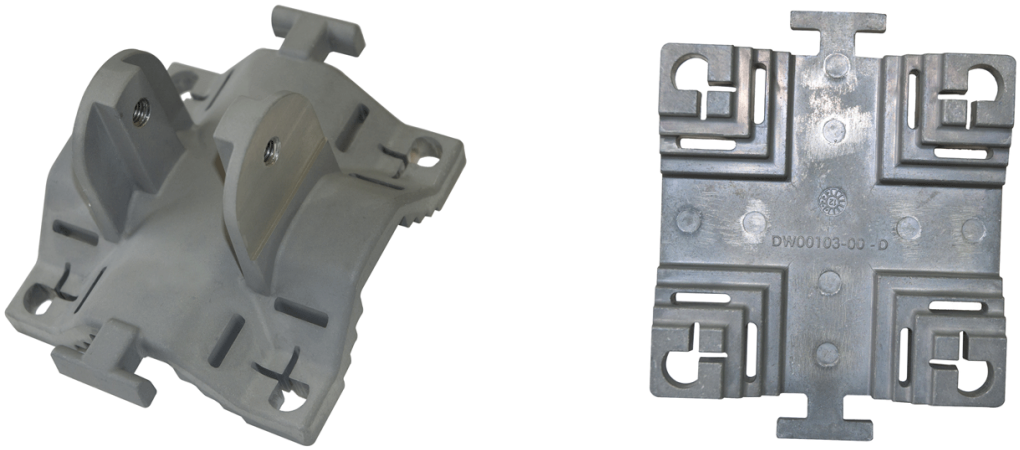


Figure 2-4: Post-Clamp

The base station should always be installed vertically, with the bottom side (with connectors and LEDs) pointing downward. To support this requirement, in regular installations (without an extender), the post clamp should be installed vertically (with the two protrusions pointing up and down). In installations with an extender, the post clamp should be installed horizontally ((with the two protrusions pointing sideways).

The slots support installation on poles with different diameters (1"-6") on either vertical or horizontal poles. The holes enable wall mount installation.

2.9.2 Wall Mount Installation

To mount the unit on a wall:

1. Place the post clamp on the wall and mark the exact location of the holes to drill. The location of the screws should be planned with maximum precision.
2. Drill the holes and use four suitable metal anchors and screws to secure the post clamp (with an extender if applicable) to the wall.

3 Attach the base station unit to the post clamp (or to the extender), with the 2 screws and washers. Tighten the screws using a 13 mm ratchet key with a torque of 18.4 lb-ft (25 Nm). As you tighten the screws, verify that the tilt of the base station unit is correct for the coverage area required.

NOTE!

In an urban setting, with a high-placed installation, a slight downwards tilt (approximately 8 - 10 degrees) will help reduce noise and interference.

4 If you use an extender, verify that the directions in the horizontal and vertical planes are correct. If needed, release slightly the applicable screws and re-adjust the direction of the base station. Tighten the screws using a 13 mm ratchet key with a torque of 18.4 lb-ft (25 Nm).

2.9.3 Pole Mount Installation

CAUTION

When climbing on a pole/tower and during installation/removal of the unit, use the security cable with the carabiner to safely attach the equipment to a suitable object.

The post clamp supports installation on polls with a diameter of 1" to 6" by using the appropriate pairs of slots.

To mount the unit on a pole:

1 Thread the two steel band through the two appropriate slot pairs. For a thinner post, the steel bands should be threaded through the inner slots, and for a wider post, through the outer slots.

2 Secure the post clamp to the pole by closing and tightening the steel bands with a torque of 3.8 lb-ft (5.1 Nm). As you tighten the screws, verify that the direction is correct for the coverage area required.

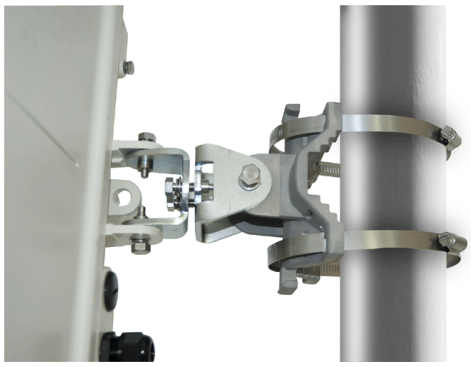
3 Attach the base station unit to the post clamp (or to the extender), with the 2 screws and washers. Tighten the screws using a 13 mm ratchet key with a torque of 18.4 lb-ft (25 Nm). As you tighten the screws, verify that the tilt of the base station unit is correct for the coverage area required.

NOTE!

In an urban setting, with a high-placed installation, a slight downwards tilt (approximately 8 - 10 degrees) will help reduce noise and interference.

4 If you use an extender, verify that the directions in the horizontal and vertical planes are correct. If needed, release slightly the applicable screws and re-adjust the direction of the base station. Tighten the screws using a 13 mm ratchet key with a torque of 18.4 lb-ft (25 Nm).

Without Extender (vertical pole)



With Extender (horizontal pole)

Figure 2-5: Pole Mounting, with/without an Extender

2.10 Connecting and Sealing Omni Antennas (if applicable)

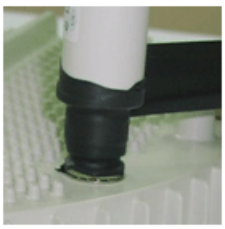
NOTE!

Only the antennas supplied in the original package should be used.
The antennas should only be connected after completing the installation procedure and prior to powering the unit.
All three antennas must be connected.

1. Screw the three antennas into the three N-type connectors on the bottom of the WBSn base station unit. Do not use excessive force.
2. After the antennas are connected, use the supplied isolation tape to cover the N-Type connectors and the lower part of the antennas to ensure IP-68 compliant protection against dust and water:

   a. Cut 18 cm of the attached splicing tape.

   b. Stretch and wrap the tape in an even, half overlapping manner around the antenna and N-Type connector. Cover this with a layer of vinyl plastic tape.



2.11 Completing the Outdoor Installation

To complete the outdoor installation:

1. Firmly connect the grounding cable to a protective ground (earth) connection.
2. Route the Ethernet cable to the intended location of the PoE Injector. Use proper means to secure the cable to the pole/tower, walls, and other objects as required.

2.12 Connecting the Indoor Equipment

IMPORTANT

NOTE!

The following instructions are for the AC PoE Injector available from Alvarion. For details on installing the DC PoE Injector available from Alvarion refer to the Quick Installation Guide supplied with it.

Figure 2-6: AC PoE Injector

After mounting the unit with the Ethernet cable connected and verifying proper grounding, proceed to complete the indoor installation.

To connect the indoor equipment:

1. Insert and crimp a shielded RJ-45 connector to the Ethernet cable. For detailed instructions on how to prepare the Ethernet cable refer to "Preparing the Base Station's Ethernet Cable" on page 116.
2. Connect the Ethernet cable to the OUT connector of the PoE Injector.
3. Use the power cable to connect the PoE Injector to a mains outlet.
4. Use a standard Gigabit Ethernet cable to connect the IN connector of the PoE Injector to the networking equipment.

2.13 Verification

Disconnect the PC from the IN port of the PoE Injector and connect the IN port to the networking equipment (that should be configured to provide connectivity from the control center to the base station). The ability to properly manage the unit from the control center must be verified before leaving the site.

Chapter 3 - Base Station Management

In This Chapter:

3.1 Using the Web-Based Element Management System

This section includes:

3.1.1 Accessing the Element Management System

To access the web-based Element Management System (EMS), follow these steps:

1 Open a web browser and connect to the following URL: http://<base_station_IP_address>.

NOTE!

The default method of setting the unit's IP parameters is DHCP client, meaning that IP parameters should be obtained automatically from a DHCP server. When IP parameters are obtained from a DHCP server, the details of the management interface IP parameters should be provided by the system administrator (based on the MAC address of the unit, which is printed on the unit's label). If a DHCP server is not available, the unit will use the fallback parameters configured for the management interface (See "Fallback IP" on page 69. The default fallback IP address is 192.168.1.1 with a subnet mask of 255.255.255.0). In this case, if static IP parameters should be used, connect directly to the unit using the default fallback address and configure the appropriate management interface parameters.

2 The log in window is displayed:

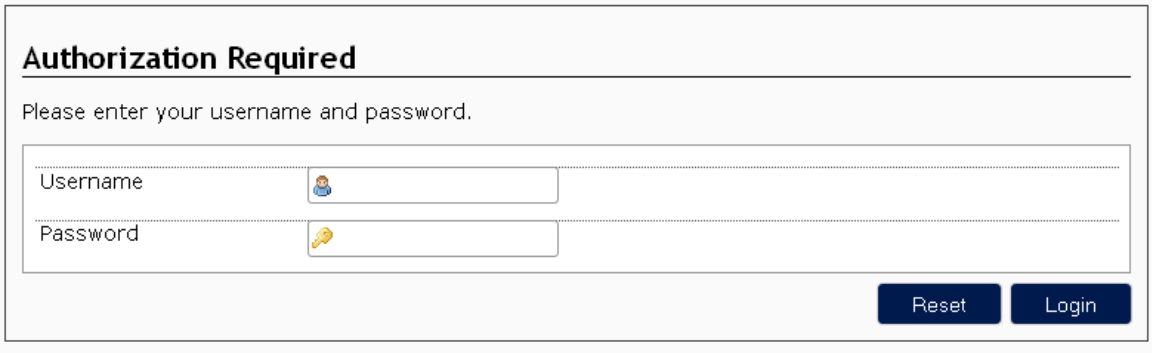


Figure 3-1: Login Window

3 Enter the Username and Password (the default Username/Password are **admin/admin**).

NOTE!

To clear the Username/Password fields click on the **Reset** button.

4 Click on the **Login** button. The Status Overview page of the management utility is displayed.

3.1.2 Using the Element Management System

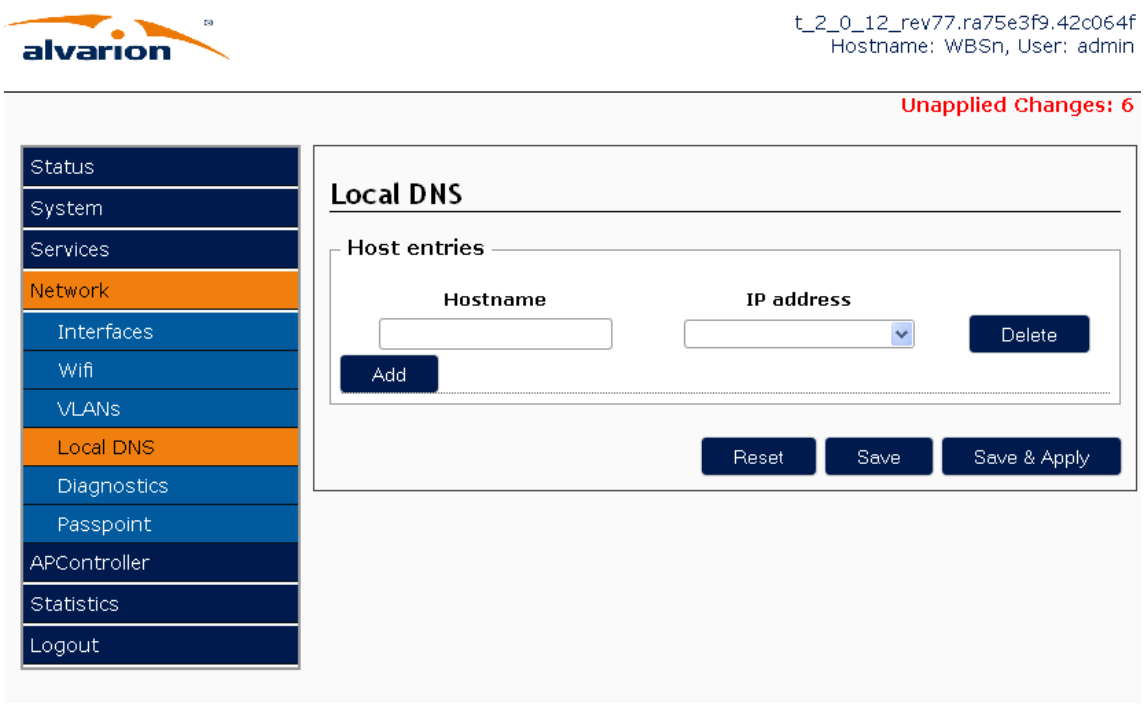


Figure 3-2: EMS Window

The management window comprises the following components:

- General Information Section
- Management Function Selection Panel
- Work Area

3.1.2.1 General Information Section

The general information section at the top right corner of the window includes:

- The version number of the currently running firmware.
- **Hostname** (the name defined for the unit) and **User** (the Username of the logged in user).
- **Unapplied Changes**, in red (if any) or **Changes: 0** if there are no unapplied changes.

3.1.2.2 Management Function Selection Panel

The management function selection panel (on the left side of the screen) enables selecting one of the following options:

- **Status**: Enables viewing current configuration of various parameters and certain status indicators and performance graphs. See "Status" on page 26.

- **System**: Enables viewing/modifying the unit's general parameters. See "System" on page 40.
- **Services**: Enables viewing/modifying various parameters that control hotspot services that may optionally be provided by the unit. See "Services" on page 53.
- **Network**: Enables viewing/modifying various parameters that control the networking functionality of the unit such as WAN and LAN interfaces, Wifi radios and wireless networks, VLANs and Passpoint profiles. See "Network" on page 61.
- **APController**: Enables viewing/modifying parameters for supporting remote management of the unit by the Arena controller. See "APController" on page 101.
- **Statistics**: Enables viewing statistics for a variety of performance and status indicators. See "Statistics" on page 103.
- **Logout**: Click on the Logout tab to logout from the management utility.

Click on a management function tab (excluding the Logout tab) to view the second-level tabs allowing selection of specific status/management pages and open the page for the first second-level tab.

Third-level tabs are available for certain second-level tabs.

3.1.2.3 Work Area

The work area displays the relevant parameters according to the selection in the management function panel, allowing a user to view current status/configuration of relevant parameters and to modify the configuration of relevant parameters (if applicable for the selected page).

- Parameter's Configuration methods
- Managing Configurable Lists
- Saving/Applying Changes

3.1.2.3.1 Parameter's Configuration methods

The following methods for selecting the required value for configurable parameters are common to most configuration pages:

- Drop-down List: Parameters with several value options are configured using drop-down list that include the available options. To configure these parameters, click on the drop-down arrow on the right side of the configuration field and select the required option from the drop-down list.
- Text Field: Parameters that are defined using a string of characters are configured using a text field. To change the setting, mark the current settings and enter the new string. Note that most parameters require a certain format (such as IP address) or are subject to certain limitations such as maximum string length.
- Checkbox: Used for either selecting/deselecting an instance or for enabling/disabling a feature/option.

Grayed-out fields are read-only. This may be due to the particular parameter being either a read-only parameter or because another parameter must be changed to enable read-write access for the required parameter.

NOTE!

The options / value range available for certain parameters depend on the current option/value set for other values. For example, the available options for the Channels parameter depend on the currently applied option for the Regulatory Domain. In certain cases you may have to apply a change and refresh the displayed information for viewing current options/range of other parameters. For example, after changing the Channel parameter you should apply the change and refresh the display to view the correct range for the Tx Power parameter.

3.1.2.3.2 Managing Configurable Lists

There are two types of configurable lists:

- A Single Elements List
- A Multiple Elements List

3.1.2.3.2.1 A Single Elements List

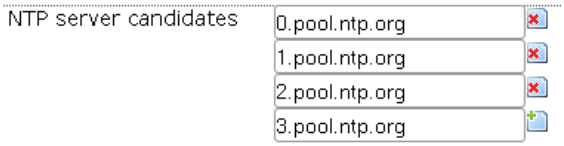


Figure 3-3: A Single Elements List

To add an entry to the list, click on the **+** sign on the right side of the last entry.

To remove an entry from the list, click on the **x** sign on the right side of the entry (the first entry cannot be removed, it can only be cleared).

NOTE!

Certain single elements lists are managed using the Add and Delete buttons as described in A Multiple Elements List below.

3.1.2.3.2.2 A Multiple Elements List

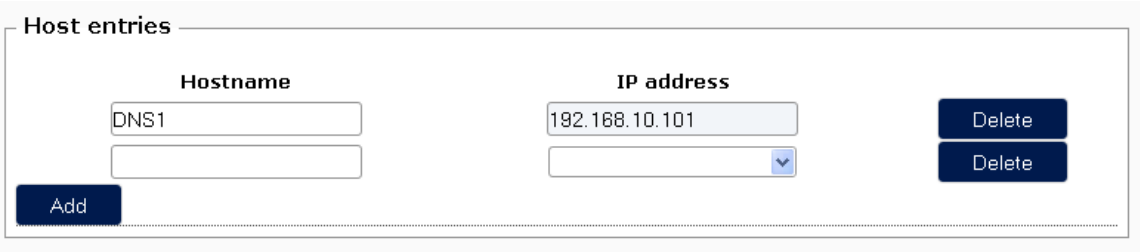


Figure 3-4: A Multiple Elements List

To add a user to the list, click on the **Add** button at the bottom left corner of the section.

To delete one of the entries added to the list, click on the **Delete** button on the right side of the entry.

3.1.2.3.3 Saving/Applying Changes

To temporarily save changes to the configuration in the GUI, click on the **Save** button at the bottom right side of the page. To permanently save the changes, click on the **Save & Apply** button. If the changes are not saved and applied, than after reboot unapplied changes will be lost. Existence of such changes are indicated in the **Unapplied Changes** message in top right corner of the page.

Changes that were not saved will be cleared upon switching to a different page or after refreshing the displayed page. You may also use the **Reset** button to clear unsaved changes.

Most changes are applied in runtime, meaning that a change becomes effective immediately after applying it (clicking the **Save & Apply** button). Changes in certain parameters require rebooting the device: the change is stored in the device after clicking on the **Save & Apply** button, but the new settings will take effect only after the device is rebooted (see "Reboot Page" on page 51). This is indicated by a suitable pop-up message displayed after applying the change, indicating that after completing all configuration changes the device should be rebooted for the new settings to take effect.

3.2 Status

The Status option provides access to the following pages:

- Status Overview Page
- Routes Page
- System Log Page
- Realtime Graphs Pages
- Hotspot Users Page

All Status parameters are read-only, providing information on current configuration of relevant parameters, general status information and graphs of certain performance indicators.

3.2.1 Status Overview Page

To access the Status Overview page click on the **Status** tab in the management function selection panel.

The Status Overview page comprises the following sections:

- Mesh Uplink Status (applicable only for a device operating in Mesh AP mode)
- Mesh (applicable only for a device operating in any Mesh mode).
- System
- Hardware Information
- Network
- Wireless
- Associated Stations
- DHCP Leases

3.2.1.1 Mesh Uplink Status

The Mesh Uplink Status section is available only for a device operating in Mesh AP mode, showing performance information for the uplink (client wireless network).

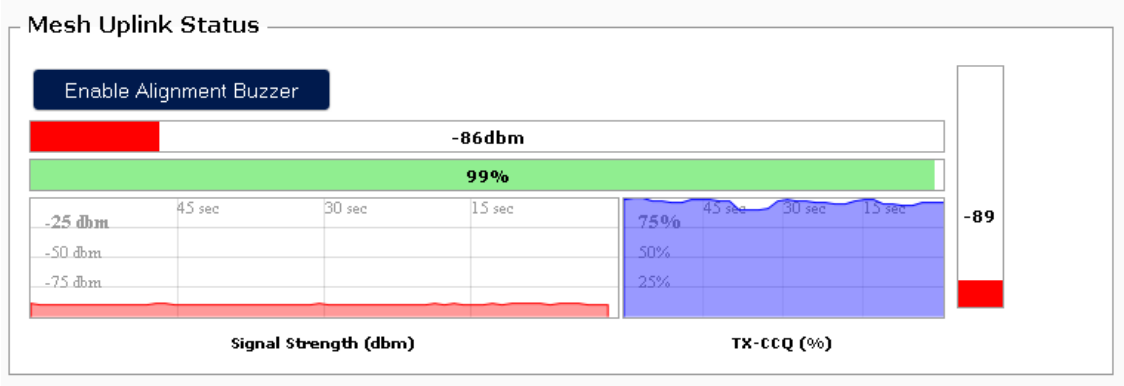


Figure 3-5: Status Overview Page, Mesh Uplink Status Section

The value on the top left box denotes the current received signal strength in dBm. The color of the vertical bar indicates the relative quality.

The box directly below it shows the current TX-CCQ (connection quality), in %. The color of the vertical bar indicates the relative quality.

The bottom left box shows a realtime graph of the received signal strength (in dBm) over the last 60 seconds. The box directly to its right shows a realtime graph of the TX-CCQ (in %) over the last 60 seconds.

On the right of this section, there is a vertical bar showing the current received signal strength at the antennas. The color of the vertical bar indicates the relative quality.

3.2.1.2 Mesh

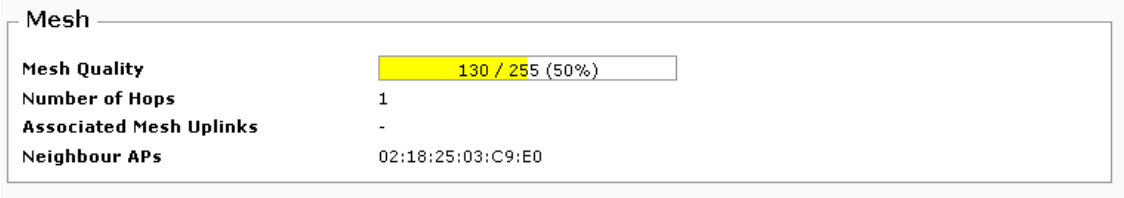


Figure 3-6: Status Overview Page, Mesh Section

The Mesh section is available only for devices operating in Mesh mode. The contents depend on the Mesh mode:

- **Mesh Quality**: Available only for a device operating in Mesh AP mode. The quality of the Mesh in %. The background color indicates the relative quality.
- **Number of Hops**: Available only for a device operating in Mesh AP mode. The current location of the unit in the Mesh leaf. The lowest number is 1, meaning the next hop is the Root-AP.
- **Associated Mesh Uplinks**: The BSSID(s) of the associated Mesh AP(s) (if any).

- **Neighbor APs**: The BSSID(s) of neighboring Mesh node(s).

3.2.1.3 System

Figure 3-7: Status Overview Page, System Section

The System section includes the following parameters:

- **Router Name**: The name of the unit
- **Main Bank Version** and **Shadow Bank Version**: The device can hold two software versions: Main Bank Version and Shadow Bank Version. Typically the Main Bank firmware is the running version and the Shadow Bank firmware is the backup version. For details on loading an managing firmware version refer to "Backup / Flash Firmware Page" on page 48.

  The Main Bank Version and Shadow Bank Version provide the version numbers for the Main Bank firmware and Shadow Bank firmware files. An asterisk sign (*) indicates the firmware file currently used as the running version.
- **Rescue Version**: The version number of the rescue mode firmware. The Rescue mode firmware enables operation in rescue mode if necessary. Rescue mode is a special operation mode allowing to access the unit when it does not operate properly and cannot be accessed using the regular login method. For details see "Restarting the Unit in Rescue Mode" on page 112.
- **Bootloader Version**: The version number of the Bootloader firmware, used for loading the operational firmware (or rescue mode firmware) after power-up.
- **Local Time**: Displays the current date and time according to the unit's real time clock. For details see System Properties "General Settings" on page 41 and "Time Synchronization" on page 43.

3.2.1.4 Hardware Information

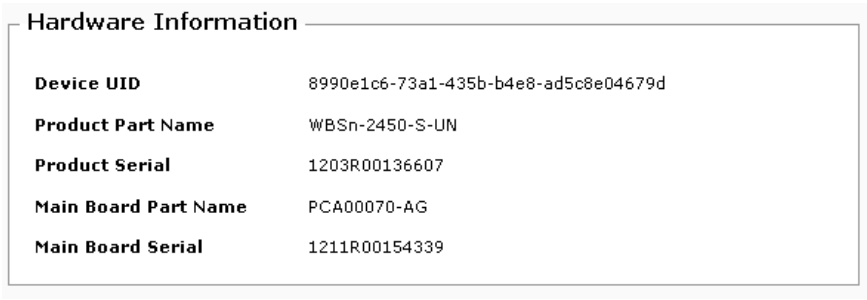


Figure 3-8: Status Overview Page, Hardware Information Section

The Hardware Information section includes the following parameters:

- **Device UID**: The Unique IDentifier of the device's hardware.
- **Product Part Name**: The device's model.
- **Product Serial**: The device's serial number.
- **Main Board Part Name**: The model of the device's main board.
- **Main Board Serial**: The serial number of the device's main board.

3.2.1.5 Network

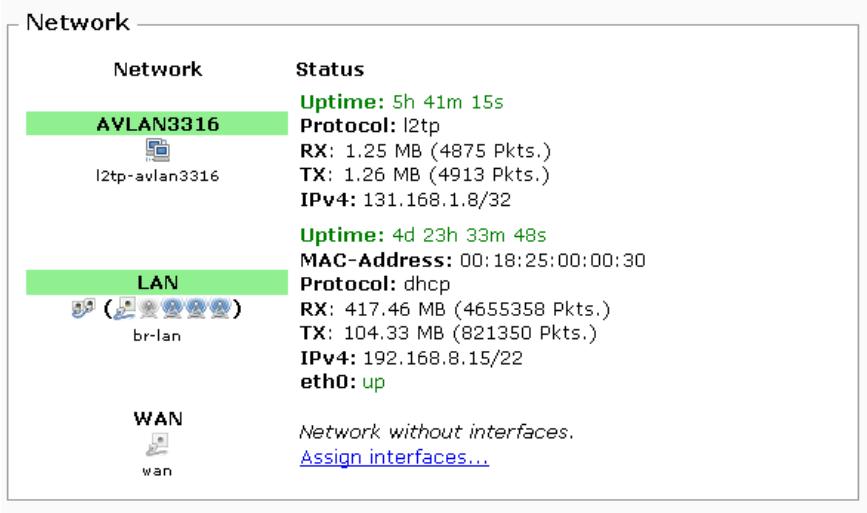


Figure 3-9: Status Overview Page, Network Section

The Network section displays the current status of the AVLAN3316 (l2tp), LAN, and WAN networks. It also displays status parameters for all configured VLANs (if applicable). The network's status parameters are:

- **Uptime**
- **MAC Address**: The MAC address of the network's interface. Not applicable for the l2tp (AVLAN3316) network.
- **Protocol**: The method used for setting the IP address (static or dhcp). For the AVLAN3316 interface the protocol is l2tp.
- **RX**: The accumulated numbers for received Bytes and Packets.
- **TX**: The accumulated numbers for transmitted Bytes and Packets.
- **IPv4**: The IP address and prefix mask.

The icons in parenthesis below the interface name provide indication regarding the Ethernet and wireless networks associated with the network:

The Ethernet icon ( ) provides a visible indication on the total number of Ethernet interfaces assigned to any network (In addition to eth0 assigned to either the LAN or the WAN zone, an Ethernet interface named eth0.<VLAN_ID> is assigned to any configured VLAN).

A wireless network icon ( ) is displayed for each wireless network assigned to the network.

Hover with the mouse over an icon to open an infotip with the name of the relevant Ethernet/wireless network it represents.

3.2.1.6 Wireless

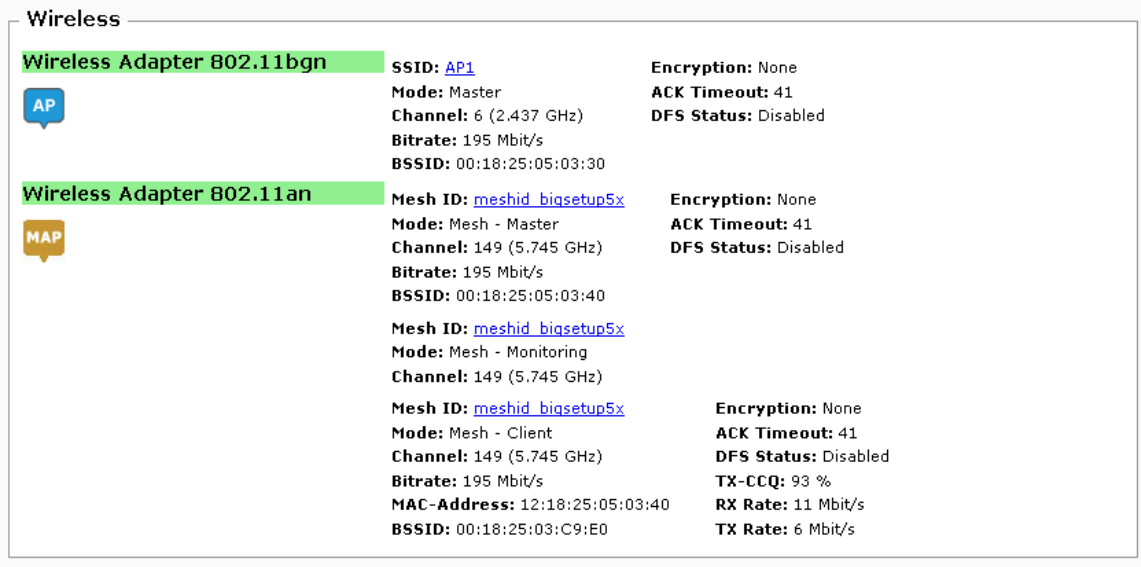


Figure 3-10: Status Overview Page, Wireless Section

A suitable icon on the left side indicates the mode/status of each of the available radio cards:

Table 3-1: Radio Operation Mode / Status

Icon	Description
	Regular Access Point
	Radio is disabled
	Mesh Root Access Point
	Mesh Access Point

For each of the available radio cards the following details for each of the configured wireless networks (SSIDs) are displayed:

INFORMATION

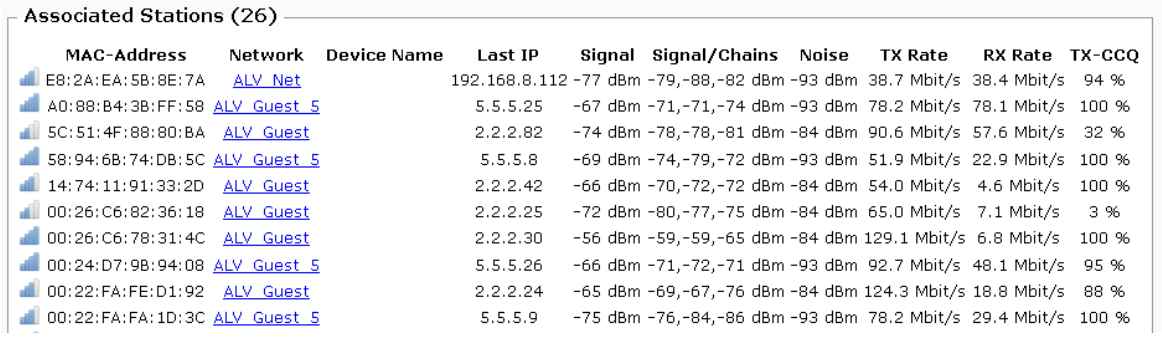
For more details on Wireless parameters refer to "Wireless Network Page" on page 77.

- **SSID / Mesh ID**: The name (Service Set IDentifier) of the wireless network. Click on the link to open the relevant Wireless Network configuration page.
- **Mode**: The operation mode of the wireless network.
- **Channel**: Shows the channel number and frequency that the AP is using.
- **Bitrate**: This is the maximum bitrate supported by the radio in the current configuration. Not applicable for a Mesh-Monitoring wireless network.
- **MAC-Address**: Applicable only for a Mesh-Client wireless network. The MAC address of the associated device.
- **BSSID**: The Basic Service Set IDentifier. Not applicable for a Mesh-Monitoring wireless network.
- **Encryption**: The wireless encryption mode being used for the wireless network. Not applicable for a Mesh-Monitoring wireless network.
- **ACK Timeout**: Shows the maximum acknowledgment time in microseconds (derived from the value configured for the Distance parameter). Not applicable for a Mesh-Monitoring wireless network.
- **DFS Status**: Indicates whether DFS (Dynamic Frequency Selection) is activated to properly support applicable regulations for the configured Regulatory Domain/Country (applicable only for the 5 GHz band). When DFS is enabled, the AP automatically switches channel if radar is detected on the current channel. Not applicable for a Mesh-Monitoring wireless network.
- **TX-CCQ**: The uplink transmission quality in % (a higher percentage means a better wireless connection quality). Applicable only for a Mesh-Client wireless network.

- **RX Rate**: The current receive bit rate in the uplink. Applicable only for a Mesh-Client wireless network.
- **TX Rate**: The current transmit bit rate in the uplink. Applicable only for a Mesh-Client wireless network.

3.2.1.7 Associated Stations

This section shows the following details for each of the end-user devices connected to the AP.



Associated Stations (26)

MAC-Address	Network	Device Name	Last IP	Signal	Signal/Chains	Noise	TX Rate	RX Rate	TX-CCQ
E8:2A:EA:5B:8E:7A	ALV_Net		192.168.8.112	-77 dBm	-79,-88,-82 dBm	-93 dBm	38.7 Mbit/s	38.4 Mbit/s	94 %
A0:88:B4:3B:FF:58	ALV_Guest_5		5.5.5.25	-67 dBm	-71,-71,-74 dBm	-93 dBm	78.2 Mbit/s	78.1 Mbit/s	100 %
5C:51:4F:88:80:BA	ALV_Guest		2.2.2.82	-74 dBm	-78,-78,-81 dBm	-84 dBm	90.6 Mbit/s	57.6 Mbit/s	32 %
58:94:6B:74:DB:5C	ALV_Guest_5		5.5.5.8	-69 dBm	-74,-79,-72 dBm	-93 dBm	51.9 Mbit/s	22.9 Mbit/s	100 %
14:74:11:91:33:2D	ALV_Guest		2.2.2.42	-66 dBm	-70,-72,-72 dBm	-84 dBm	54.0 Mbit/s	4.6 Mbit/s	100 %
00:26:C6:82:36:18	ALV_Guest		2.2.2.25	-72 dBm	-80,-77,-75 dBm	-84 dBm	65.0 Mbit/s	7.1 Mbit/s	3 %
00:26:C6:78:31:4C	ALV_Guest		2.2.2.30	-56 dBm	-59,-59,-65 dBm	-84 dBm	129.1 Mbit/s	6.8 Mbit/s	100 %
00:24:D7:9B:94:08	ALV_Guest_5		5.5.5.26	-66 dBm	-71,-72,-71 dBm	-93 dBm	92.7 Mbit/s	48.1 Mbit/s	95 %
00:22:FA:FE:D1:92	ALV_Guest		2.2.2.24	-65 dBm	-69,-67,-76 dBm	-84 dBm	124.3 Mbit/s	18.8 Mbit/s	88 %
00:22:FA:FA:1D:3C	ALV_Guest_5		5.5.5.9	-75 dBm	-76,-84,-86 dBm	-93 dBm	78.2 Mbit/s	29.4 Mbit/s	100 %

Figure 3-11: Status Overview Page, Associated Stations Section

- **MAC-Address**: Displays the MAC address of the station's radio.
- **Network**: States the name of the wireless network (SSID) to which the device is connected. You can click on the link to open the applicable page.
- **Device Name**: Shows the name of the station.
- **Last IP**: States the most recent IP address of the station as seen by the AP.
- **Signal**: The current total strength (in dBm) of the signal received from the station.
- **Signal/Chains**: The current strength of the signal received from the station per chain (the value of -95 dBm is taken to mean "no antenna").
- **Noise**: The current received noise level at the AP.
- **TX Rate**: The current transmit bit rate from the AP towards this station.
- **RX Rate**: The current receive bit rate at the AP from this station.
- **TX-CCQ**: The current transmission quality in % (a higher percentage means a better wireless connection quality).

The signal quality icon is displayed on the left side of each entry. Hover with the mouse over the icon to see the signal and noise levels.

If there are no associated stations, the text "No information available" is displayed.

3.2.1.8 DHCP Leases

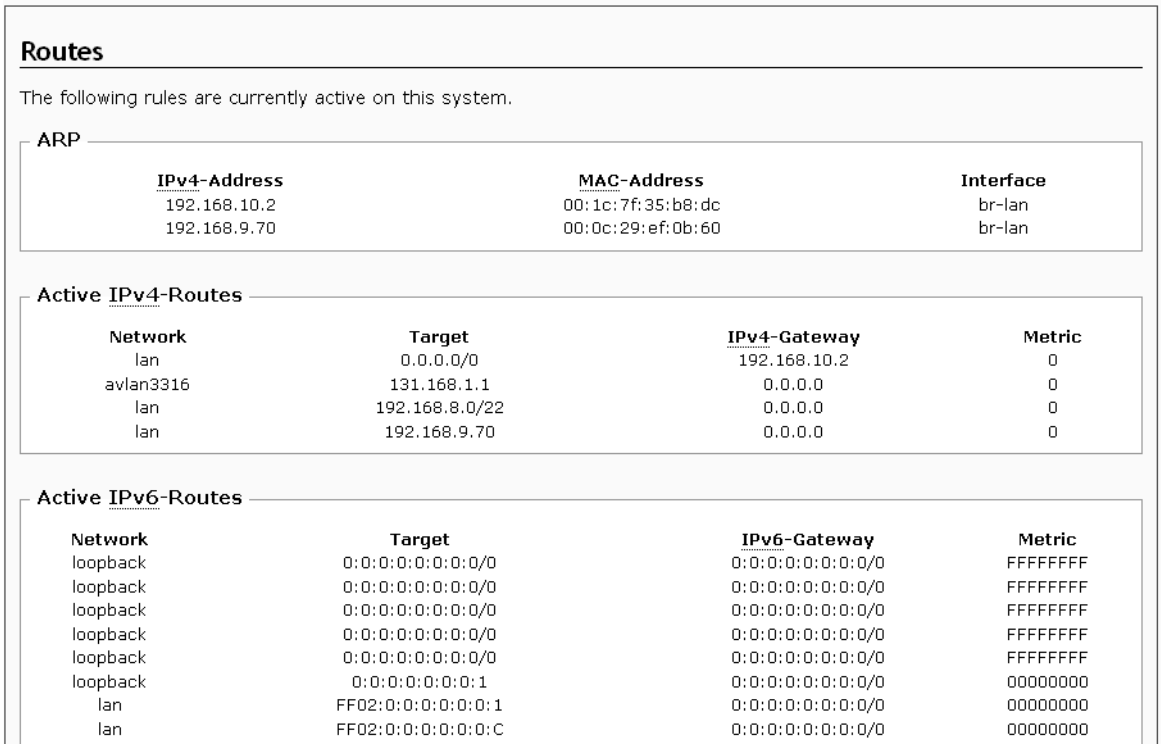
The **DHCP Leases** section shows the following details for each connected device with a DHCP leases (see "DHCP Server" on page 70 and "Static Leases" on page 72).

Figure 3-12: Status Overview Page, DHCP Leases Section

- **Hostname**: An optional symbolic name assigned to the device.
- **IPv4-Address**: The IP address assigned to the device.
- **MAC Address**: The device's MAC address.
- **Leasetime Remaining**: The remaining lease time.

3.2.2 Routes Page

To access the Routes page click on the **Status>Routes** tab in the management function selection panel.



Routes

The following rules are currently active on this system.

ARP

IPv4-Address	MAC-Address	Interface
192.168.10.2	00:1c:7f:35:b8:dc	br-lan
192.168.9.70	00:0c:29:ef:0b:60	br-lan

Active IPv4-Routes

Network	Target	IPv4-Gateway	Metric
lan	0.0.0.0/0	192.168.10.2	0
avlan3316	131.168.1.1	0.0.0.0	0
lan	192.168.8.0/22	0.0.0.0	0
lan	192.168.9.70	0.0.0.0	0

Active IPv6-Routes

Network	Target	IPv6-Gateway	Metric
loopback	0:0:0:0:0:0:0:0/0	0:0:0:0:0:0:0:0/0	FFFFFFFF
loopback	0:0:0:0:0:0:0:0/0	0:0:0:0:0:0:0:0/0	FFFFFFFF
loopback	0:0:0:0:0:0:0:0/0	0:0:0:0:0:0:0:0/0	FFFFFFFF
loopback	0:0:0:0:0:0:0:0/0	0:0:0:0:0:0:0:0/0	FFFFFFFF
loopback	0:0:0:0:0:0:0:0/0	0:0:0:0:0:0:0:0/0	FFFFFFFF
loopback	0:0:0:0:0:0:0:1	0:0:0:0:0:0:0:0/0	00000000
lan	FF02:0:0:0:0:0:0:1	0:0:0:0:0:0:0:0/0	00000000
lan	FF02:0:0:0:0:0:0:C	0:0:0:0:0:0:0:0/0	00000000

Figure 3-13: Status Routes Page

The Status Routes page displays the routing rules that are currently active on the device:

- **ARP**: The Address Resolution Protocol (ARP) table displays the IP address and corresponding MAC address and interface of each device on the network.

- **Active IPv4-Routes**: This table displays the Network, Target (Network ID), IPv4-Gateway and Metric for each active subnet.
- **Active IPv6-Routes**: This table displays the Network, Target (Network ID), IPv6-Gateway and Metric for each active subnet.

3.2.3 System Log Page

To access the Status System Log page click on the **Status>System Log** tab in the management function selection panel.

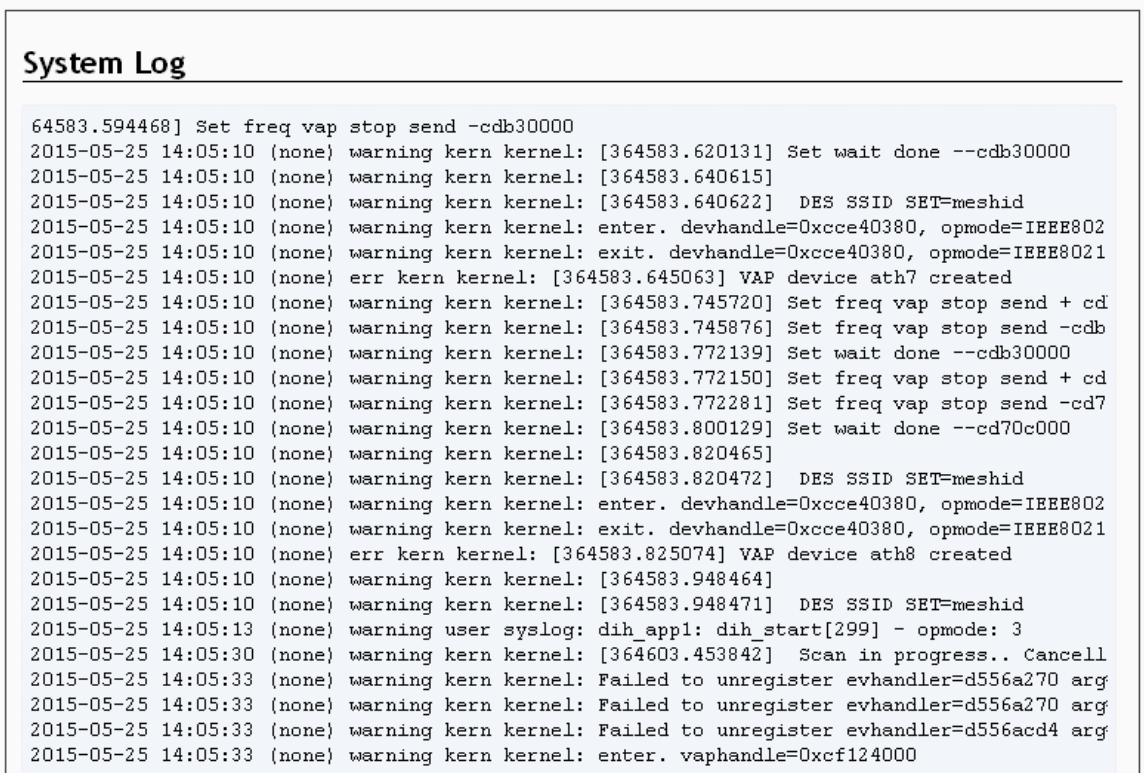


Figure 3-14: Status System Log Page

The System Log page displays the last reported system events.

3.2.4 Realtime Graphs Pages

To access the Realtime Graphs pages click on the **Status>Realtime Graphs** tab in the management function selection panel.

The following pages are available for the **Status Realtime Graphs** option:

- Load Page
- Traffic Page

- Wireless Page
- Connections Page

All graphs display the applicable real time data in a sliding time window (starting with data from the last minute) using 3 seconds intervals. The size in minutes of the sliding window depends on screen resolution and window size.

Below the table the Current, Average and Peak values for applicable items are displayed. Average and Peak values are calculated for the elapsed time since starting to display the graph.

Labels for colors of displayed graphs are provided as underlines for the applicable items below each graph.

3.2.4.1 Load Page

To access the Load page click on the **Status>Realtime Graphs>Load** tab in the management function selection panel.

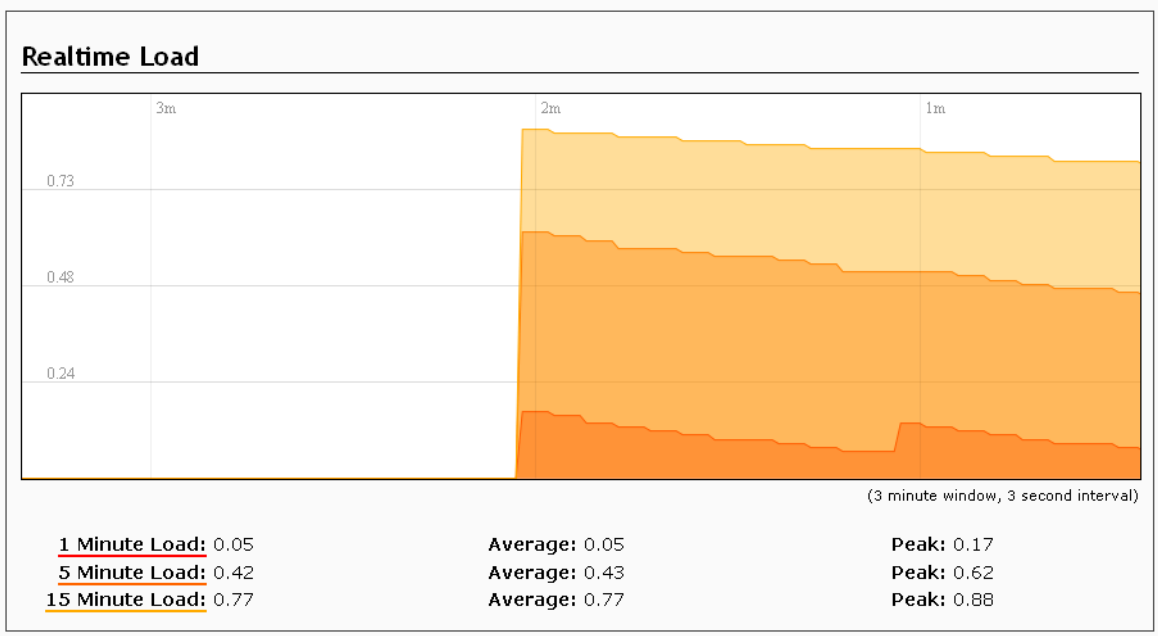


Figure 3-15: Status Realtime Graphs, Load Page

The Realtime Load page displays the graphs for the average CPU loads during the last1 Minute, 5 Minutes and 15 Minutes.

3.2.4.2 Traffic Page

To access the Traffic page click on the **Status>Realtime Graphs>Traffic** tab in the management function selection panel.

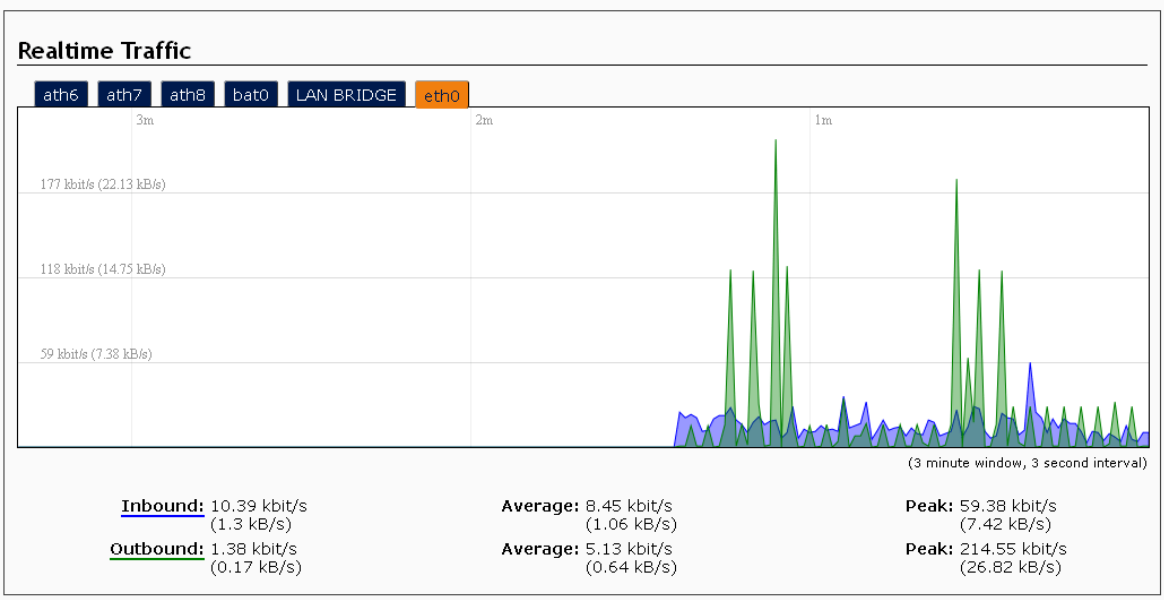


Figure 3-16: Status Realtime Graphs, Traffic Page

The Realtime Traffic page includes several tabs, one for each of the available physical and logical interfaces.

For each interface, the Realtime Traffic graphs display the realtime Inbound and Outbound traffic in bits/s and in bytes/s.

3.2.4.3 Wireless Page

To access the Wireless page click on the **Status>Realtime Graphs>Wireless** tab in the management function selection panel.

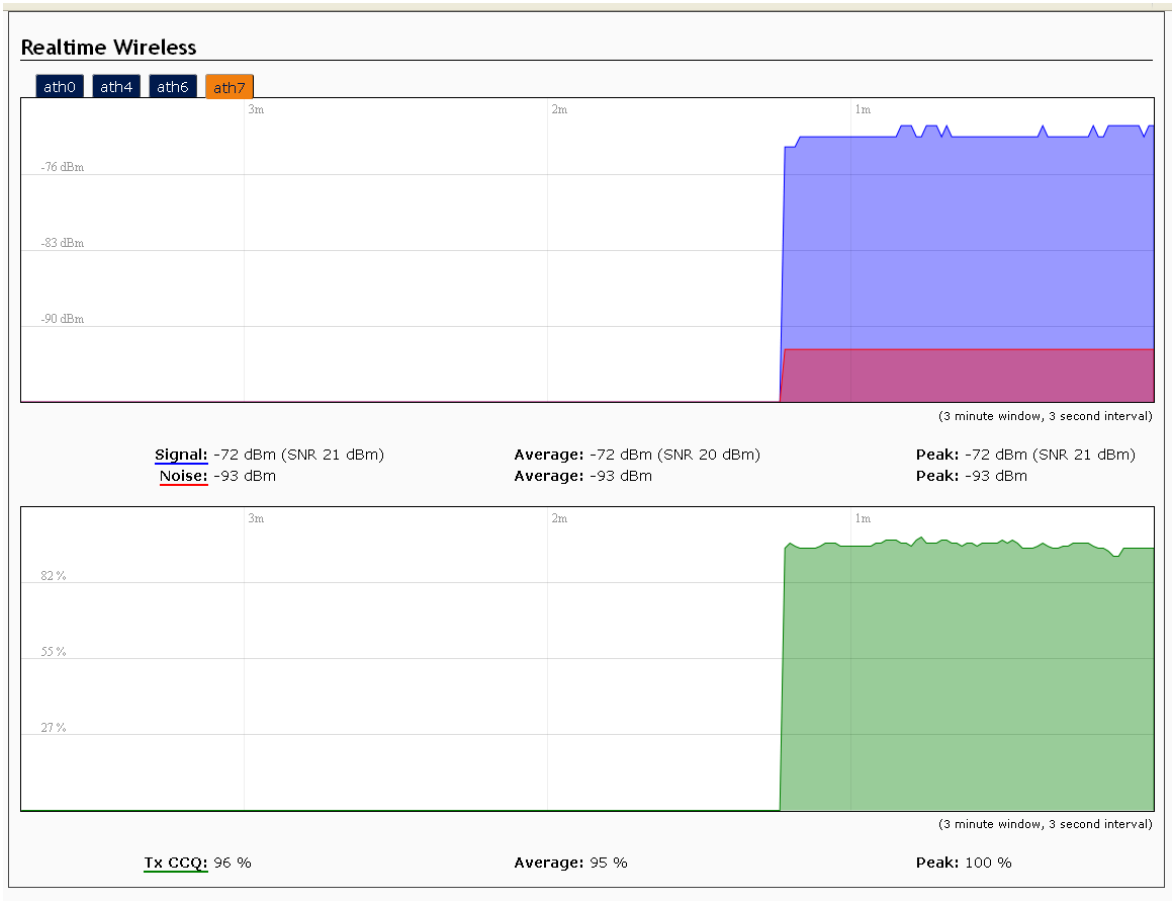


Figure 3-17: Status Realtime Graphs, Wireless Page

The Realtime Wireless page may include one or several tabs, one for each of the available wireless networks.

For each wireless network, there are two types of real time graphs:

- Signal and Noise Graph: Display the realtime Signal and Noise levels (in dBm).
- Tx CCQ Graph: Display the realtime Tx CCQ (the transmission quality in %).

3.2.4.4 Connections Page

To access the Connections page click on the **Status>Realtime Graphs>Connections** tab in the management function selection panel.

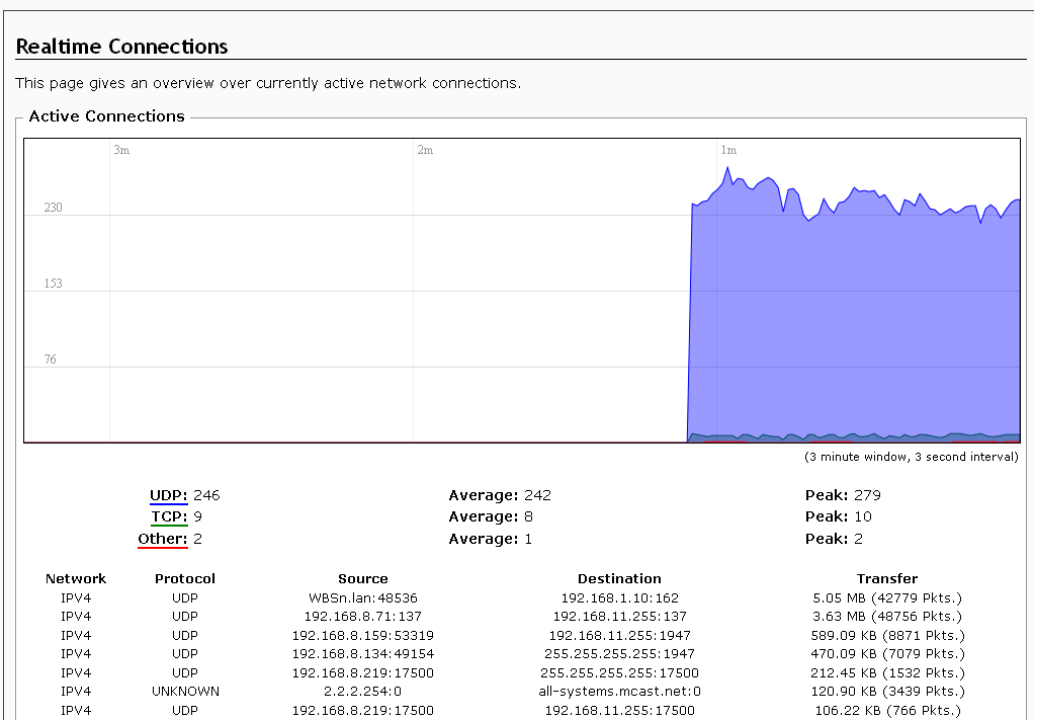


Figure 3-18: Status Realtime Graphs, Connections Page

The Realtime Connections page displays the graphs for the numbers of currently active connections using UDP, TCP or Other (UNKNOWN + ICMP) protocols.

In addition, below the graph there is a table providing the following details for each connection:

- **Network:** Internet Protocol.
- **Protocol**: Type of protocol (UDP, TCP, ICMP or UNKNOWN).
- **Source**: Source address and port.
- **Destination**: Destination address and port.
- **Transfer**: Transferred traffic in Bytes and in Packets.

3.2.5 Hotspot Users Page

To access the Hotspot page click on the **Status>Hotspot Users** tab in the management function selection panel.

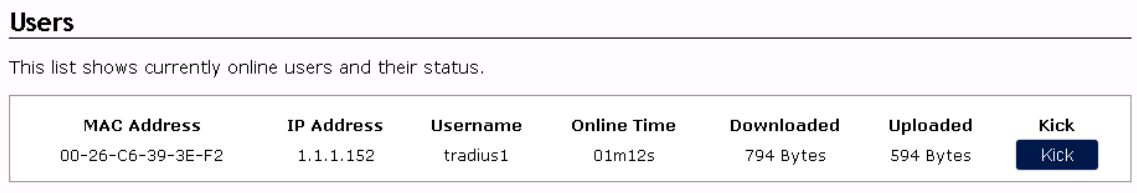


Figure 3-19: Status Hotspot Users Page

The Hotspot Users page provides the following details for each of the currently connected hotspot users (if applicable):

- **MAC Address**
- **IP Address**
- **Username**
- **Online Time**: Total amount of time used by the user in the current session.
- **Downloaded**: Total amount of data downloaded by the user in the current session.
- **Uploaded**: Total amount of data uploaded by the user in the current session.

Click on the **Kick** button on the right side of an online user's entry to disconnect the active session and force the user to login again.

3.3 System

The System option provides access to the following pages:

- System Page
- Administration Page
- Services Page
- SNMP Page
- Backup / Flash Firmware Page
- Reboot Page
- Diagnostics Page

3.3.1 System Page

To access the System page click on the **System>System** tab in the management function selection panel.

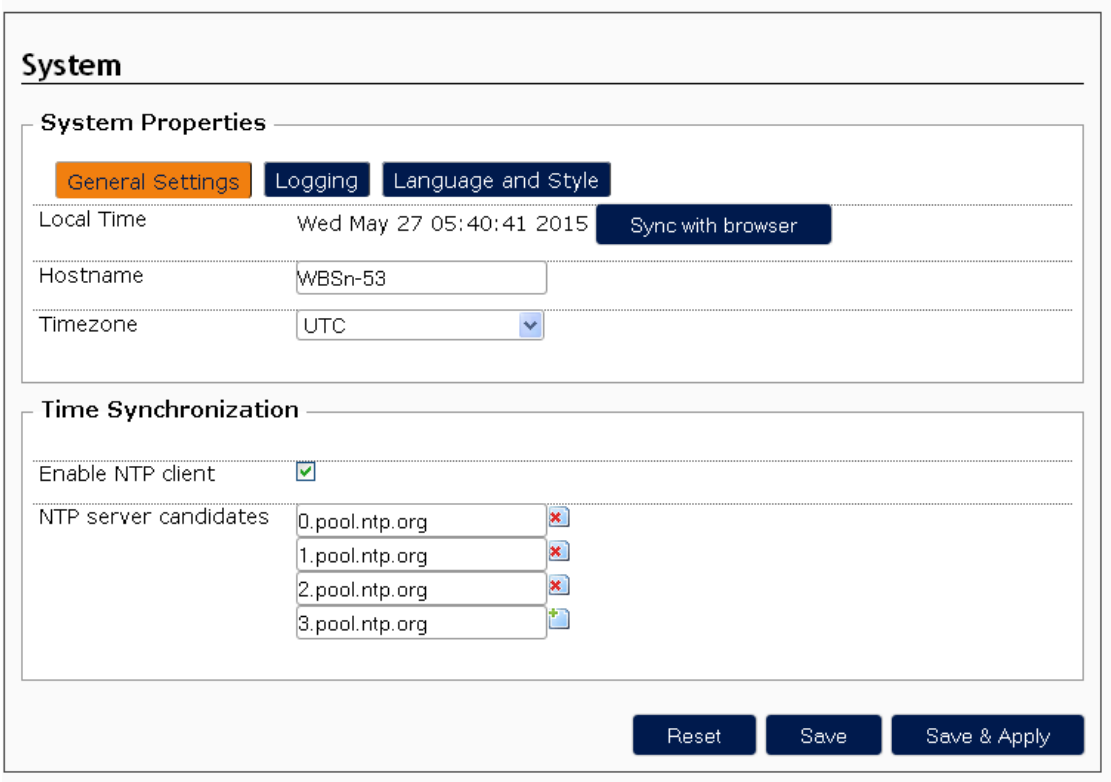


Figure 3-20: System System Page

The System page includes the following sections:

- System Properties
- Time Synchronization

3.3.1.1 System Properties

The following tabs are available in the System Properties section:

- General Settings
- Logging
- Language and Style

3.3.1.1.1 General Settings

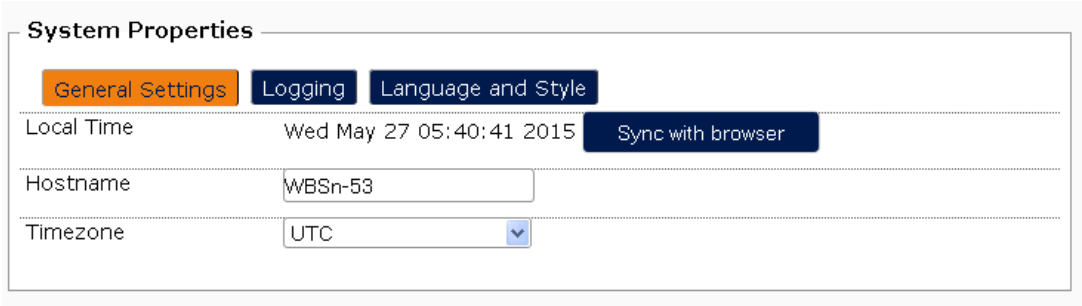


Figure 3-21: System System Page, System Properties Section, General Settings Tab

The General Settings tab includes the following:

- **Local Time**: The current read-only date and time of the unit's real time clock. To synchronize with the date and time of your PC click on the **Sync with browser** button.
- **Hostname**: The device's name.
- **Timezone**: The appropriate time zone for the geographical location of the unit.

For more details on date and time settings see "Time Synchronization" on page 43.

3.3.1.1.2 Logging

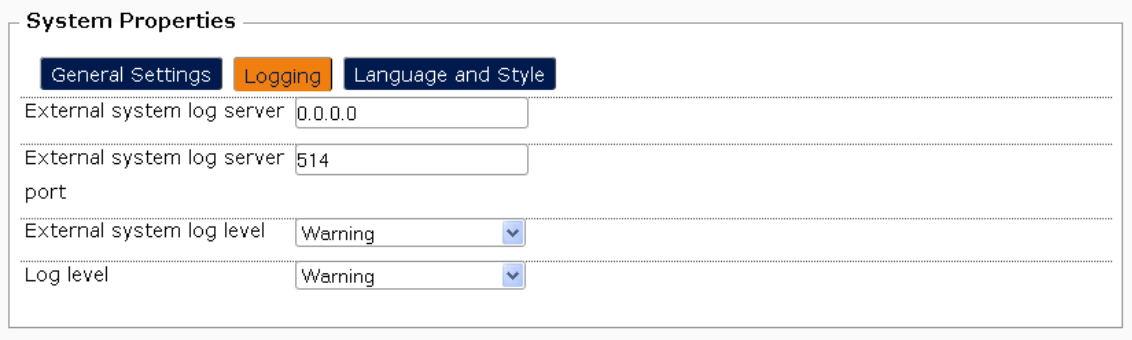


Figure 3-22: System System Page, System Properties Section, Logging Tab

The Logging tab includes the following parameters used for managing system's events log:

- **External system log server**: The IP address of the external log server to which relevant events will be transferred.
- **External system log server port**: The port to be used for communicating with the external log server (default is 514).
- **External system log level**: The minimal severity level of events to be sent to the external log server. Only events with a severity level identical to or higher than the specified level will be transferred. The levels available in the drop-down list are Debug / Info / Notice / Warning / Error/ Critical / Alert / Emergency. The default is Warning.
- **Log level**: The minimal severity level of events to be recorded in the events log of the device (see "System Log Page" on page 34). Only events with a severity level identical to or higher than the specified level will be recorded. The levels available in the drop-down list are Debug / Info / Notice / Warning / Error/ Critical / Alert / Emergency. The default is Warning.

3.3.1.1.3 Language and Style

Figure 3-23: System System Page, System Properties Section, Language and Style Tab

In the current release only the English language is supported for the web pages.

3.3.1.2 Time Synchronization

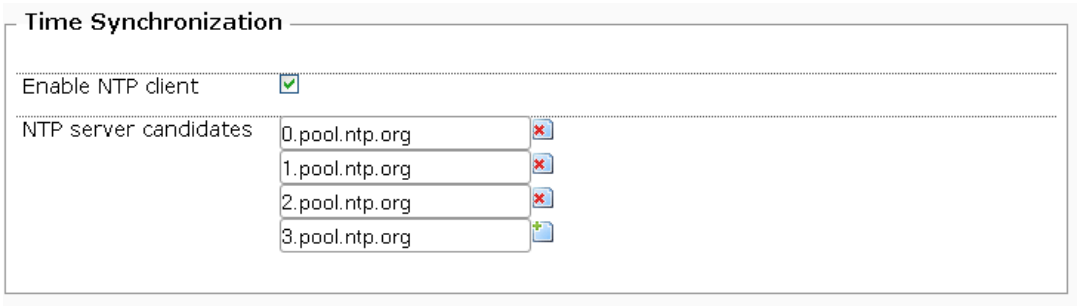


Figure 3-24: System System Page, Time Synchronization Section

Automatic settings of the system's real-time clock is based on using NTP (Network Time Protocol) for acquiring the date and time from an NTP time server.

The Time Synchronization section includes the following parameters:

- **Enable NTP client**: Enables selection of whether to use an NTP time server for setting the device's date and time.
- **NTP server candidates**: Available only if operation as an NTP client is enabled. Enable specifying names (or IP addresses) of NTP servers (or servers pools). By default 4 popular servers pools (0.pool.ntp.org, 1.pool.ntp.org, 2.pool.ntp.org, 3.pool.ntp.org) are configured.

The time provided by a time server is always UTC (Coordinated Universal Time). You should properly configure the Timezone parameter (see "General Settings" on page 41 above) to adjust the real-time clock to local time.

Note that GMT (Greenwich Mean Time) is an absolute reference time and does not change with the seasons. You can change the Timezone parameter for adjusting the real-time clock in accordance with local daylight saving changes.

3.3.2 Administration Page

To access the Administration page click on the **System>Administration** tab in the management function selection panel.

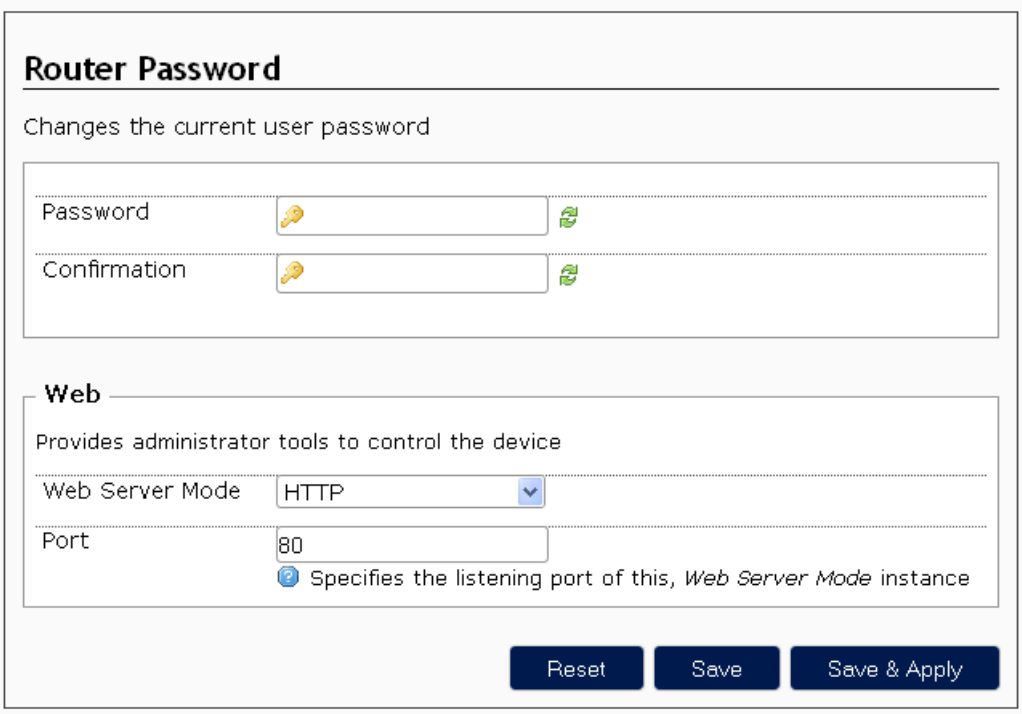


Figure 3-25: System Administration Page

The Administration page includes the following sections:

- Router Password
- Web

3.3.2.1 Router Password

In the Router Password section you can change the login password. Enter the new password in the Password text field and enter it again in the Confirmation text field. You can click on the **Reveal/hide password** icon ( ) on the right side of each field to hide (the default) or reveal the typed string.

3.3.2.2 Web

- **Web Server Mode**: This can be set to HTTP (Hypertext Transfer Protocol) or HTTPS (Hypertext Transfer Protocol Secure. The default is HTTP.
- **Port**: Specifies the listening port, the default being 80 for HTTP and 443 for HTTPS.

3.3.3 Services Page

To access the System Services page click on the **System>Services** tab in the management function selection panel.

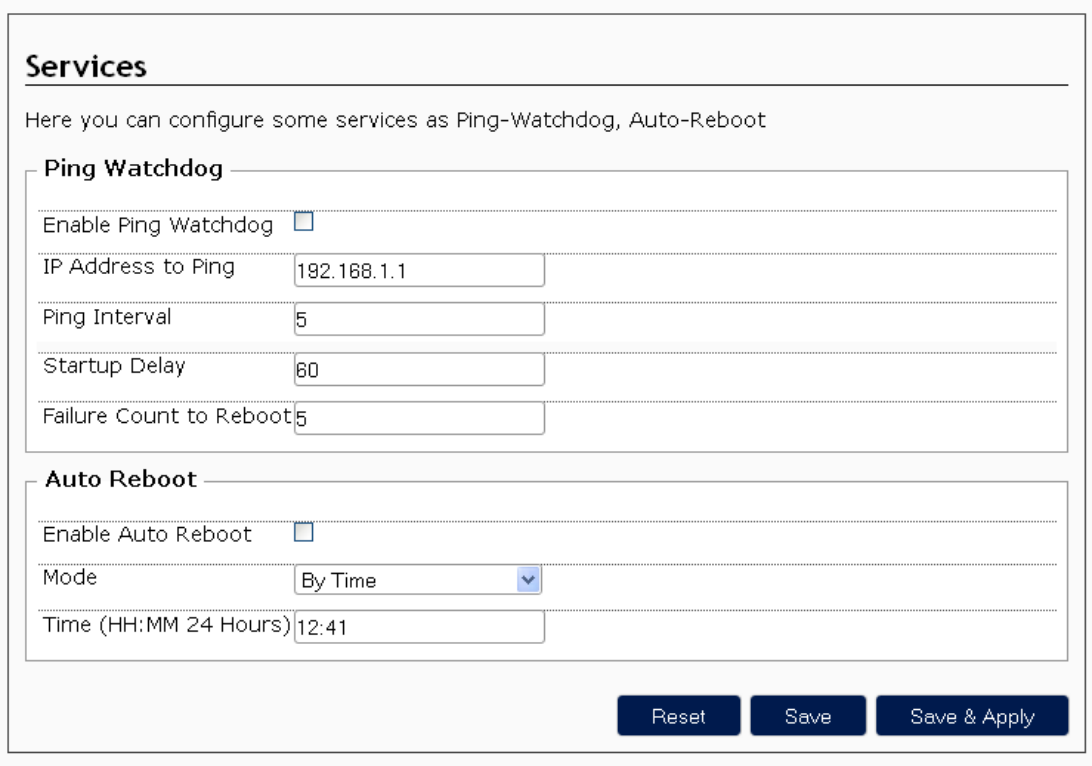


Figure 3-26: System Services Page

The Services page includes the following sections:

- Ping Watchdog
- Auto Reboot

3.3.3.1 Ping Watchdog

The ping watchdog service enables performing an on-going health check by monitoring connectivity to a certain address. The system will reboot if a certain number of subsequent pings to the given IP address will fail.

The Ping Watchdog section includes the following parameters:

- **Enable Ping Watchdog**: Select to enable the Ping Watchdog service. The default is disabled (de-selected).
- **IP Address to Ping**: Sets the remote IP address to ping.
- **Ping Interval**: Specifies the time between successive pings, the default being 5 seconds.
- **Startup Delay**: Sets the time delay after the device finishes rebooting, before running the Ping Watchdog. The default is 60 seconds.
- **Failure Count to Reboot**: Specifies the number of failed pings before the device reboots automatically.

3.3.3.2 Auto Reboot

The Auto Reboot service enables configuring scheduled automatic reboot of the device. The Auto Reboot section includes the following parameters:

- **Enable Auto Reboot**: Select to enable the Auto Reboot service. The default is disabled (de-selected).
- **Mode**: Chooses the Auto Reboot mode By Time of day or By Number of Hours.
- **Time (HH:MM 24 Hours)**: Available only if selected Mode is By Time. Sets the time of day to reboot.
- **Number of Hours**: Available only if selected Mode is By Number of Hours. Sets the number of hours between periodical auto reboots. The default is 24 hours.

3.3.4 SNMP Page

To access the SNMP page click on the **System>SNMP** tab in the management function selection panel.

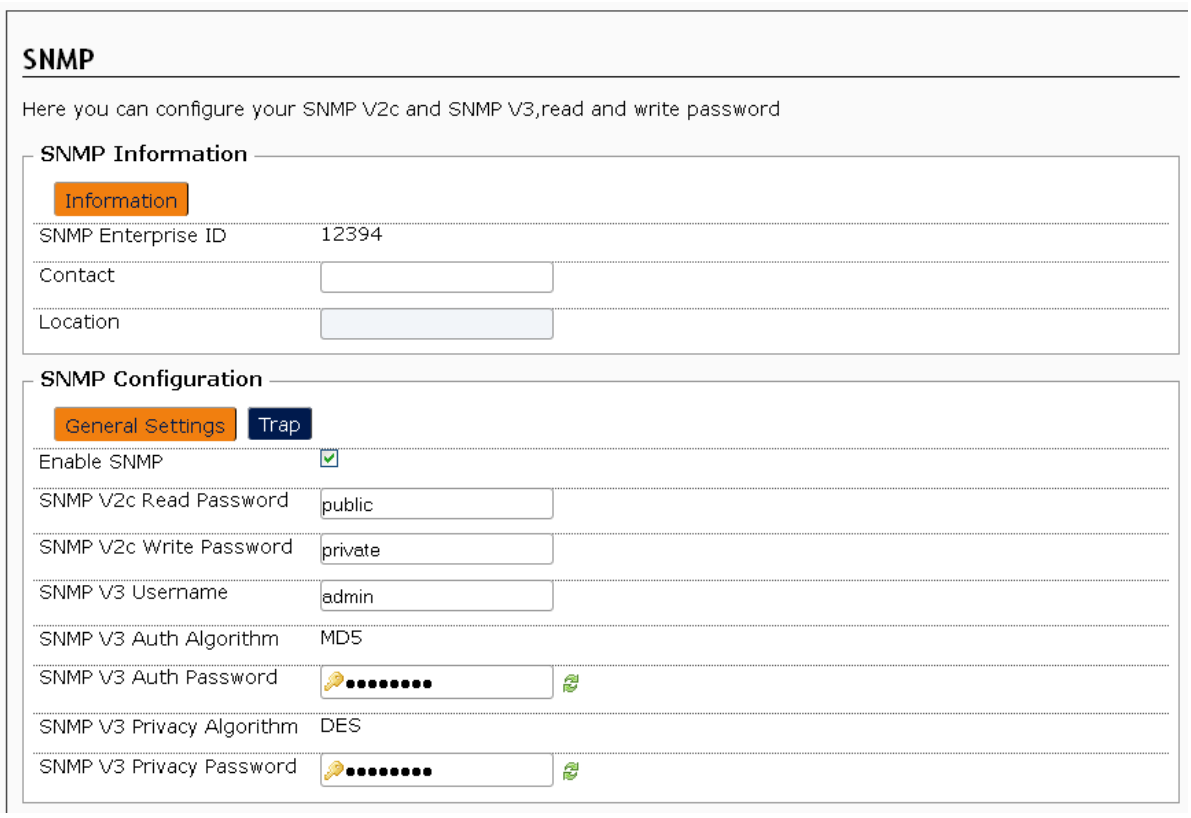


Figure 3-27: System SNMP Page

The SNMP page includes the following sections:

- SNMP Information
- SNMP Configuration

3.3.4.1 SNMP Information

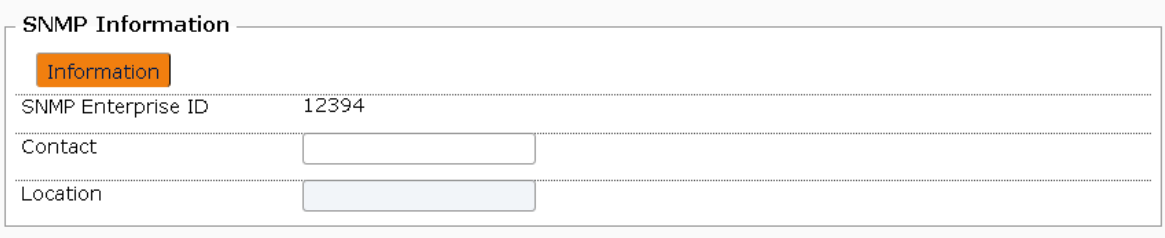


Figure 3-28: System SNMP Page, SNMP Information Section

The SNMP Information section includes the following general SNMP parameters:

- **SNMP Enterprise ID**: The read-only SNMP Enterprise ID.
- **Contact**: The system contact (sysContact) string.
- **Location**: The system location (sysLocation) string.

3.3.4.2 SNMP Configuration

The following tabs are available in the SNMP Configuration section:

- General Settings
- Trap

3.3.4.2.1 General Settings

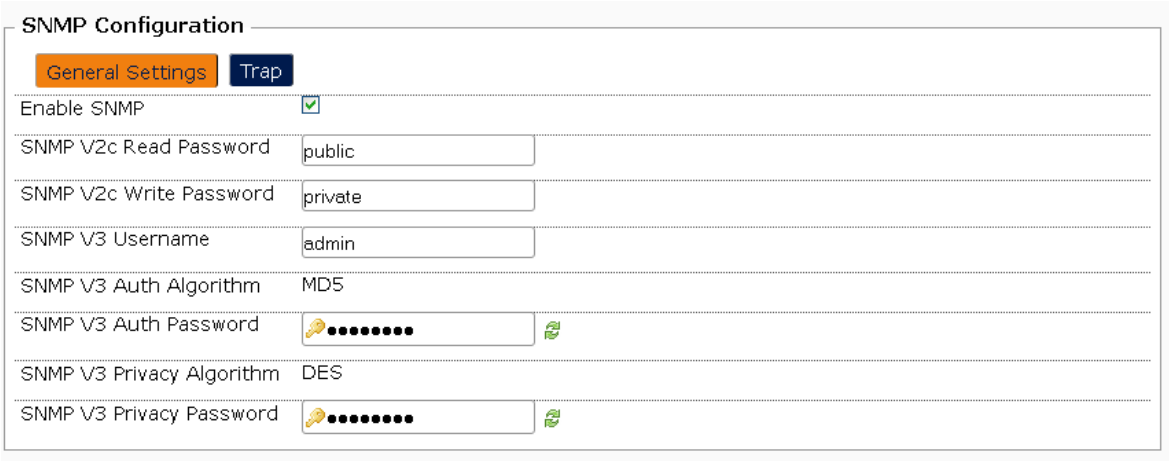


Figure 3-29: System SNMP Page, SNMP Configuration Section, General Settings Tab

The SNMP Configuration General Settings tab includes the following parameters:

- **Enable SNMP**: Select (the default) to enable management using SNMP.

- **SNMP V2c Read Password**: The SNMPv2c community string used for read (get) operations. The default is public.
- **SNMP V2c Write Password**: The community string used for write (put) operations. Can also be used for read (get) operations. The default is private.
- **SNMP V3 Username**: The name assigned to the SNMPv3 user for authentication purposes. The default is admin.
- **SNMP V3 Auth Algorithm**: Read-only. The authentication algorithm used, e.g., MD5.
- **SNMP V3 Auth Password**: The password for user authentication (default: password). You can click on the **Reveal/hide password** icon ( ) on the right side to hide (the default) or reveal the typed string.
- **SNMP V3 Privacy Algorithm**: Read-only. The data encryption algorithm used, e.g., DES.
- **SNMP V3 Privacy Password**: The password for data encryption (default: password). You can click on the **Reveal/hide password** icon ( ) on the right side to hide (the default) or reveal the typed string.

3.3.4.2.2 Trap

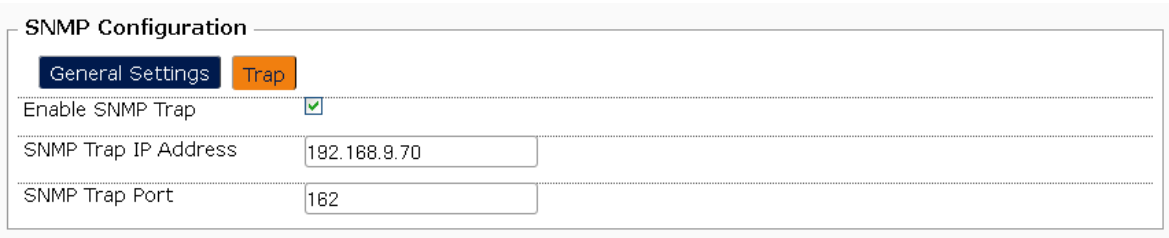


Figure 3-30: System SNMP Page, SNMP Configuration Section, Trap Tab

The Trap tab includes the following parameters:

- **Enable SNMP Trap**: Select (the default) to enable the SNMP agent to send events notifications to the SNMP Trap manager.
- **SNMP Trap IP Address**: The IP address of the SNMP Trap manager which receives the trap messages.
- **SNMP Trap Port**: The SNMP Traps port number (default is 162).

3.3.5 Backup / Flash Firmware Page

To access the Backup / Flash Firmware page click on the **System>Backup / Flash Firmware** tab in the management function selection panel.

The Backup / Flash Firmware page includes the following sections:

- Backup / Restore
- Flash new firmware

- Firmware Banks

3.3.5.1 Backup / Restore

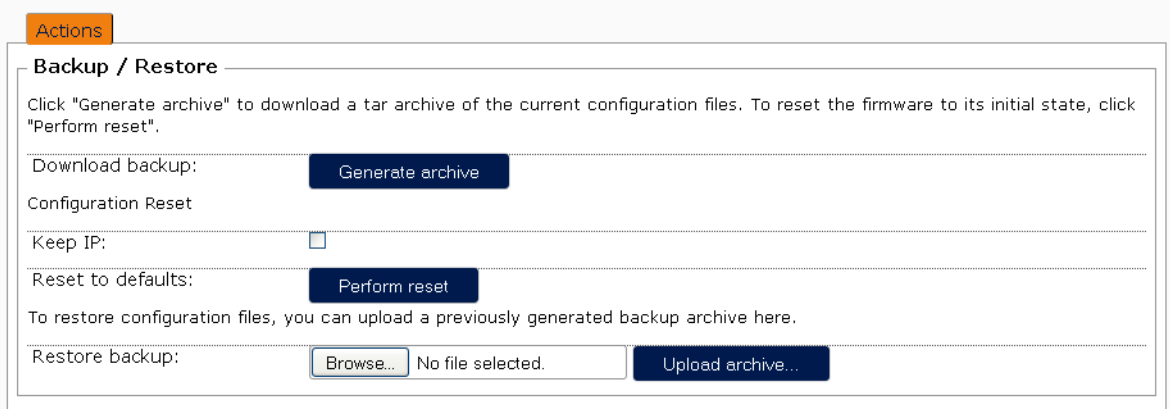


Figure 3-31: System Backup / Flash Firmware Page, Backup / Restore Section

In the Backup / Restore section you can execute the following actions related to management of configuration files:

- Saving the current configuration file
- Restoring the factory default configuration
- Restoring a previously saved configuration file

3.3.5.1.1 Saving the current configuration file

To generate and download a tar archive of the current configuration files:

Click on the **Generate archive** button.

The backup file will be downloaded to your PC (either to the Downloads directory or to a selectable location - depending on the browser used). The default file name is “backup-AP-<Date>.tar”.

3.3.5.1.2 Restoring the factory default configuration

To revert to the factory default configuration:

Click on the **Perform reset** button.

A confirmation request message will be displayed. After confirmation the device will reboot and restart running with the default configuration.

CAUTION

If the **Keep IP** checkbox is unchecked (the default), then after the device reverts to the factory default configuration (including management IP parameters and other parameters related to management) you may loose the ability to remotely manage the device.

Check the **Keep IP** checkbox before clicking on the **Perform reset** button to revert to the factory default configuration excluding parameters required for maintaining remote management connectivity.

3.3.5.1.3 Restoring a previously saved configuration file

To restore a previously saved backup file:

1. Click on the **Browse** button and navigate to the location of the required backup file.
2. The path to the selected file will be displayed next to the Browse button.
3. Click on the **Upload archive...** button. You will be requested to confirm the action.

After confirmation the system will upload the backup file and reboot. After reboot the uploaded backup file will be used as the running configuration file.

3.3.5.2 Flash new firmware

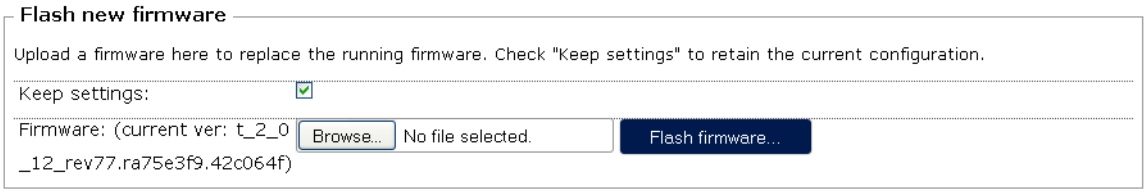


Figure 3-32: System Backup / Flash Firmware Page, Flash new firmware Section

In the Flash new firmware section you can upload a new firmware file that will be used as the running version.

To upload a new firmware file:

1. Verify that the required file is available on your PC.
2. Click on the **Browse** button and navigate to the location of the required firmware file.
3. The path to the selected file will be displayed next to the Browse button.
4. Click on the **Flash firmware...** button. You will be requested to confirm the action.

After confirmation the system will upload the firmware file and reboot. After reboot the uploaded firmware file will be used as the running firmware file.

CAUTION

Check (the default) the **Keep settings** checkbox to save the previous configuration and continue using it after switching to the new firmware version. If **Keep settings** is unchecked, the new firmware will start running using the factory default configuration. In this case you may loose the ability to remotely manage the device.

3.3.5.3 Firmware Banks

Figure 3-33: System Backup / Flash Firmware Page, Firmware Banks Section

In the Firmware Banks section you can switch to the previous firmware version:

Each firmware has its own configuration file. After a firmware upgrade procedure is performed, a new configuration file is included in the upgrade. This configuration file will adopt the current configuration settings once the newly upgraded firmware is run. The new configuration file may contain new features that could modify current configurations. Also, even if no new features are included in the upgrade, but new configurations were specified by the user, a newer version of the configuration file is created.

If you wish to revert back to the previous firmware and keep using the new configuration file (excluding parameters that are not supported by the previous firmware), click on the **Switch Bank** button. After reboot the device will run using the previous firmware and the new configuration file.

If you wish to revert back to the previous firmware and the previous configuration file, you need to perform a rollback procedure by clicking on the **Rollback** button. After reboot the device will run using the previous firmware and the previous configuration file.

3.3.6 Reboot Page

To access the Reboot page click on the **System>Reboot** tab in the management function selection panel.

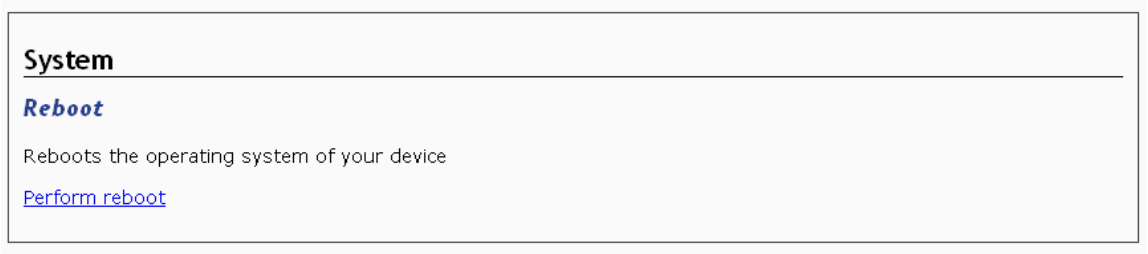


Figure 3-34: System Reboot Page

Click on the **Perform reboot** link to reboot the device. This is similar to a power-off / power-on cycle. The system configuration remains the same. However, changes that were not applied (using the **Save & Apply** button) will be lost. If there are any such changes, a suitable warning message will be displayed.

3.3.7 Diagnostics Page

To access the System Diagnostics page click on the **System>Diagnostics** tab in the management function selection panel.

Figure 3-35: System Diagnostics Page

The Diagnostics page enables preparing diagnostics compressed TAR files (tar.gz) that may be sent to the support team of the supplier for advice on solving problems.

Click on the **Tech Support** button to create and save a compressed TAR file with detailed information regarding current configuration and possible problems.

Click on the **KPI files** button to create and save a compressed TAR file with detailed information on KPI (Key Performance Indicators).

The file's name includes information on file's type (TechSupport/KPI), device's name and date and time at which the file was created.

3.4 Services

The Services tab provides access to the following:

- Hotspot Service Pages
- Discovery Page

3.4.1 Hotspot Service Pages

The Hotspot service allows you to control the access and usage of the Internet by connected devices.

This section includes:

- Introduction to Hotspot Services
- Hotspot General Settings Page
- Hotspot Network Page
- Hotspot RADIUS Page
- Hotspot Authentication Page
- User's Configuration Page

3.4.1.1 Introduction to Hotspot Services

The following subsections contain guidelines on how to configure the device to implement hotspot services. It is recommended to configure the LAN, Wifi, and WAN, then test it before enabling the hotspot setting:

- WAN/LAN Interfaces
- Wifi Settings
- Test Internet Connection
- Setting up the Hotspot

3.4.1.1.1 WAN/LAN Interfaces

To support Hotspot services configure the device to operate in Router mode. Refer to "Switching from Bridge Mode to Router Mode and Vice Versa" on page 64.

3.4.1.1.2 Wifi Settings

The wireless networks that should be available for hotspot services should be set up to allow any user to access the Internet, assuming that the hotspot is not yet enabled. This means:

- ESSID should not be hidden (see **Hide ESSID** in "General Setup" on page 80).
- **Wireless Security** mode should be set to No Encryption (see "Wireless Security" on page 82).

3.4.1.1.3 Test Internet Connection

At this point, before setting up the hotspot, it is recommended to test the Internet connection by connecting a mobile phone or any other device to a wireless network in the LAN zone of the hotspot AP and use a browser to perform an Internet search. If search results are returned, this means that the Internet connection is working fine.

3.4.1.1.4 Setting up the Hotspot

The hotspot can now be set up and enabled. The following sections describe the Hotspot settings available in the AP's web pages.

3.4.1.2 Hotspot General Settings Page

To access the Hotspot General Settings page click on the **Services>Hotspot** tab in the management function selection panel.

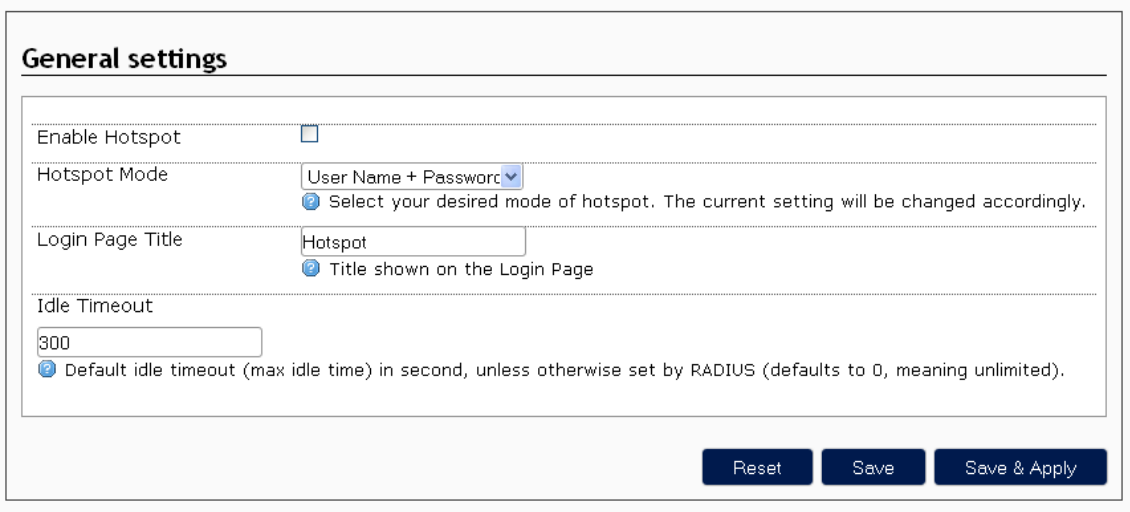


Figure 3-36: Hotspot General Settings Page

The Hotspot General Settings page includes the following parameters:

- **Enable Hotspot**: Select to activate the hotspot service. It is recommended to enable the hotspot service after competing all necessary settings as described in "Introduction to Hotspot Services" on page 53.

- **Hotspot Mode**: Selects your required mode of hotspot. You can choose to use the hotspot together with a third party or external RADIUS authentication server. The available options are:
  - » User Name + Password (Radius Required)
  - » Agreement (Radius Required)
  - » Password (Radius Required)
  - » Agreement (Radius not Required)
  - » Password (Radius not Required)
- **Password**: Available only if selected mode is Password (Radius not Required). The password to be used for allowing access to the Internet. You can click on the **Reveal/hide password** icon ( ) on the right side to hide (the default) or reveal the typed string.
- **Login Page Title**: Sets the title shown on the Login Page, e.g., **HotSpot**.
- **Idle Timeout**: The timeout in seconds before disconnecting non-active users (unless otherwise set by the RADIUS server). A value of 0 means unlimited time. The default is 300 seconds.

3.4.1.3 Hotspot Network Page

To access the Hotspot Network page click on the **Services>Hotspot>Network** tab in the management function selection panel.

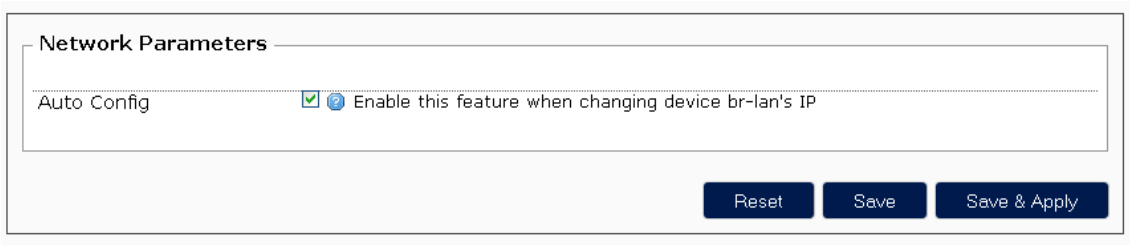


Figure 3-37: Hotspot Network Page (Auto Config Enabled)

- **Auto Config**: When enabled (the default), Network Address and DNS Server will be configured automatically based on the settings in the LAN page. Disable only when you want to manually modify these settings. Auto Config should be enabled prior to modifying the IP parameters of the LAN interface.

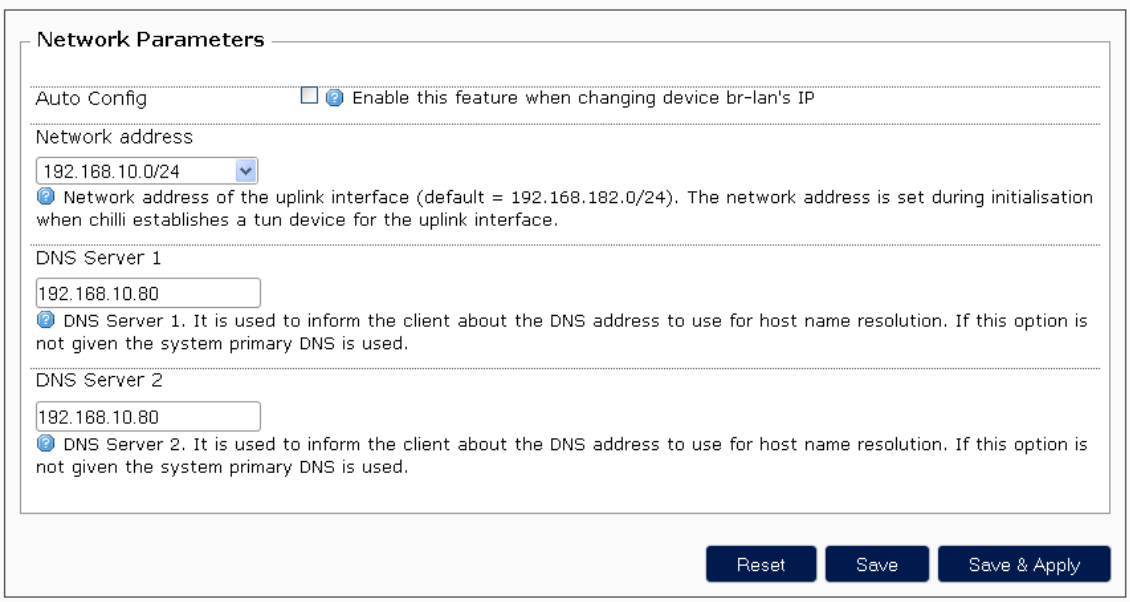


Figure 3-38: Hotspot Network Page (Auto Config Disabled)

The parameters that become available when Auto Config is disabled are:

- Network Address: The default address and netmask prefix are derived from the network address of the LAN interface.
- **DNS Server 1** and **DNS Server 2**: The default for both is the management IP address of the AP.

3.4.1.4 Hotspot RADIUS Page

To access the Hotspot RADIUS page click on the **Services>Hotspot>RADIUS** tab in the management function selection panel.

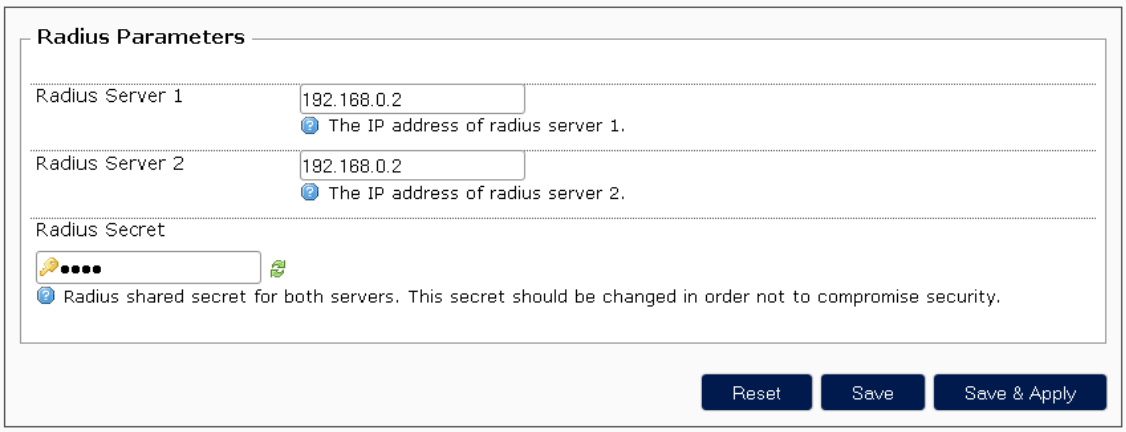


Figure 3-39: Hotspot RADIUS Page

The RADIUS Parameters page is applicable only if Hotspot Mode is set to an option where a RADIUS server is required (see **Hotspot Mode** in "Hotspot General Settings Page" on page 54). It includes the following parameters:

- **Radius Server 1**: The IP address of the primary RADIUS server.
- **Radius Server 2**: The IP address of the secondary RADIUS server.
- **Radius Secret**: The Radius shared secret for both servers. You can click on the **Reveal/hide password** icon ( ) on the right side to hide (the default) or reveal the typed string.

3.4.1.5 Hotspot Authentication Page

To access the Hotspot Authentication page click on the **Services>Hotspot>Authentication** tab in the management function selection panel.

Figure 3-40: Hotspot Authentication Page

Here you can set the Universal Access Method (UAM) parameters.

- **UAM Server**: Sets the URL of the web server to use for authenticating clients. The default (http://1.0.0.1/www/login.html) is relevant when working with the Arena controller. If a different server is used, this URL should include a full path to the login page in the server, and the server IP address or Domain should be added to the applicable Walled Garden list (see below).
- **UAM Secret**: Configures the shared secret between the UAM server and the device. This secret should be set so as not to compromise security (default: blank). You can click on the **Reveal/hide password** icon ( ) on the right side to hide (the default) or reveal the typed string.
- **Walled Garden (Domain)**: A comma separated list of resources the client can access without first authenticating. Only these servers, together with servers included in the Walled Garden (IP Address)

list (see below), will be available to the Hotspot user before they authenticate. Each entry in the list is a domain name. Do not put www in the domain name. For example: google.com is a valid domain name, www.google.com is not acceptable.

- **Walled Garden (IP Address)**: A comma separated list of resources the client can access without first authenticating. Only these servers, together with servers included in the Walled Garden (Domain) list (see above), will be available to the Hotspot user before they authenticate. Each entry in the list is an IP Address. The list must include the IP addresses of the AP's web page.

3.4.1.6 User's Configuration Page

To access the Hotspot User's Configuration page click on the **Services>Hotspot>User's Configuration** tab in the management function selection panel.

The User's Configuration page enables configuration of the users' network access and bandwidth limitations.

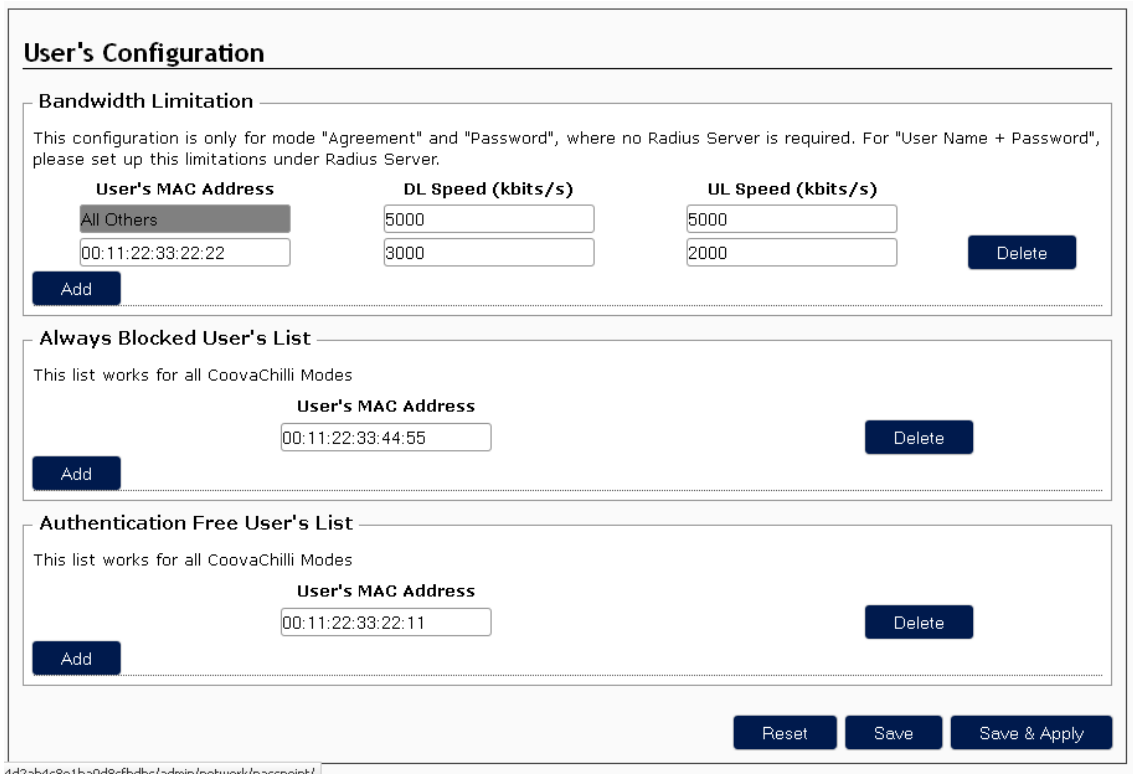


Figure 3-41: Hotspot User's Configuration Page

The User's Configuration page includes the following sections:

- Bandwidth Limitation
- Always Blocked User's List
- Authentication Free User's List

3.4.1.6.1 Bandwidth Limitation

This section only applies only if Hotspot Mode is set to an option where a RADIUS server is not required (see **Hotspot Mode** in "Hotspot General Settings Page" on page 54). If a RADIUS Server is required, this section is ignored and relevant limitations should be provided by the RADIUS server.

You may add entries defining limitations for specific users. Each entry consists of the following three fields:

- **User's MAC Address**: Use the format xx:xx:xx:xx:xx:xx.
- **DL Speed (kbits/s)**: The maximal download speed, in kbits/s.
- **UL Speed (kbits/s)**: The maximal upload speed, in kbits/s.

There is one default entry that cannot be either deleted or modified:

- User's MAC Address: All Others
- DL Speed (kbits/s): 5000
- UL Speed (kbits/s): 5000

This means that all hotspot users are subjected to 5000 kbits/s bandwidth limitation in both directions. To prevent any limitation, it may be set to a very high value like 5000000 kbits/s.

3.4.1.6.2 Always Blocked User's List

The Always Blocked User's List can be used to prepare a list of users that will always be blocked from accessing hotspot service. Each entry in the list consists of a single parameter, **User's MAC Address** (in the format xx:xx:xx:xx:xx:xx).

3.4.1.6.3 Authentication Free User's List

The Authentication Free User's List can be used to prepare a list of users (by their MAC Address) that will not need any authentication at all and can get immediate access to the network. Each entry in the list consists of a single parameter, **User's MAC Address** (in the format xx:xx:xx:xx:xx:xx).

3.4.2 Discovery Page

To access the Discovery page click on the **Services>Discovery** tab in the management function selection panel.

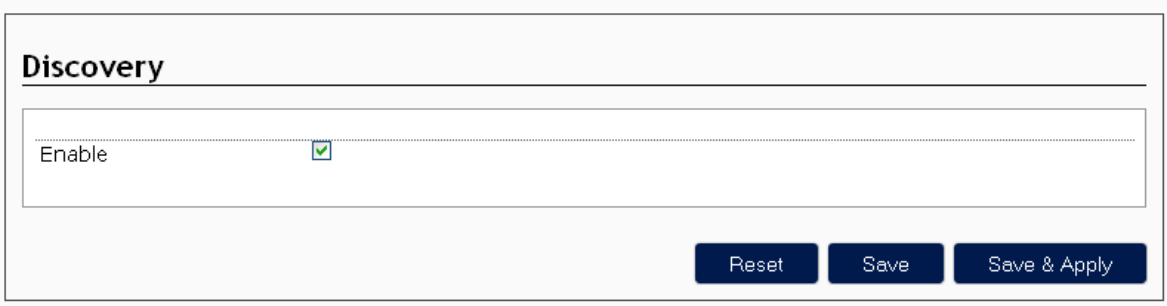


Figure 3-42: Services Discovery Page

- **Enable**: Select Enable (the default) to allow discovery of the device by an Arena controller.

3.5 Network

The Network tab provides access to the following:

- Interfaces Pages
- Wifi Pages
- VLANs Page
- Local DNS Page
- Diagnostics Page
- Passpoint Pages

3.5.1 Interfaces Pages

The Network Interfaces option provides access to the following:

- Interfaces Page
- Per Interface Pages

3.5.1.1 Interfaces Page

To access the Interfaces page click on the **Network>Interfaces** tab in the management function selection panel.

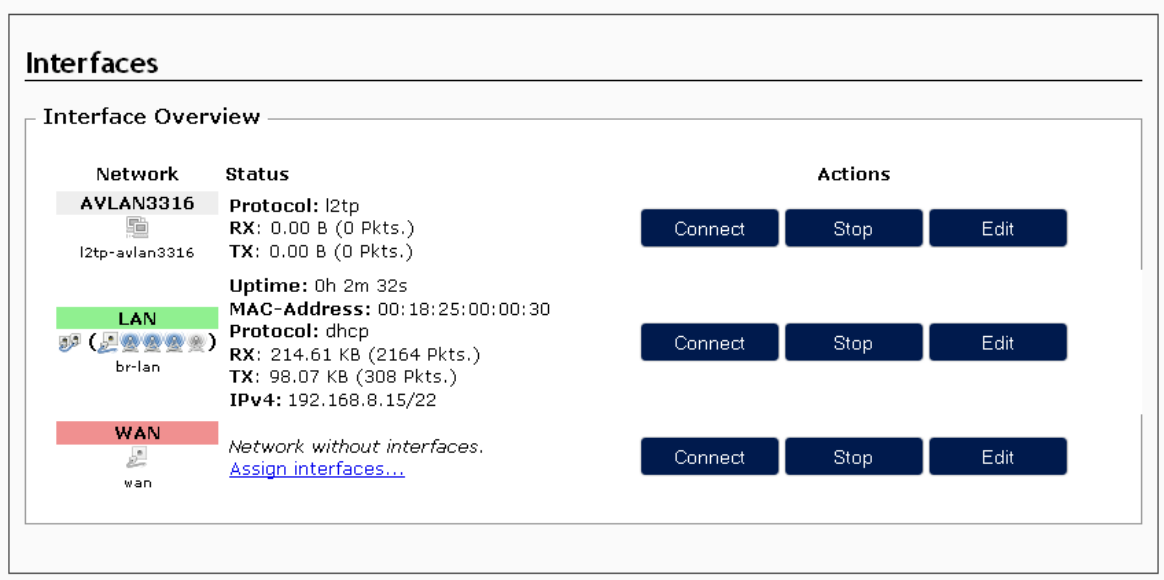


Figure 3-43: Network Interfaces Page

The Interfaces page displays the current status of the AVLAN3316 (l2tp), LAN, and WAN networks. It also displays status parameters for all configured VLANs (if applicable). The network's status parameters are:

- **Uptime**
- **MAC Address**: The MAC address of the network's interface. Not applicable for the l2tp (AVLAN3316) network.
- **Protocol**: The method used for setting the IP address (static or dhcp). For the AVLAN3316 interface the protocol is l2tp.
- **RX**: The accumulated numbers for received Bytes and Packets.
- **TX**: The accumulated numbers for transmitted Bytes and Packets.
- **IPv4**: The IP address and prefix mask.

The icons in parenthesis below the interface name provide indication regarding the Ethernet and wireless networks associated with the network:

The Ethernet icon ( ) provides a visible indication on the total number of Ethernet interfaces assigned to any network (In addition to eth0 assigned to either the LAN or the WAN zone, an Ethernet interface named eth0.<VLAN_ID> is assigned to any configured VLAN).

A wireless network icon ( ) is displayed for each wireless network assigned to the network.

Hover with the mouse over an icon to open an infotip with the name of the relevant Ethernet/wireless network it represents.

The following action buttons are available for each interface:

- **Connect**: Click the button to connect a network that is currently disabled.
- **Stop**: Click the button to disable an interface

CAUTION

If you stop the network used for managing the device you may loose the ability to manage the device from remote.
If you stop the AVLAN3316 network you may loose the ability to properly manage the device from the Arena controller.

- **Edit**: Click the button to switch to the relevant Interface's page.

3.5.1.2 Per Interface Pages

This section includes:

- Fallback IP
- DHCP Server
- Static Leases

3.5.1.2.1 Introduction

Click on the **Network>Interfaces** option to access the per Interfaces pages.

By default, the following interface pages are available:

- **AVLAN3316 page**: The AVLAN3316 page is associated with the L2TP network used for management of the unit by an Arena controller. In the Status section at the top of the page you can view whether this interface is up and if there is traffic on this interface indicating proper connectivity with the controller (for details on relevant configuration parameters refer to "APController" on page 101).

CAUTION

Except to viewing the status of the AVLAN3316 interface, do not make any changes in this page as this may affect the management connectivity with the Arena controller.

- **LAN page**: In the LAN page you can view/configure various parameters of the LAN zone.
- **WAN page**: In the WAN page you can view/configure various parameters of the WAN zone (if applicable).

If VLANs are defined in the device (see "VLANs Page" on page 85), a **VLAN<#>** configuration page becomes available for each defined VLAN, allowing to optionally define IP parameters associated with this VLAN.

When you access an interface page for the first time (excluding the LAN page), you will get an initial Protocol selection page:

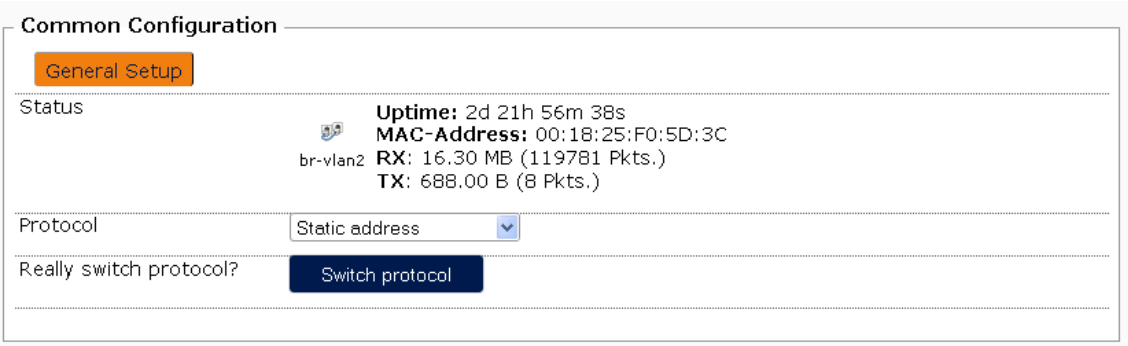


Figure 3-44: Network Per Interface Page, Initial Protocol Selection

To view/configure additional parameters, you must first select the required **Protocol** (for more details see Protocol in "Common Configuration" on page 65 below) and click on the **Switch protocol** button (even if the currently displayed Protocol option is the one you want to use).

CAUTION

Do not execute the **Switch protocol** action in the AVLAN3316 page.

By default, the device is supplied in Bridge mode with all physical interfaces assigned to the LAN zone. The LAN interface is configured as the management interface (see Management Interface in "Common Configuration" on page 65 below). The default Protocol is DHCP client. In this mode no physical interface is assigned to the WAN interface.

3.5.1.2.2 Switching from Bridge Mode to Router Mode and Vice Versa

To switch from Bridge mode to Router mode:

To avoid possible lose of management connectivity, follow these steps:

1. In the WAN page:
   a. In the Common Configuration section select the General Setup tab. In the Management Interface parameter drop-down list select the Management option to enable remote management via the Ethernet backbone.
   b. Make sure that the Fallback IP parameters (see "Fallback IP" on page 69) are configured properly (applicable for the default DHCP client option for the Protocol parameter).
   c. In the Physical Settings tab select the Ethernet Adapter: "eth0" option to assign the Ethernet interface to the WAN.
   d. Click on the **Save** button to apply the change.
2. In the LAN page:
   a. Set the Protocol to Static address (you will be requested to confirm the action by clicking on the **Switch protocol** button that will become available) and configure relevant parameters. Make sure that different subnets are configured for the LAN and WAN zones.
   b. In the DHCP Server section, enable the DHCP server and configure relevant parameters (see "DHCP Server" on page 70). You may configure also Static Leases (see "Static Leases" on page 72).
3. Click on the **Save & Apply** button to apply the changes.

To switch from Router mode to Bridge mode:

To avoid possible lose of management connectivity, follow these steps:

NOTE!

If Hotspot service is enabled (see "Hotspot General Settings Page" on page 54, it must be disabled before starting the process of switching from Router mode to Bridge mode.

1. In the LAN page:
   a. In the Common Configuration select the General Setup tab. Change the Protocol to DHCP client (you will be requested to confirm the action by clicking on the **Switch protocol** button that will become available).
   b. In the Management Interface parameter drop-down list select the Management option.
   c. Make sure that the Fallback IP parameters (see "Fallback IP" on page 69) are configured properly.
   d. Click on the **Save** button.
2. In the Common Configuration section of the WAN page, select the Physical Settings tab. In the Physical Settings tab select the No Interface option.
3. Click on **Save & Apply** to apply the changes.

3.5.1.2.3 Common Configuration

The Common Configuration section is available in all per interface pages.

The Common Configuration section includes the following tabs:

- General Setup
- Advanced Settings
- Physical Settings

3.5.1.2.3.1 General Setup

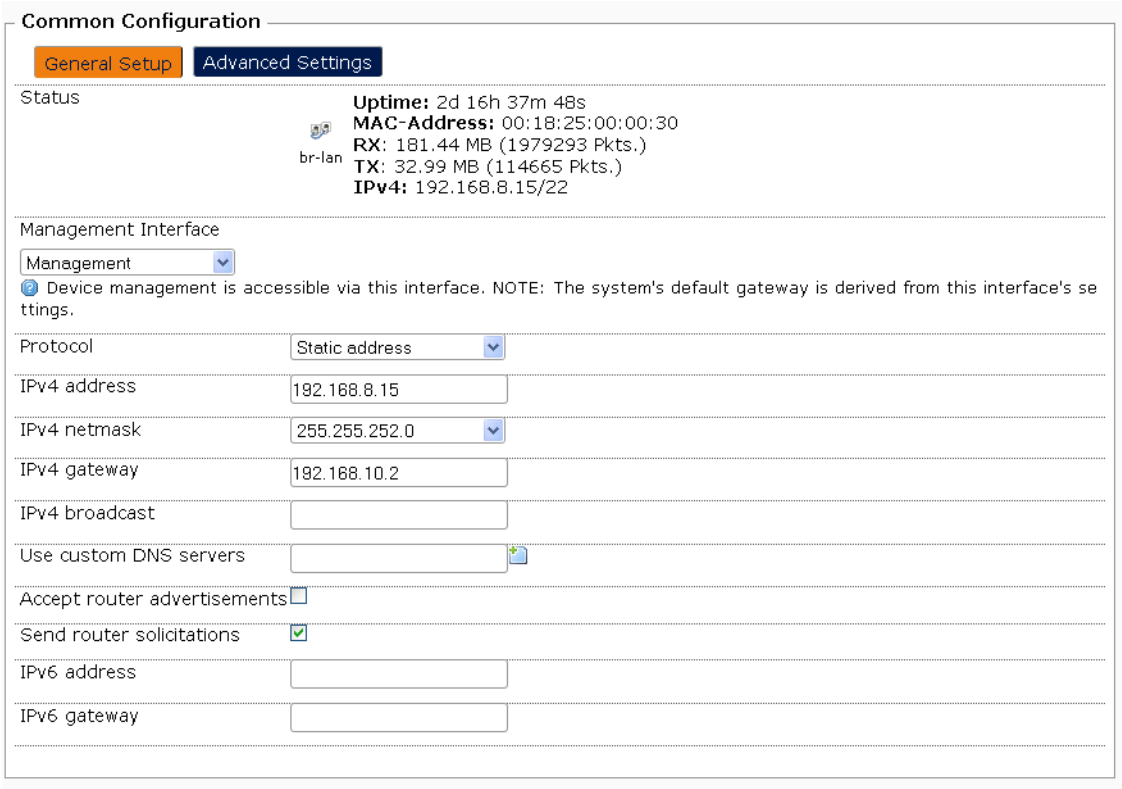


Figure 3-45: Network Per Interface Page, Common Configuration Section, General Setup Tab (Static address Protocol)

The General Setup tab includes the following components:

- **Status**: A read-only display of the following details for the interface:
  - Uptime (if active)
  - MAC Address (not applicable for the AVLAN3316 interface)
  - RX (accumulated numbers for Bytes and Packets received on this interface since it became active)
  - TX (accumulated numbers for Bytes and Packets transmitted on this interface since it became active)
  - IPv4 (the IP address of the interface)
- **Management Interface**: This parameter indicates whether the interface is configured as the management interface. Only one interface can be defined as the Management interface. In all other interfaces the configured option is No. To change the management interface, select the Management option in the selected interface. Once applied, the configuration of this parameter in the previous management interface will change automatically to No.

By default, the LAN interface is configured as the Management interface. To set the WAN interface as the management interface, the Management option should be selected in the WAN interface page.

CAUTION

The process of changing the management interface should be executed very carefully, otherwise you may loose the ability of managing the unit from remote. For details on the full process of changing the management interface from LAN (bridge mode) to WAN (router mode) and vice versa, refer to "Switching from Bridge Mode to Router Mode and Vice Versa" on page 64.

- **Protocol**: The method for setting IP parameters for the interface (Static address or DHCP client). When attempting to change the selected method, a **Switch protocol** button will become available prompting you to confirm the action.

  In DHCP client mode you can view it's IPv4 address and subnet in the Status section. The actual gateway can be seen in the Active IPv4-Routes section of the System>Routes page (see "Routes Page" on page 33).

  The option configured for the Protocol parameter affect availability of and configuration guidelines for other parameters in the interface's page:

3.5.1.2.3.1.1 Static address Parameters

The additional parameters available when Protocol is set to Static address mode are:

- **IPv4 address**
- **IPv4 netmask**
- **IPv4 gateway**: The default gateway for the device. Applicable only for the interface configured as the management interface.
- **IPv4 broadcast**: There is no need to configure this parameter - the value will be calculated automatically.
- **Use custom DNS servers**: An optional list (in order of priority) of IP addresses of preferred DNS server(s).
- **Accept router advertisements**: In the current release the default configuration (unchecked) should not be changed.
- **Send router solicitations**: In the current release the default configuration (checked) should not be changed.
- **IPv6 address**: In the current release this parameter should not be used.
- **IPv6 gateway**: In the current release this parameter should not be used.

3.5.1.2.3.1.2 DHCP client parameters

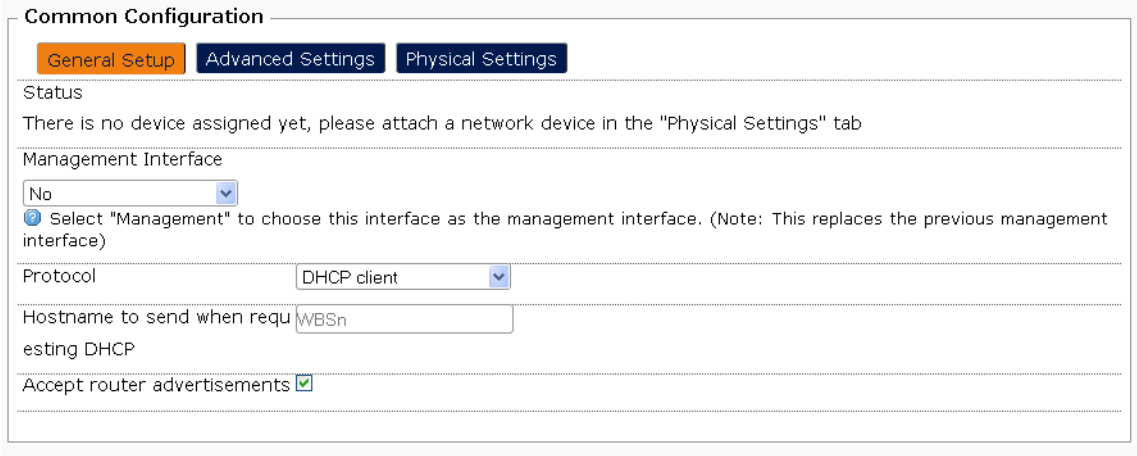


Figure 3-46: Network Per Interface Page, Common Configuration Section, General Setup Tab (DHCP client Protocol)

The additional parameters available when Protocol is set to DHCP client mode are:

- **Hostname to send when requesting DHCP**: The default is the configured device's Hostname (see "General Settings" on page 41).
- **Accept router advertisements**: In the current release the default configuration (checked) should not be changed.

3.5.1.2.3.2 Advanced Settings

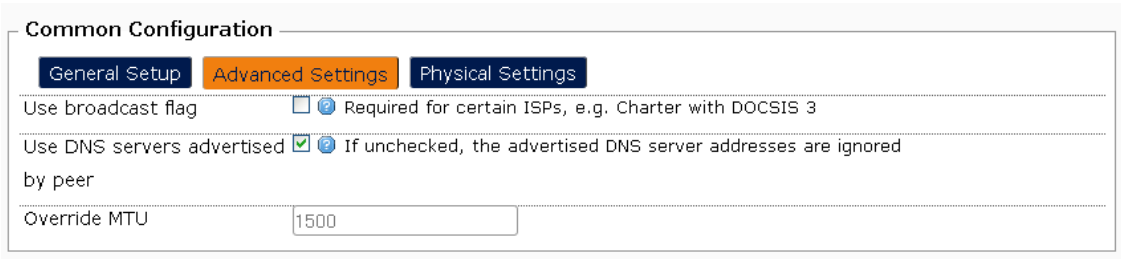


Figure 3-47: Network Per Interface Page, Common Configuration Section, Advanced Settings Tab (DHCP client Protocol)

The Advanced Settings tab includes the following components:

- **Use broadcast flag**: Available only when Protocol is set to DHCP client mode. When sending DHCP requests, a client can indicate if it wants an answer in a unicast or broadcast message by setting the broadcast flag. This may be required for certain service providers. Unchecked by default.
- **Use DNS servers advertised by peer**: Available only when Protocol is set to DHCP client mode. Check (the default) to use the DNS servers settings advertised by the DHCP server.

- **Override MTU**: The maximum transmission unit (MTU), in bytes. The allowed range is from 1200 to 1500 bytes, the default being 1500. Unless required by the service provider, it is not recommended to change this setting.

NOTE!

If a VLAN interface is used for management, it is recommended to set the MTU to 1496 bytes.

3.5.1.2.3.3 Physical Settings

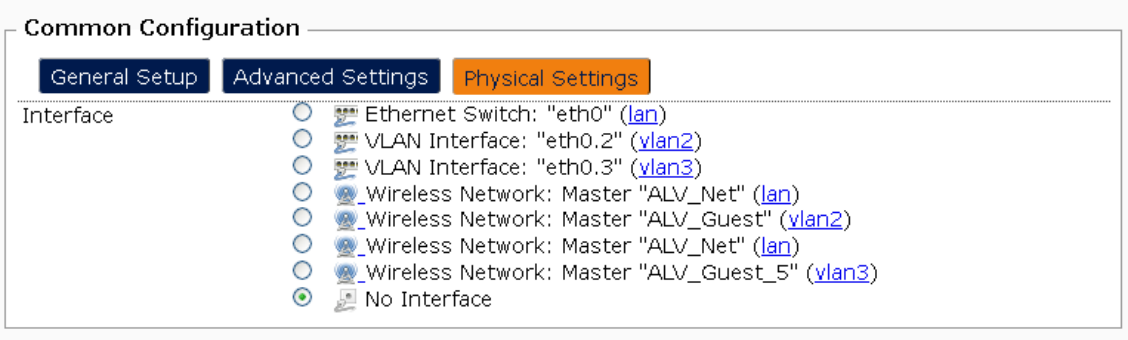


Figure 3-48: Network Per Interface Page, Common Configuration Section, Physical Settings Tab

The Physical Setting tab is available only for the WAN interface, enabling to select the physical interface to be assigned to the WAN zone. For more details refer to "Switching from Bridge Mode to Router Mode and Vice Versa" on page 64.

3.5.1.2.4 Fallback IP

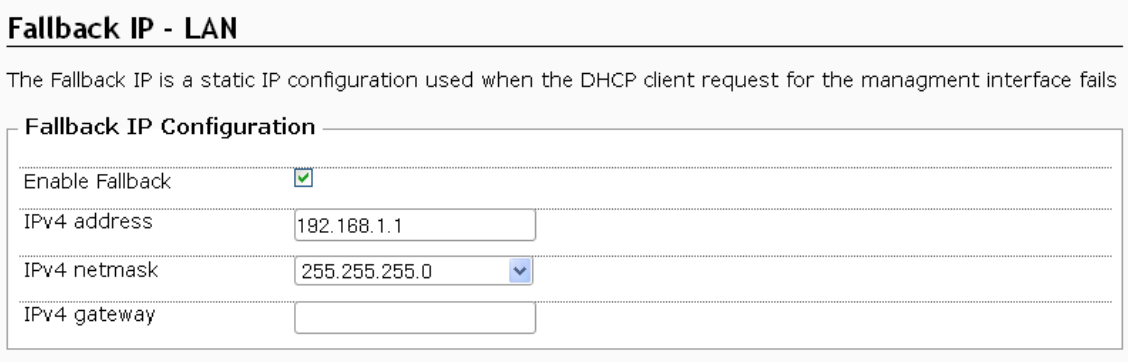


Figure 3-49: Network Per Interface Page, Fallback IP Section

The Fallback IP section is available only for the management interface when it is set to acquire IP parameters from a DHCP server (Protocol parameter set to DHCP client).

The fallback IP parameters are the static IP parameters to be used when a DHCP server is not available. The default values (Enable Fallback checked, IPv4 address 192.168.1.1, IPv4 netmask 255.255.255.0) enable initial local management access for a new unit. Verify that these parameters are properly configured and that configuration details are properly documented to ensure management access at all times when for any reason DHCP server is not available.

3.5.1.2.5 DHCP Server

The DHCP Server option is available only in the LAN page when a static address is configured for the interface (Protocol is set to Static address).

NOTE!

Do not enable the DHCP Server feature when the unit operates in Bridge mode.

In the default configuration only a single parameter is available in the DHCP Server section:

- **Ignore interface**: Check (the default) to disable the DHCP server feature.

Uncheck the Ignore interface checkbox to enable the DHCP server and open the following tabs:

- General Setup
- Advanced Settings

3.5.1.2.5.1 General Setup

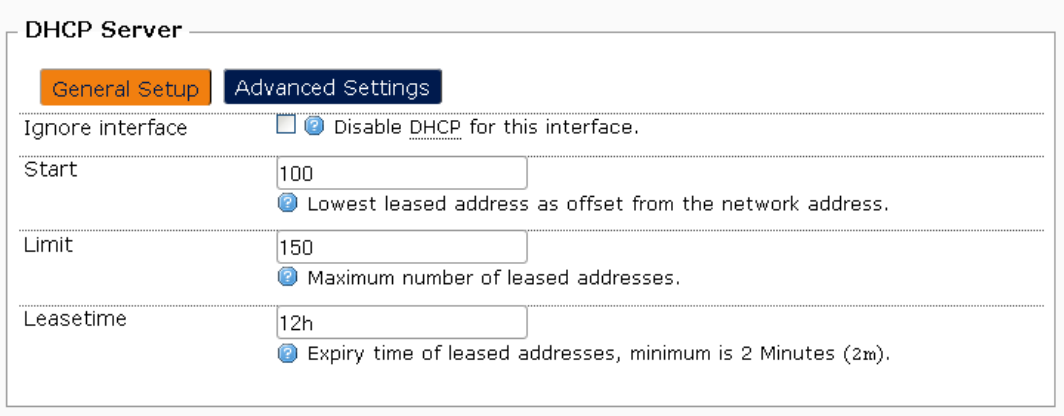


Figure 3-50: Network Per Interface Page, DHCP Server Section, Advanced Setup Tab

The General Setup tab includes the following parameters:

- **Start**: The offset from the network IP address of the lowest address to be leased. The default is 100.
- **Limit**: The maximum number of addresses to be leased. The default is 150.

- **Leasetime**: The expiry time of leased addresses, including static leases if applicable (see Static Leases below). You can specify leasetime in minutes (such as 2m for a two minutes leasetime), hours (such as 12h which is the default for a 12 hours leasetime), or days (such as 7d for seven days leasetime).

3.5.1.2.5.2 Advanced Settings

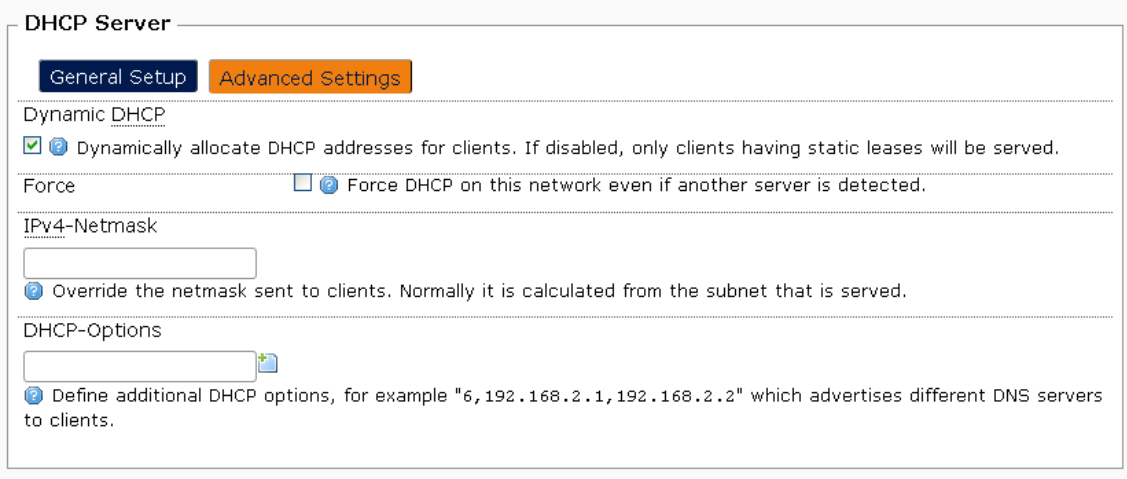


Figure 3-51: Network Per Interface Page, DHCP Server Section, General Setup Tab

The Advanced Settings tab includes the following parameters:

- **Dynamic DHCP**: Check (the default) to enable dynamic allocations of DHCP addresses for clients. If disabled, only clients having static leases (see Static Leases below) will be served.
- **Force**: Check to respond to DHCP requests on this network even if another DHCP server is detected. The default is unchecked, meaning that if another DHCP server is detected the built-in DHCP server will not respond to DHCP requests on this network.
- **IPv4-Netmask**: By default, the IP netmask used in DHCP IP addresses allocations is the netmask specified for the network. If necessary, you can define a different IP netmask to be used in addresses allocations. The default is null (use the default netmask).
- **DHCP Options**: You may optionally define a list of additional DHCP options to be advertised to clients. In each comma separated string you should specify the option code and relevant value(s). For example, to use option 6 (Domain Name Server) to advertise one or more DNS servers (in order of priority) to clients, specify the string “6,<IP_address_1>,<IP_address_2>...”.

3.5.1.2.6 Static Leases

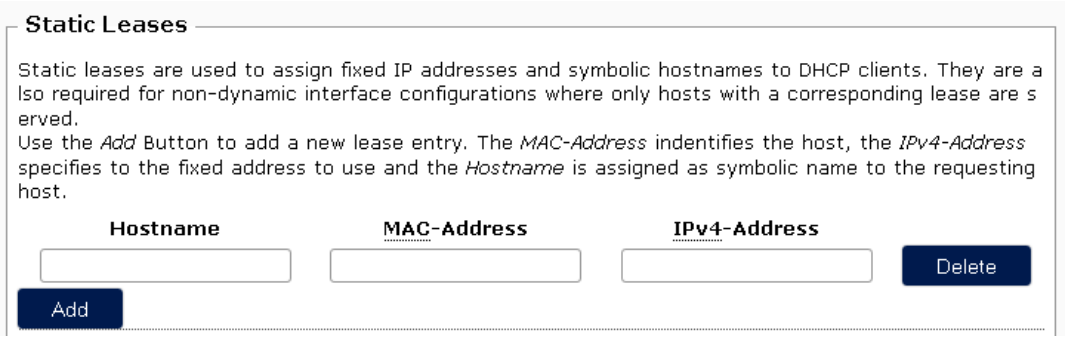


Figure 3-52: Network Per Interface Page, Static Leases Section

In this section, you can specify IP addresses to be allocated by the DHCP server to particular DHCP clients. Static leases are applicable only when the DHCP Server is enabled (**Ignore interface** is unchecked). The IP addresses to be allocated as static leases should belong to the configured network. However, if **Dynamic DHCP** is enabled, than IP addresses in the range configured for dynamic allocation by the **Start** and **Limit** parameters should not be used for static leases.

A static lease entry include the following parameters:

- **Hostname**: An optional symbolic name to be assigned to the device.
- **MAC-Address**: The device's MAC address (use the format xx:xx:xx:xx:xx:xx).
- **IPv4-Address**: The static IP address to be assigned to the device.

3.5.2 Wifi Pages

Click on the Wifi option to open the Wifi Wireless Overview Page. In addition, the third-level tabs are revealed under the Wifi tab, one tab for each of the defined wireless networks (SSIDs), enabling to open the applicable Wireless Network Page.

3.5.2.1 Wifi Wireless Overview Page

The Wireless Overview page includes the following sections:

- Wireless Adapter 802.1bgn
- Wireless Adapter 802.1an (if available)
- Associated Stations

3.5.2.1.1 Wireless Adapter 802.1bgn

The Wireless Adapter 802.11bgn section provides general configuration and status details for the 2.4 GHz radio as well as some general configuration and status details for each of the configured wireless networks. It also includes some buttons enabling general management of the radio and its wireless networks.

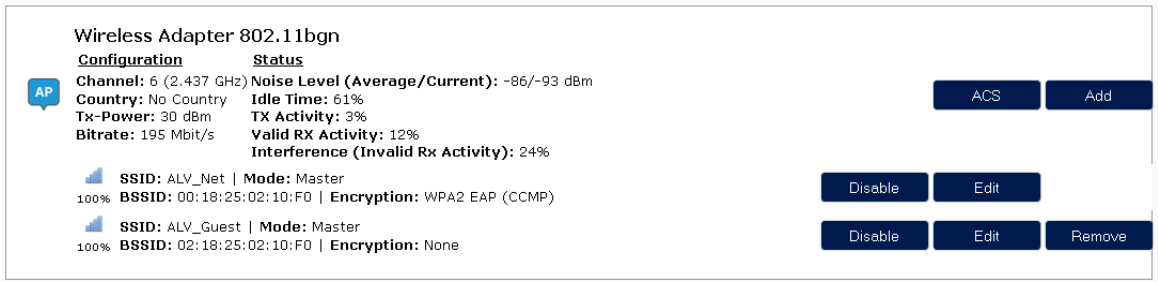


Figure 3-53: Network Wifi Wireless Overview Page, Wireless Adapter 802.11bgn Section

A suitable icon on the left side indicates the mode/status of the radio cards:

Table 3-2: Radio Operation Mode / Status

Icon	Description
AP	Regular Access Point
X	Radio is disabled
RAP	Mesh Root Access Point
MAP	Mesh Access Point

The following information and buttons are available in the Wireless Adapter section:

- General Radio Configuration Details
- General Radio Status Details
- Per Wireless Network Configuration Details
- General Radio Buttons
- Per Wireless Network Buttons

3.5.2.1.1.1 General Radio Configuration Details

- Channel
- Country
- Tx-Power
- Bitrate

For details on these general radio parameters refer to "General Setup" on page 78.

3.5.2.1.1.2 General Radio Status Details

- Noise Level (Average/Current): The average (over the last 10 seconds) and current levels of noise (in dBm) measured by the device. An Average Noise Level in the range from -85 dBm to -75 dBm indicates moderate interference. An Average Noise Level higher than -75 dBm indicates a high level of interference. This indication may trigger a decision to try searching for a channel with a better quality.
- Idle Time: Percentage of time that the device has been idle during the last 10 seconds.
- TX Activity: Percentage of time that the device has spent transmitting during the last 10 seconds.
- Valid RX Activity: Percentage of time that the device has been occupied receiving valid data (Wi-Fi transmissions) during the last 10 seconds.
- Interference (Invalid Rx activity): Percentage of time that the device has been occupied receiving non-valid data (i.e. interfering traffic) during the last 10 seconds.

3.5.2.1.1.3 Per Wireless Network Configuration Details

- SSID or Mesh ID:
  - » SSID is applicable when the device is configured to operate as a regular AP. The wireless network name.
  - » Mesh ID is applicable when the device is configured to operate in Mesh mode. The mesh ID of the mesh network.
- Mode:
  - » For a regular AP: Master
  - » For a Mesh node:
    - ◊ Mesh - Master: A wireless network operating as an AP.
    - ◊ Mesh - Monitoring: A wireless network used for batman-adv protocol.
    - ◊ Mesh - Client: A wireless network operating as a client (WDS station).
    - ◊ Router - Client: A wireless network operating as a client that provides connectivity to the backbone.
- BSSID: The Basic Service Set IDentifier (the MAC address of the radio card). Not applicable for a wireless network in Mesh - Monitoring mode.
- Encryption: The selected Wireless Security mode (see "Wireless Security" on page 82). Not applicable for a wireless network in Mesh - Monitoring mode.

Hover with the mouse over the link quality icon (to the left of the SSID/Mesh ID parameter) to reveal the Signal and Noise levels for the wireless network.

3.5.2.1.1.4 General Radio Buttons

The following general radio management buttons are available:

- **Add**: Click to create another wireless network. A new wireless network with default values for Interface Configuration parameter (see "Interface Configuration" on page 79) will be added. Up to 6 wireless networks may be created per radio.
- **ACS**: Click to display the Radio Channel Scan Report page:

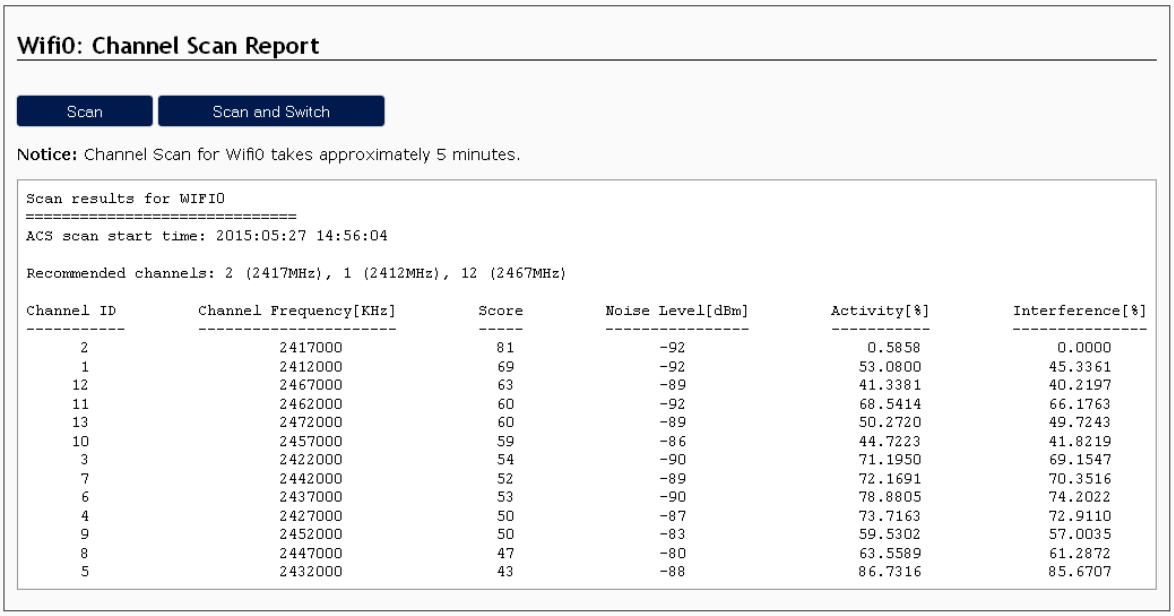


Figure 3-54: Radio Channel Scan Report Page

The last Scan results (if any) include:

- **ACS scan start time**: The date and time at which the last scan has started.
- **Recommended Channels**: Channel Number and Frequency (in MHz) of the 3 best channels (highest quality score) according to the last scan results.

- Scan results table, sorted by Score value (see below) providing the following details for each channel:
  - **Channel ID**: The channel number.
  - **Channel Frequency [KHz]**
  - **Score**: An indicator of the channel's quality based on the measurements of Noise Level, Activity and Interference (see below).
  - **Noise Level [dBm]**: The measured noise level in dBm.
  - **Activity [%]**: Percentage of time that there has been activity in the channel during the measurement period.
  - **Interference [%]**: Percentage of time that there has been interference (non-valid traffic) in the channel during the measurement period.

Click on the **Scan** button to run the interference analyzer for the radio band.

Click on the **Scan and Switch** button to run the interference analyzer and automatically switch to the best channel after completion of the task.

NOTE!

During channel scan process normal operation of the device is interrupted.

3.5.2.1.1.5 Per Wireless Network Buttons

The following buttons are available for each configured wireless network:

- **Disable/Enable**: Click to disable/enable the wireless network.
- **Edit**: Click to open the configuration page for the specific wireless network.
- **Remove**: Click to remove the specific wireless network.

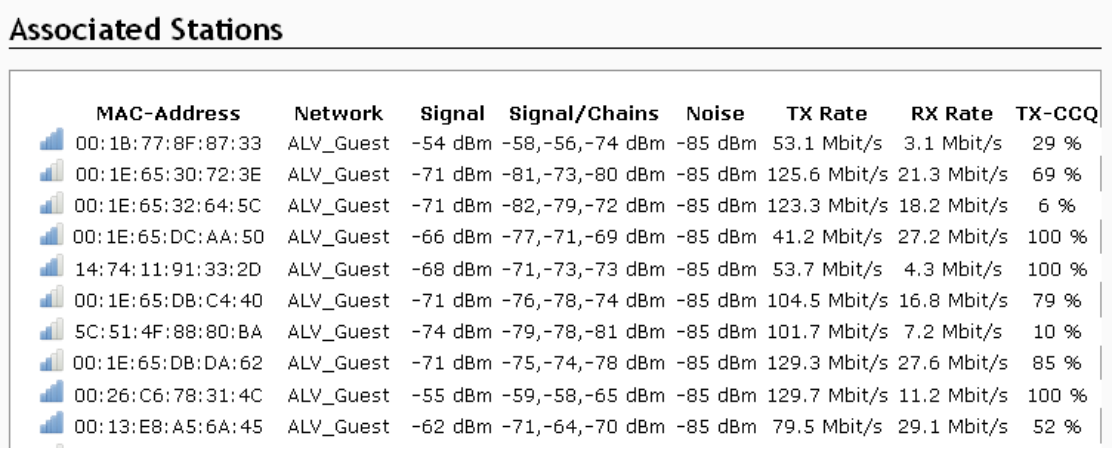
By default, there is one wireless network for each radio. This wireless network cannot be removed.

3.5.2.1.2 Wireless Adapter 802.1an

The Wireless Adapter 802.11an section (not applicable for WBSn-2400 units) provides for the 5 GHz radio the same information and general management functionality as the provided for the 2 GHz radio in "Wireless Adapter 802.1bgn" on page 72.

3.5.2.1.3 Associated Stations

This section shows the following details for each of the end-user devices connected to the AP.



Associated Stations

MAC-Address	Network	Signal	Signal/Chains	Noise	TX Rate	RX Rate	TX-CCQ
00:1B:77:8F:87:33	ALV_Guest	-54 dBm	-58,-56,-74 dBm	-85 dBm	53.1 Mbit/s	3.1 Mbit/s	29 %
00:1E:65:30:72:3E	ALV_Guest	-71 dBm	-81,-73,-80 dBm	-85 dBm	125.6 Mbit/s	21.3 Mbit/s	69 %
00:1E:65:32:64:5C	ALV_Guest	-71 dBm	-82,-79,-72 dBm	-85 dBm	123.3 Mbit/s	18.2 Mbit/s	6 %
00:1E:65:DC:AA:50	ALV_Guest	-66 dBm	-77,-71,-69 dBm	-85 dBm	41.2 Mbit/s	27.2 Mbit/s	100 %
14:74:11:91:33:2D	ALV_Guest	-68 dBm	-71,-73,-73 dBm	-85 dBm	53.7 Mbit/s	4.3 Mbit/s	100 %
00:1E:65:DB:C4:40	ALV_Guest	-71 dBm	-76,-78,-74 dBm	-85 dBm	104.5 Mbit/s	16.8 Mbit/s	79 %
5C:51:4F:88:80:BA	ALV_Guest	-74 dBm	-79,-78,-81 dBm	-85 dBm	101.7 Mbit/s	7.2 Mbit/s	10 %
00:1E:65:DB:DA:62	ALV_Guest	-71 dBm	-75,-74,-78 dBm	-85 dBm	129.3 Mbit/s	27.6 Mbit/s	85 %
00:26:C6:78:31:4C	ALV_Guest	-55 dBm	-59,-58,-65 dBm	-85 dBm	129.7 Mbit/s	11.2 Mbit/s	100 %
00:13:E8:A5:6A:45	ALV_Guest	-62 dBm	-71,-64,-70 dBm	-85 dBm	79.5 Mbit/s	29.1 Mbit/s	52 %

Figure 3-55: Wifi Wireless Overview Page, Associated Stations Section

- **MAC-Address**: Displays the MAC address of the station's radio.
- **Network**: States the name of the wireless network (SSID / Mesh ID) to which the device is connected.
- **Signal**: The total strength (in dBm) of the signal received from the station.
- **Signal/Chains**: The strength of the signal received from the station per chain (the value of -95 dBm is taken to mean "no antenna").
- **Noise**: The received noise level at the AP.
- **TX Rate**: The transmit bit rate from the AP towards this station.
- **RX Rate**: Shows the receive bit rate at the AP from this station.
- **TX-CCQ**: The transmission quality in % (a higher percentage means a better wireless connection quality).

3.5.2.2 Wireless Network Page

A Wireless Network page is available for each configured wireless network.

The page title is "Wireless Network <Mode> <Network Name (SSID)> (<ath#>)". In current release Mode is always Master and ath# indicates the number of the wireless network interface, where # can be from 0 to 5 for the 2.4 GHz radio (wifi0) and from 6 to 11 for the 5 GHz radio (wifi1).

To open the Wireless Network page for a specific wireless network:

- From the management function selection panel, click on the relevant tab.
- From the Wifi Wireless Overview page, click on the relevant **Edit** button.
- From the Status Overview page, click on the SSID's name in the Wireless section.

The Wireless Network page includes the following sections:

- Device Configuration
- Interface Configuration

3.5.2.2.1 Device Configuration

The Device Configuration section includes configuration parameters for the entire relevant radio, and is available only for the first wireless network of each radio.

The following tabs are available in the Device Configuration section:

- General Setup
- Advanced Settings

3.5.2.2.1.1 General Setup

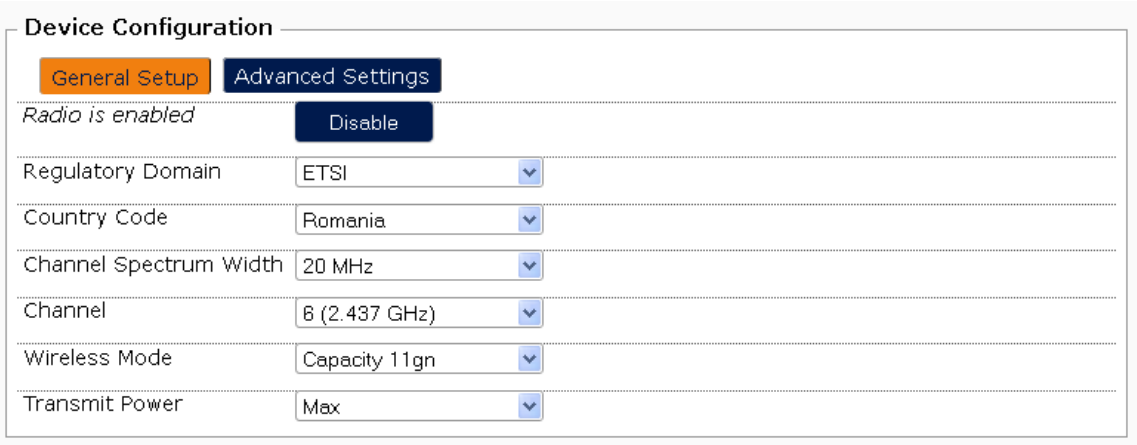


Figure 3-56: Wireless Network Page, Device Configuration Section, General Setup Tab

- **Radio is enabled/disabled**: The operational status of the radio. To change the operational status click on the **Disable/Enable** button.
- **Regulatory Domain**: The regulatory domain to be used. The regulatory domain (together with the Country parameter) affects certain parameters such as available channels, maximum transmit power and required usage of Dynamic Frequency Selection (DFS).
- **Country**: Select the country in which the device operates to ensure that the applicable regulatory requirements are enforced. Local regulations affects parameters such as available channels, maximum transmit power and DFS.

NOTE!

When two radios are available, the Regulatory Domain and Country parameters are available only for the 2.4 GHz radio (Wifi0). The configuration of these parameters will be applicable for both radios.

- **Spectrum Width**: The available options for the channel bandwidth are:
  - 20 MHz
  - 20/40 MHz, allows both 20 and 40 MHz bands to be used (depending on the connected device).
- **Channel**: Select a specific channel (the Auto option for selecting the channel with the least interference is a future feature).
- **Wireless Mode:** Defines the method of optimizing various wireless parameters:
  - **Capacity** mode provides maximum capacity to the maximum number of users. For a 2.4 GHz radio you may select whether to support also low rate IEEE 802.11b clients (**Capacity 11bgn**) or not (**Capacity 11gn**).
  - **Coverage** mode enables achieving maximum coverage (range) with some degradation in the overall system capacity. Coverage mode can be useful in cases of low noise level (below -80dBm) and low total Rx activity (when valid Rx activity plus interference is below 30%) as shown on the Radio Status page. For a 2.4 GHz radio you may select whether to support also low rate IEEE 802.11b clients (**Coverage 11bgn**) or not (**Coverage 11gn**).
  - **High Density** mode provides optimization for serving a maximum number of clients in a crowded area located at a relatively short distance from the base station. High Density mode provides an optimal solution for environments where multiple base stations are use to effectively serve a very large number of users in highly crowded areas such as sport stadiums, music arenas and exhibition halls.
- **Transmit Power**: The total transmit power at the antennas ports. Select a specific value or Max. The maximum allowed value depends on applicable regulatory limitations and, in certain cases, the operating channel.

3.5.2.2.1.2 Advanced Settings

Figure 3-57: Wireless Network Page, Device Configuration Section, Advanced Settings Tab

- **Distance**: The maximum distance (in Km) of any station from the AP. This parameter affects the value of the ACK timeout to be used by the communication protocol and it should be set to a value that is slightly higher than the physical distance between the AP and the farthest station.

3.5.2.2.2 Interface Configuration

The Interface Configuration section enables configuring various operational parameters for the wireless network.

The following tabs are available in the Interface Configuration section:

- General Setup
- Wireless Security
- MAC-Filter
- Advanced Settings

3.5.2.2.2.1 General Setup

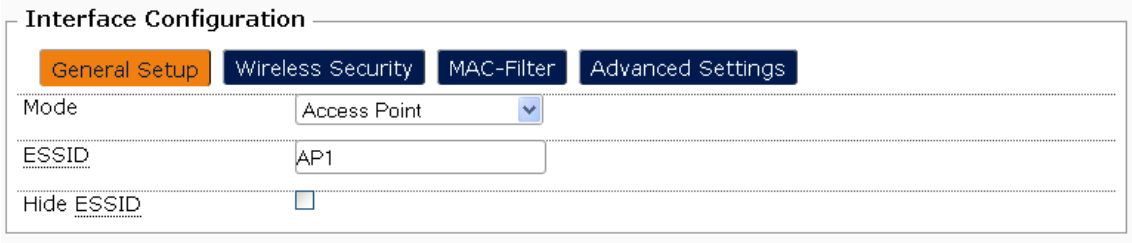


Figure 3-58: Wireless Network Page, Interface Configuration Section, General Setup Tab

The General Setup tab includes the following parameters:

- **Mode**: The operation mode of the wireless network. The available options are Access Point (the default) and Mesh. When attempting to change the selected mode, a **Switch mode** button will become available prompting you to confirm the action. The availability of the following parameters depend on the configured mode.

IMPORTANT

NOTE!

1 Mesh mode is applicable only for a dual band device.

2 Only one radio should be set to operate in set mode (the other band is to be used for providing access to client devices.

3 before configuring a radio to operate in Mesh mode, verify that only a single wireless network (the default) is defined. This is the wireless network to be set to Mesh mode.

3.5.2.2.2.1.1 Access Point Mode Parameters

- **ESSID**: The name or extended service set identifier (ESSID) of the wireless network. A string of up to 32 characters. This is used also as the name for the wireless network (SSID). For a newly added wireless network, the default ESSID is AP#, where # is the sequential number of the wireless network.
- **Hide ESSID**: Yes or No (the default). Select Yes to hide the ESSID from being broadcasted publicly. Hiding the SSID can decrease the amount of devices that may try connecting to the wireless network. If Hotspot service is enabled, SSID should not be hidden.

3.5.2.2.2.1.2 Mesh Mode Parameters

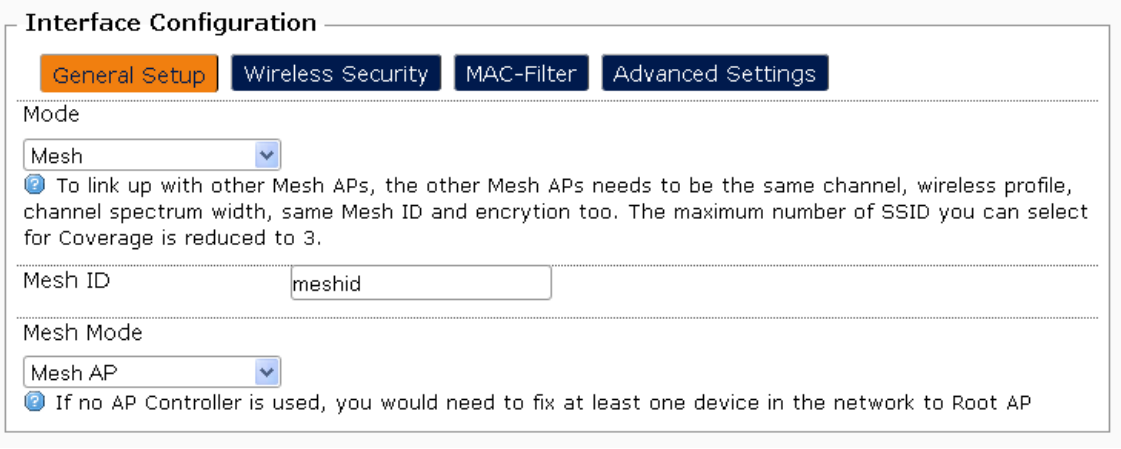


Figure 3-59: Wireless Network Page, Interface Configuration Section, General Setup Tab (Mesh Mode)

- **Mesh ID**: The Mesh ID of the mesh network. Functionality is similar to that of SSID in regular Access Point mode. All mesh network nodes must use the same Mesh ID.
- **Mesh Mode**: The mesh node type. The available options are Root AP (RAP), Mesh AP (MAP) and Root AP + Router Client.

  The current (first wireless network in the radio) is always set to Mesh - Master (Access Point) mode. The following wireless network(s), with the same Mesh ID, will be created automatically:

  - For Root AP mode: One additional wireless network (the second wireless network in the radio), operating in Mesh - Monitoring mode (used for the batman-adv protocol).
  - For Root AP + Router Client: Two additional wireless networks will be created.
    1. The second wireless network in the radio, operating in Mesh - Monitoring mode.
    2. The third wireless network in the radio, operating in Router - Client mode (used for connectivity to the backbone).
  - For Mesh AP: Two additional wireless networks will be created.
    1. The second wireless network in the radio, operating in Mesh - Monitoring mode.
    2. The third wireless network in the radio, operating in Mesh - Client mode.

NOTE!

The configuration of the automatically created wireless network(s) cannot be modified.

3.5.2.2.2 Wireless Security

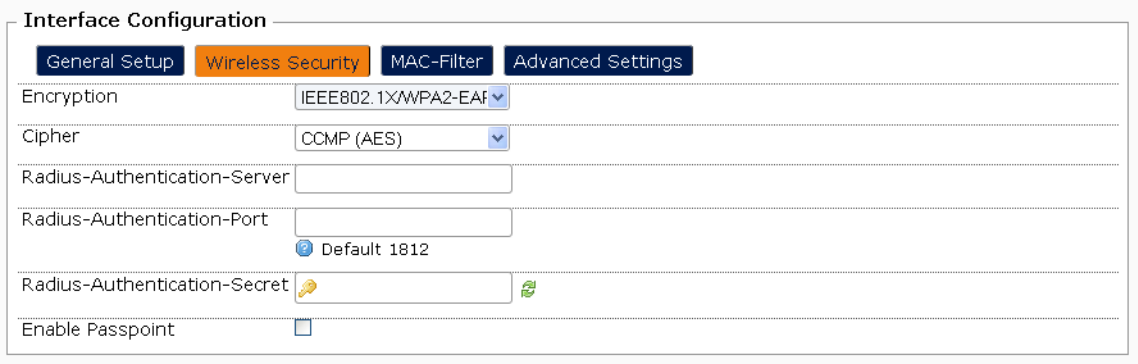


Figure 3-60: Wireless Network Page, Interface Configuration Section, Wireless Security Tab

The Wireless Security tab enables setting the following:

- Encryption Mode and Parameters
- Passpoint Parameters

3.5.2.2.2.1 Encryption Mode and Parameters

The selected Encryption option and relevant parameters define the methods to be used for authentication of client devices and for protecting the information transferred over the wireless link. The available options are:

- No Encryption
- WEP Open System
- WEP Shared Key
- WPA-PSK
- WPA2-PSK
- WPA-PSK/WPA2-PSK Mixed Mode
- IEEE802.1X/WPA-EAP
- IEEE802.1X/WPA2-EAP

No Encryption: No authentication, no encryption of over the air information. This is the default mode that should typically be used for testing purposes or for enabling any client to connect with the AP (e.g. to support Hotspot services).

WEP: Wired Equivalent Privacy (WEP) is the oldest and least secure encryption algorithm. In 2004 the IEEE declared that both WEP-40 and WEP-104 "have been deprecated as they fail to meet their security goals". Stronger encryption using WPA or WPA2 should be used where possible.

The same shared WEP key must be configured in both side of the wireless link, and is used for both authentication and encryption of over the air traffic.

For the WEP Open System and WEP Shared Key encryptions, you can specify up to 4 keys and only 1 would be used at a time. The following parameters are available:

- **Used Key Slot**: Chooses from Key #1 to Key #4.
- **Key #1**: Specifies a string of characters to be used as the password. You can click on the **Reveal/hide password** icon ( ) on the right side of each field to hide (the default) or reveal the typed string.
- **Key #2, Key #3, and Key #4**: Similar to Key #1.

WPA or WPA2 with PSK: WPA (Wi-Fi Protected Access) became available in 2003 and was intended as an intermediate measure in anticipation of the availability of the more secure and complex WPA2. WPA is a more powerful security technology for Wi-Fi networks than WEP. It provides strong data protection by using encryption as well as better access control and user authentication. TKIP (Temporal Key Integrity Protocol) is used for data encryption. TKIP is no longer considered secure and was deprecated in the 2012 revision of the 802.11 standard.

WPA has been replaced by WPA2 using the much stronger AES-based security. The WPA options are available for supporting some client devices that do not support WPA2 with AES encryption. These options are no longer supported for client using the IEEE 802.11n standard.

For WPA-PSK, WPA2-PSK, WPA-PSK/WPA2-PSK Mixed Mode encryptions, we have the following options.

- **Cipher**: The options are CCMP(AES) or TKIP and CCMP(AES). The Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) is based on the Advanced Encryption Standard (AES) and is the most secure protocol.
- **Key**: The pre-shared key (PSK) is the password for the wireless network. This may consist of 8 to 63 printable ASCII characters. You can click on the **Reveal/hide password** icon ( ) on the right side of each field to hide (the default) or reveal the typed string.

IEEE802.1X/WPA-EAP or **IEEE802.1X/WPA2-EAP**: The Extensible Authentication Protocol (EAP) is encapsulated by the IEEE 802.1X authentication method. IEEE 802.1X is equivalent to EAP over LAN or WLAN. Enterprise networks commonly use this authentication method.

Required parameters:

- **Cipher**: The options are CCMP(AES) or TKIP and CCMP(AES).
- **Radius-Authentication-Server**: The IP address of the RADIUS authentication server.
- **Radius-Authentication-Port**: The port number for the RADIUS authentication server. Normally, the port number is 1812.
- **Radius-Authentication-Secret**: The password for authentication transaction. You can click on the **Reveal/hide password** icon ( ) on the right side of each field to hide (the default) or reveal the typed string.

3.5.2.2.2.2 Passpoint Parameters

The Passpoint (Hotspot 2.0) feature can be enabled only if the selected Encryption mode is IEEE802.1X/WPA2-EAP.

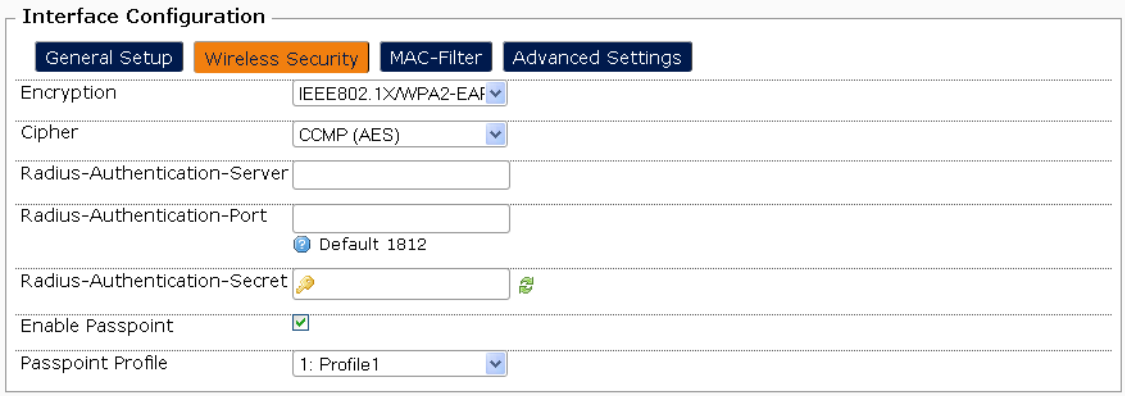


Figure 3-61: Wireless Network Page, Interface Configuration Section, Wireless Security Tab (Passpoint Enabled)

- **Passpoint Enable**: Check to enable Passpoint (the default is unchecked - Passpoint disabled).
- **Passpoint Profile**: Available only if Passpoint is enabled. The drop-down list includes profile ID and name of all configured Passpoint profiles (see "Passpoint Page" on page 91).

3.5.2.2.3 MAC-Filter

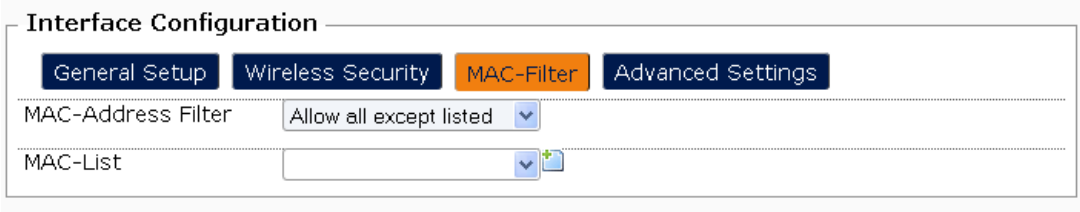


Figure 3-62: Wireless Network Page, Interface Configuration Section, MAC-Filter Tab

- **MAC-Address Filter**: The options are Disable (the default), Allow listed only and Deny all except listed.

A MAC access list is a group of client MAC addresses that can be either permitted or denied access to the network.

If the selected option is **Allow listed only**, only devices with a MAC address included in the MAC-List are allowed to associate to the wireless network, and an association attempt by any device whose MAC address is not included will be rejected.

If the selected option is **Deny all except listed**, an association attempt by any device whose MAC address is included in the MAC-List will be rejected. All devices with a MAC address that is not included in the ACL are allowed to associate to the network.

If either Allow or Deny option is selected, you can define a list of MAC addresses that will be included in the Allow/Deny list.

To add a MAC address to the list, click on the text field to open the drop-down list. The drop-down list includes the MAC addresses of all devices currently connected to the wireless network, plus the "--custom--" option. The --custom-- option enables manually adding a MAC address to the list, using the format xx:xx:xx:xx:xx:xx (or for clearing the entry).

3.5.2.2.2.4 Advanced Settings

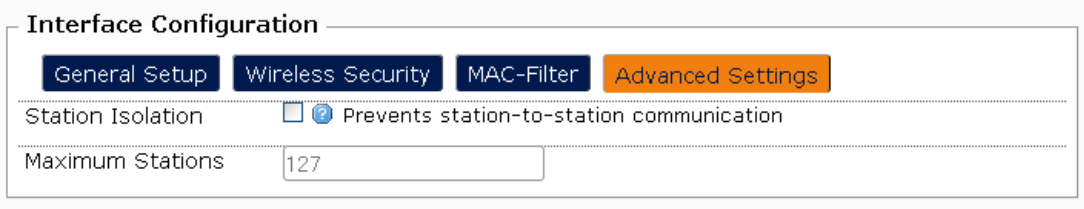


Figure 3-63: Wireless Network Page, Interface Configuration Section, Advanced Settings Tab

The parameters available in the Advanced Settings tab are:

- **Station Isolation**: When Station Isolation is disabled (the default), wireless clients can communicate with one another normally by sending traffic through the wireless network. When Station Isolation is enabled, the device blocks communication between wireless clients on the same wireless network.
- **Maximum Stations**: The maximum number of stations that can associate with the wireless network (the default is 127, which is the maximum allowed).

3.5.3 VLANs Page

NOTE!

In the current release, do not use VLANs when the unit is configured to operate in Router mode.

To access the VLANs page click on the **Network>VLANs** tab in the management function selection panel.

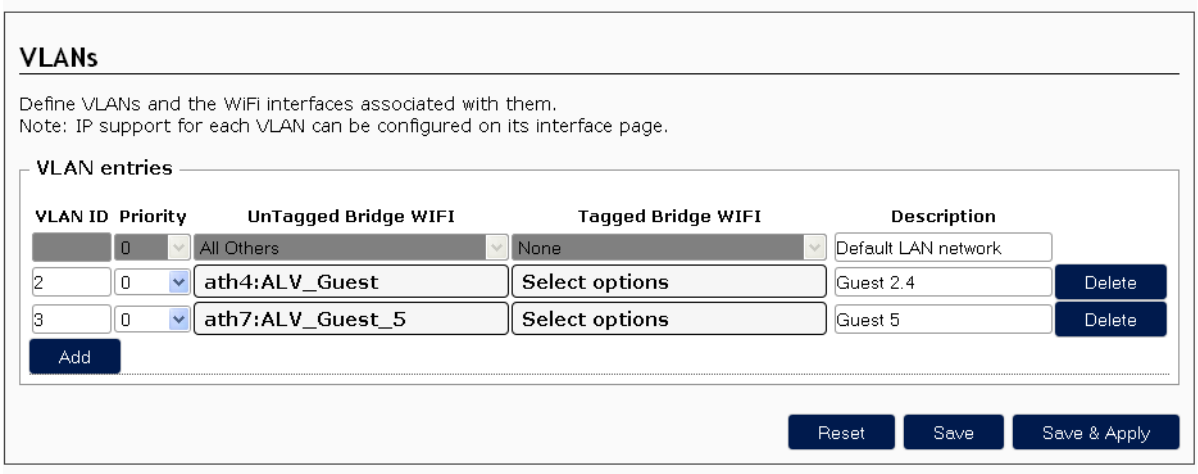


Figure 3-64: Network VLANs Page

The VLANs page enables defining the rules for forwarding traffic between wireless networks and the Ethernet interface (eth0).

One rule is defined by default, with a null VLAN ID. This is the transparent VLAN forwarding rule, defining that all traffic, excluding packets tagged with a VLAN ID to which any wireless network is assigned, will be forwarded between the Ethernet interface and all wireless networks that are not assigned as untagged to any VLAN ID (All Others). This rule cannot be either deleted or modified (excluding the Description).

NOTE! At any given moment, the "All Others" list includes all wireless networks that are not assigned as untagged to any VLAN ID, taking into account possible configuration changes such as adding a new wireless network or cancelling assignment of a wireless network as untagged.

To define a new VLAN forwarding rule, click on the **Add** button to add a new entry and configure the following parameters:

- **VLAN ID**: The VLAN ID (from 2 to 4094).
- **Priority**: The 802.1p based Priority Code Point applied to outgoing packets when a VLAN tag is added. The range is from 0 to 7, the default being 0.
- **Untagged Bridge WIFI**: Click on the definition box to open the wireless network(s) selection dialog box. Select (check) the wireless network(s) to be assigned to the VLAN ID as untagged. You may click on the Check all/Uncheck all options to simplify the selection/de-selection process.

If a wireless network is assigned to a certain VLAN ID (VID) as untagged:

» All untagged traffic arriving from the wireless network will be forwarded to the Ethernet interface (eth0) tagged with the specified VID.

» All traffic arriving to the Ethernet interface tagged with the specified VID will be forwarded untagged to the specified wireless network(s).

- **Tagged Bridge WIFI**: Assignment process is the same as described above for Untagged Bridge WIFI. If a wireless network is assigned to a certain VID as tagged, all traffic from the wireless network tagged with the specified VID will be forwarded to the Ethernet interface as is (tagged with the specified VID), and vice versa.
- **Description**: A text box enabling to configure a description for the VLAN ID forwarding rule.

Note the following configuration rules:

- A wireless network can be assigned as untagged only to a single VLAN ID.
- For a specific VLAN ID, a wireless network can be assigned as either tagged or untagged.

To edit a rule, just modify the relevant parameters.

NOTE!

A VLAN <ID> tab, enabling to open the VLAN <ID> configuration page, is created automatically for each VLAN ID defined in the VLANs page.
VLANs are created without any IP parameters. To configure IP and other parameters open the relevant VLAN <ID> page (Network>Interfaces>VLAN <ID>).

3.5.4 Local DNS Page

To access the Local DNS page click on the **Network>Local DNS** tab in the management function selection panel.

Figure 3-65: Network Local DNS Page

In the Local DNS page you can create and manage of local DNS servers to be used by devices in your network for fast name resolution of other devices in the network.

To configure the parameters of a new host name or to modify an existing entry:

1. Enter the host domain name for a local DNS server in the **Hostname** text field. Do not put www in the domain name. For example: abcd.com is a valid domain name, www.abcd.com is not acceptable.
2. Click on the **IP address** text field to open the drop-down list for available IP addresses. The list includes IP addresses of all potential candidates on your network, plus the "--custom--" option. The --custom-- option enables manually adding an IP address to the list. Select the appropriate IP address or enter it manually.

NOTE!

The IP address of the AP should be configured as the preferred DNS server in the devices in your network in order to interpret these custom hostname(s).

3.5.5 Diagnostics Page

To access the Network Diagnostics page click on the **Network>Diagnostics** tab in the management function selection panel.

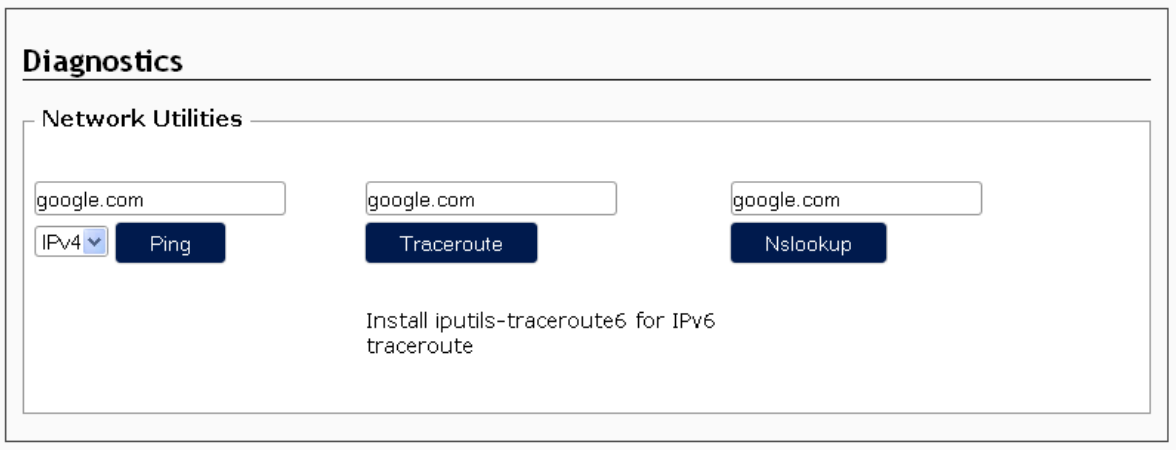


Figure 3-66: Network Diagnostics Page

The Diagnostics enables using the following diagnostic tools:

- Ping
- Traceroute
- Nslookup

3.5.5.1 Ping

Ping is a diagnostic tool for checking connectivity to and measuring transit delay to a destination address.

To perform a ping test:

1. Select whether you want to ping an IPv4 (the default) or an IPv6 address.
2. Enter the destination IP address or host name in the text field.
3. Click on the **Ping** button

5 packets will be sent to the target host. The test results will be displayed below.

3.5.5.2 Traceroute

Trace (or Traceroute) is a diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network.

To perform a traceroute test to a destination device:

1. Enter the destination IP address or host name in the text field.
2. Click on the **Traceroute** button.

The test results will be displayed below.

3.5.5.3 Nslookup

Nslookup is an administrative tool that lets you enter a host name and find out the corresponding IP address. It will also do reverse name lookup and find the host name for an IP address you specify.

To query the IP address of a host by its name:

1. Enter the host name in the text field.
2. Click on the **Nslookup** button.

The query results will be displayed below.

To query the name of a host by its IP address:

1. Enter the host IP address in the text field.

2 Click on the **Nslookup** button.

The query results will be displayed below.

3.5.6 Passpoint Pages

To access the Passpoint page click on the **Network>Passpoint** tab in the management function selection panel.

Wi-Fi Certified Passpoint, also known as Hotspot 2.0, is an industry-wide solution for streamline network access in hotspots eliminating the need for users to find and authenticate a network each time they connect. In Wi-Fi networks that do not support Passpoint, users must search for and choose a network, request the connection to the access point (AP) each time, and in many cases, must re-enter their authentication credentials. Passpoint automates that entire process, enabling a seamless connection between hotspot networks and mobile devices, all while delivering the highest WPA2 security. Passpoint is enabling a more cellular-like experience when connecting to Wi-Fi networks.

The solution supports the following network deployment scenarios:

- Deployment using cellular network credentials for authentication.
- Deployment using non-cellular network credentials for authentication.
- Deployment when network credentials are needed by the device.

For more details about Hotspot 2.0 and relevant configuration guidelines, refer to www.wi-fi.org/file/passpoint-release-2-deployment-guidelines.

To access the Passpoint pages click on the **Network>Passpoint** tab in the management function selection panel. The following pages become available:

- Passpoint Page
- Profile # Pages (4 pages, from Profile 1 through Profile 4).

3.5.6.1 Passpoint Page

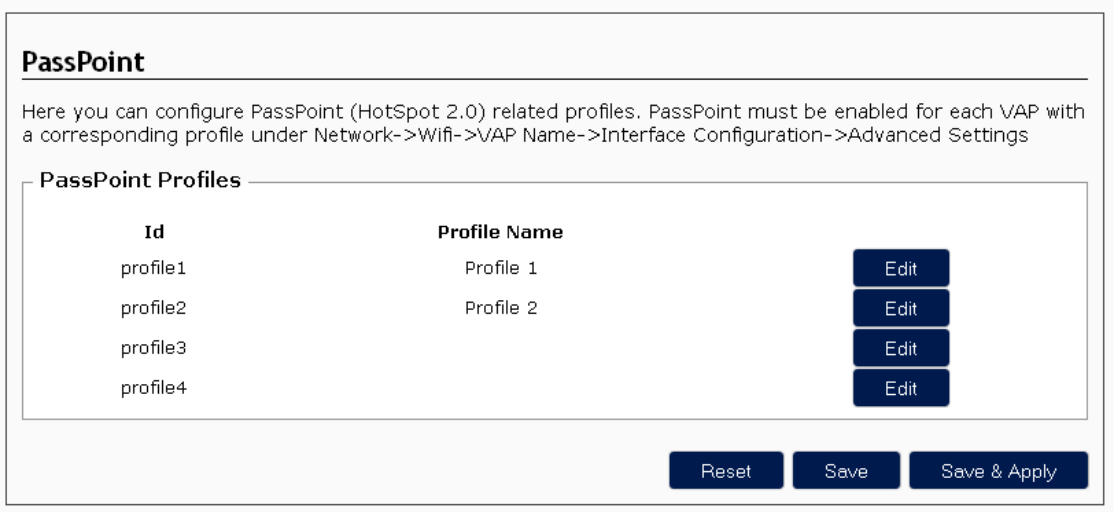


Figure 3-67: Network Passpoint Page

The Passpoint page provides the following details for each of the available profiles:

- **Id**: The read-only profile number (from 1 to 4).
- **Profile Name**: The configured name of the profile.

Click on the **Edit** button on the right side of a profile to open the configuration page for the profile.

For details on enabling Passpoint and selecting profiles to be used on a specific wireless network refer to "Passpoint Parameters" on page 84.

3.5.6.2 Profile # Pages

To access a Profile # (from 1 to 4) page click on the **Network>Passpoint>Profile #** tab in the management function selection panel, or click on the applicable **Edit** button in the PassPoint page.

Each Passpoint profile # page includes the following sections:

- Network Configuration
- Operator Name
- NAI Realm information
- Service Provider Information
- 3GPP Cellular Network information
- Domains
- Provider Authentication
- Venue Configuration

- Online Sign-Up
- Online Sign-Up Icons
- Online SignUp Providers
- IP Address Type Availability
- Connection Capability

3.5.6.2.1 Network Configuration

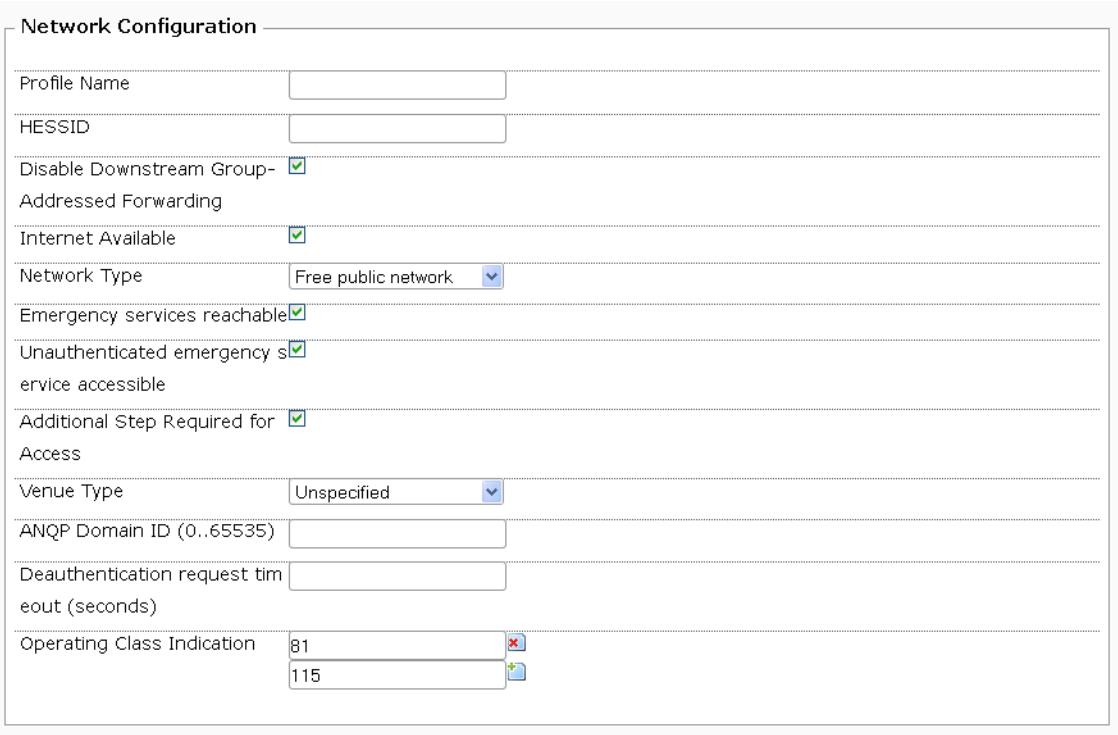


Figure 3-68: Network Passpoint Profile # Page, Network Configuration Section

The Network Configuration section includes the following parameters:

- **Profile Name**: The unique name of the profile.
- **HESSID**: The HESSID (Homogeneous Extended Service Set Identifier) is used to identify a collection of APs, e.g. in a venue, or other "contiguous area". The SP (Service Provider) networks reachable at any one AP is reachable from all the APs configured with the same HESSID. The HESSID, a globally unique identifier, is used to give a single identifier for a group of APs connected to the same SP or other destination network(s). The HESSID is a MAC address that should be configured with the same value as the basic service set identifier (BSSID) of one of the APs in the network. All APs in the wireless network should be configured with the same HESSID value.
- **Disable Downstream Group-Addressed Forwarding**: Check (the default) to disable downstream forwarding of group-addressed (multicast/broadcast) frames.

- **Internet Available**: Checked (the default) to indicate that the network provides connectivity to the Internet. The Hotspot Operator configures this field to inform the connected device whether Internet access is available at a hotspot, which might not be the case in walled-garden environments, where the Hotspot operator (for example, a museum) may limit Wi-Fi access to locally available content. Otherwise (if unchecked) it is unspecified whether the network provides connectivity to the Internet.
- **Network Type**: The following options are available in the drop-down list:
  - » Private network: Non-authorized users are not permitted on this network. Examples of this access network type are home networks and enterprise networks, which may employ user accounts. Private networks do not necessarily employ encryption.
  - » Private network with guest access: Private network but guest accounts are available. Example of this access network type is enterprise network offering access to guest users.
  - » Chargeable public network: The network is accessible to anyone, however, access to the network requires payment. Further information on types of charges may be available through other methods (e.g., IEEE 802.21, http/https redirect or DNS redirection). Examples of this access network type is a hotspot in a coffee shop offering internet access on a subscription basis or a hotel offering in-room internet access service for a fee.
  - » Free public network (the default): The network is accessible to anyone and no charges apply for the network use. An example of this access network type is an airport hotspot or municipal network providing free service.
  - » Personal device network: A network of personal devices. An example of this type of network is a camera attaching to a printer, thereby forming a network for the purpose of printing pictures.
  - » Test or experimental: The network is used for test or experimental purposes only.
- **Emergency service reachable**: Checked (the default) to indicate that emergency service is reachable. Otherwise (if unchecked) it indicates that it is unspecified whether emergency services are reachable
- **Unauthenticated emergency service accessible**: Checked (the default) to indicate that higher layer unauthenticated emergency services are reachable through this AP. Otherwise (if unchecked) it indicates that no unauthenticated emergency services are reachable through this AP.
- **Additional Step Required for Access**: Checked (the default) to indicate that additional steps are required for authentication. Applicable when network credentials are needed by the device, and at least one OSU (Online SignUp) Provider is configured (see "Online SignUp Providers" on page 97).
- **Venue Type**: The Venue Type provides additional information about the group and type of hotspot venue. The group and type descriptors are drawn from the International Code Council's International Building Code document. The default is Unspecified.
- **ANQP Domain ID (0..65535)**: Access Network Query Protocol An identifier for a set of APs in an ESS (Extended Service Set) that share the same common ANQP (Access Network Query Protocol) information. 0 (the default) means that some of the ANQP information is unique to this AP.

- **Deauthentication request timeout (seconds)**: If the RADIUS server indicates that the device is not allowed to connect to the BSS/ESS, the AP can allow the device some time to download a notification page (URL included in the message). This parameter sets that timeout in seconds. The default is null (0).
- **Operating Class Indication**: The Operating Class Indication provides information on the channels and frequency band(s) used by the AP(s) in the hotspot. Passpoint APs may be aware of operating class information (without additional configuration) based on the radio frequency (RF) band capabilities of the individual AP. In a multi-AP hotspot venue, the Hotspot Operator may configure additional information describing the operating classes in use by other APs in the venue having the same SSID. The device may use operating class information to make network selection decisions. If a device supports more than one frequency band (e.g., 5 GHz as well as 2.4 GHz), it may use this information to select a hotspot operating in the 5 GHz band if this is the preferred band and it is available.

  For details on available operating class indications refer to Table E-4 (Global operating classes) in IEEE 802.11-2012 Annex E.

  The default list includes two operating classes: 81 (channel starting frequency 2.407GHz, channel spacing 25MHz, channel set: 1-13) and 115 (channel starting frequency 5GHz, channel spacing 5MHz, channel set: 36, 40, 44, 48).

3.5.6.2.2 Operator Name

The Operator Name includes a list of one or more names in different human languages. This allows the device to display the Operator Friendly Name in alternate languages based on the language selected in the setting of the mobile device. Friendly names can and should be provided in several human languages when the hotspot is located in a country having more than one national language (e.g., Switzerland) or, for example, in locations having a lot of international travelers (e.g., airports). The mobile device will choose from the provided human languages the best choice to display to the user.

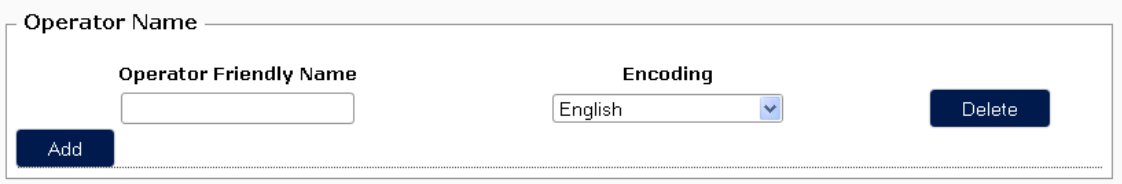


Figure 3-69: Network Passpoint Profile # Page, Operator Name Section

The Operator Name section includes the following parameters for each entry:

- **Operator Friendly Name**: The name of the Hotspot Operator.
- **Encoding**: A drop-down list of languages, allowing to identify the language used for defining the Operator Friendly Name. The default is English.

3.5.6.2.3 NAI Realm information

The NAI Realm List provides a list of Network Access Identifier (NAI) realms corresponding to home service providers which can authenticate a mobile device using different credentials types.

Figure 3-70: Network Passpoint Profile # Page, NAI Realm information Section

The NAI Realm information section includes the following parameters for each entry:

- **Realm**: The NAI Home Realm Name.
- **EAP Method**: In the drop-down list that includes different EAP methods select the EAP method according to the type of credentials used for authentication. The default is EAP-TLS, which is the method used for certificate credentials (for username/password credentials EAP-TTLS should be used).
- **Credential Type**: The type of credentials used by the device for authentication. The default is None, which means server-side authentication only.

3.5.6.2.4 Service Provider Information

The Service Provider Information section includes a list of Roaming Consortiums and Service Providers that are roaming partners of the hotspot. Each element of the list contains an OI (Organizational Identifier, assigned by IEEE) that identifies the Roaming Consortium (group of SPs with an inter-SP roaming agreement) or a single Service Provider.

Registering for an OI is mandatory for large hotspot operators (e.g. national or regional operators) and optional for smaller operators (e.g. hotels)

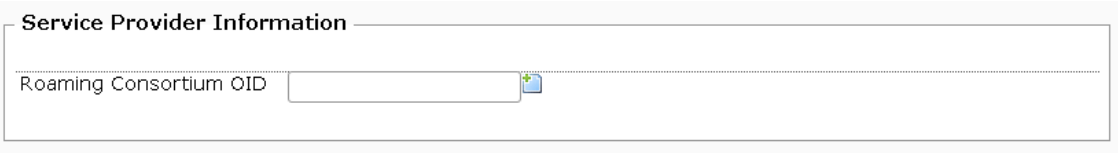


Figure 3-71: Network Passpoint Profile # Page, Service Provider Information Section

3.5.6.2.5 3GPP Cellular Network information

The 3GPP Cellular Network Information section contains a list PLMN (Public Land Mobile Network) IDs of 3GPP (The 3rd Generation Partnership Project) Service Providers that have a roaming agreement with the Hotspot SP. This is to assist a mobile device with Subscriber Identity Module (SIM) or Universal SIM

(USIM) credentials issued by a 3GPP home provider to establish whether the AP has a roaming arrangement with 3GPP SPs.

Figure 3-72: Network Passpoint Profile # Page, 3GPP Cellular Network information Section

Each entry is a PLMN ID that comprises the following elements:

- **MCC**: Mobile Country Code (3 digits).
- **MNC**: Mobile Network Code (2 or 3 digits).

3.5.6.2.6 Domains

The Domains section includes a list of one or more domain names of the entity operating the hotspot network. It is possible that a Hotspot Operator might have more than one domain name that it uses to identify itself.

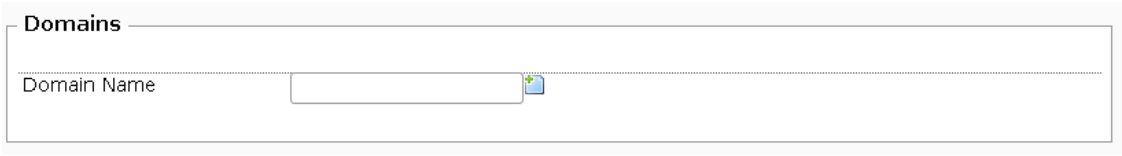


Figure 3-73: Network Passpoint Profile # Page, Domains Section

3.5.6.2.7 Provider Authentication

The Provider Authentication section provides the authentication type when ASRA (Additional Step Required for Access, see in "Network Configuration" on page 91) is set to true (checked).

Figure 3-74: Network Passpoint Profile # Page, Provider Authentication Section

The Provider Authentication parameters are:

- **Authentication Type**: The drop-down list includes the following options:
  - » Acceptance of terms and conditions: The user will be required to accept agreement's terms and conditions.
  - » On-line enrollment supported: The network supports on line enrollment. Higher layer protocols may indicate to the user that accounts may be created.
  - » http/https redirection: The network infrastructure performs http/https redirect.
  - » DNS redirection: The network supports DNS redirection. Higher layer software will exchange credentials with the network.
- **Redirect URL**: Applicable only if the selected Authentication Type is http/https redirect. The URL to which the user will be redirected for authentication.

3.5.6.2.8 Venue Configuration

The Venue Configuration section provides optional general information about the hotspot. Venue Configuration elements can and should be provided in several human languages when the hotspot is located in a country having more than one national language (e.g., Switzerland) or, for example, in locations having a lot of international travelers (e.g., airports). The mobile device will choose from the provided human languages the best choice to display to the user.

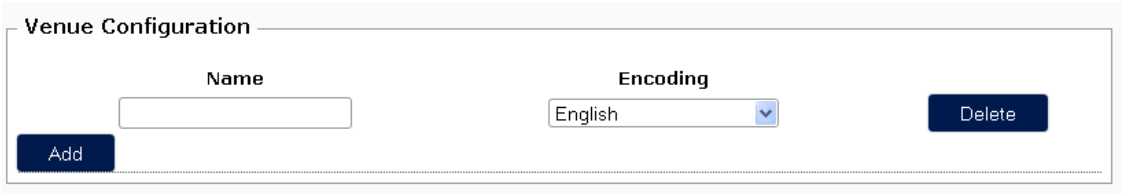


Figure 3-75: Network Passpoint Profile # Page, Venue Configuration Section

The Venue Configuration section includes the following parameters for each entry:

- **Name**: The name of the venue.
- **Encoding**: A drop-down list of languages, allowing to identify the language used for defining the venue's Name. The default is English.

3.5.6.2.9 Online Sign-Up

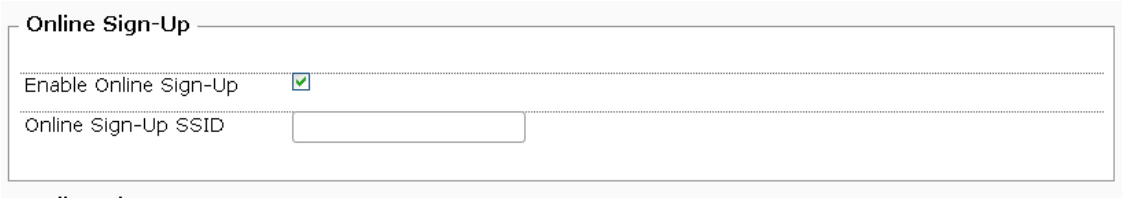


Figure 3-76: Network Passpoint Profile # Page, Online Sign-Up Section

The Online Sign-Up section includes the following parameters:

- **Enable Online Sign-Up**: Check to enable Online Sign-Up. The default is disabled (unchecked).
- **Online Sign-Up SSID**: Available only of Online Sign-Up is enabled (checked). The SSID used for all OSU (online Sign-Up) connections to all the listed OSU Providers (see "Online SignUp Providers" on page 97).

3.5.6.2.10 Online Sign-Up Icons

The Online Sign-Up Icons section contains optional icons of available OSU (Online Sign-Up) Providers to support Icon Request & Response exchange between the device and the AP when the mobile device is configured to display the OSU Icon.

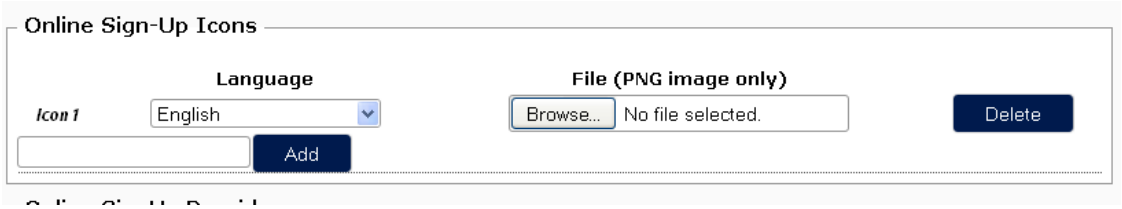


Figure 3-77: Network Passpoint Profile # Page, Online Sign-Up Icons Section

To add an OSU Icon enter it's name in the text box on the left side of the **Add** button and click on the button.

The Online Sign-Up Icons section includes the following parameters for each entry:

- **Language**: A drop-down list of languages, allowing to identify the language used for defining the icon. The default is English.
- **File**: The icon's PNG file. Click on the **Browse** button to load the suitable icon file.

3.5.6.2.11 Online SignUp Providers

The Online SignUp Providers List ANQP-element contains a list of entities that offer online sign-up service at the hotspot.

Figure 3-78: Network Passpoint Profile # Page, Online SignUp Providers Section

The **Online SignUp Server URL** is a mandatory parameter when defining a new Online SignUp Provider. An entry in which the **Online SignUp Server URL** is empty enables definition of additional parameters for the last Online SignUp Provider.

The Online SignUp Providers section includes the following parameters for each entry:

- **Online SignUp Server URL**: The URL of the OSU server. If left empty it indicates that additional parameters are applied to the last defined server.
- **Online SignUp Friendly Name**: For each OSU Provider one or more names in different human languages can be configured. This allows the device to display the name in alternate languages based on the language selected in the setting of the mobile device. Friendly names can and should be provided in several human languages when the hotspot is located in a country having more than one national language (e.g., Switzerland) or, for example, in locations having a lot of international travelers (e.g., airports). The mobile device will choose from the provided human languages the best choice to display to the user.
- **Online SignUp NAI**: Network Access Identifier (NAI) realm(s) that can be used by the OSU Provider (see also "NAI Realm information" on page 94).
- **Online SignUp method list**: The preferred list of encoding methods that the OSU server supports in order of priority.
- **Icon**: The icon(s) associated with the OSU Provider. The drop-down list includes all relevant icons (see "Online Sign-Up Icons" on page 97). The default is None.
- **Language**: A drop-down list of languages, allowing to identify the language used for defining the language dependent parameters (Online SignUp Friendly Name, Icon, Description) that are displayed to the user. The default is English.
- **Description**: The SP's description of the service offering.

3.5.6.2.12 IP Address Type Availability

The IP Address Type Availability parameters provides information about the IP address version and type that the Hotspot Operator uses and that would be allocated and available to a mobile device after it authenticates to the network.

The the information in the AP should be configured to reflect the IP address configuration of the wireless area network (WAN) router, the Dynamic Host Configuration Protocol (DHCP) server if present, and the firewall behind the AP.

When direct access to a single core network (e.g., the 3GPP Evolved Packet Core [EPC]) is provided, IP Address Type Availability configuration may take into account the address type supported by the core network.

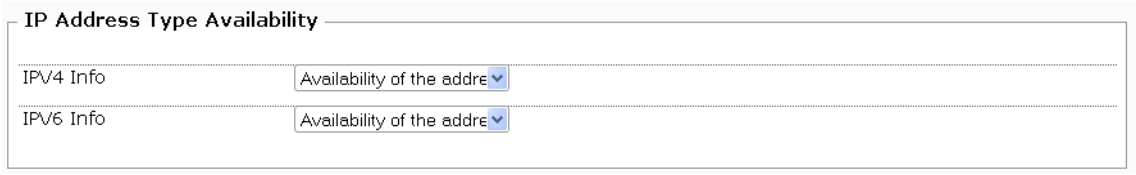


Figure 3-79: Network Passpoint Profile # Page, IP Address Type Availability Section

The IP Address Type Availability section includes the following parameters:

- **IPV4 Info**: The available options are:
  - Address type not available: The Hotspot Operator cannot allocate an IPv4 address to the mobile devices.
  - Public IPv4 address available: The hotspot allocates a public IPv4 address to the mobile device after association.
  - Port-restricted IPv4 address available: Not used currently.
  - Single NATed private IPv4 address available: The hotspot allocates a private IPv4 address to the mobile device after association.
  - Double NATed private IPv4 address available: Access to a single core network is provided and the combination of the hotspot network and the core network allocates a double-NAT IPv4 address to the mobile device after association.
  - Port-restricted public IPv4 address and single NATed IPv4 address available: Not used currently.
  - Port-restricted public IPv4 address and double NATed IPv4 address available: Not used currently.
  - Availability of the address type is not known: Address allocation is outside the Hotspot Operator's administrative control.

  The default is "Availability of the address type is not known".
- **IPV6 Info**: The available options are:
  - Address type not available: The Hotspot Operator cannot allocate an IPv4 address to the mobile devices.
  - Address type available: The Hotspot Operator is able to natively route IPv6.
  - Availability of the address type is not known: Address allocation is outside the Hotspot Operator's administrative control.

The default is "Availability of the address type is not known".

3.5.6.2.13 Connection Capability

The Connection Capability section provides information on the status of commonly used communication protocols and ports in the hotspot.

The Hotspot Operator should configure the AP with information regarding each of the commonly used protocol and port number values as either closed, open or unknown. Reasonable efforts should be made to avoid using the value "unknown".

The mobile device uses connection capability information to make network selection decisions by determining which services are blocked or supported at the hotspot.

Figure 3-80: Network Passpoint Profile # Page, Connection Capability Section

Each entry defines the status for a certain combination of IP protocol and destination port number. The Connection Capability parameters are:

- **Protocol**: The IP protocol. The options available in the drop-down list are:
  - ICMP (Internet Control Message Protocol)
  - TCP (Transmission Control Protocol)
  - UDP (User Datagram Protocol)
  - ESP (Encapsulating Security Payload)
- **Port**: The destination port number.
- **Port Status**: The options available in the drop-down list are:
  - Closed: The IP protocol or the associated port number is not open for communication (i.e., it is blocked by a firewall or a Network Address Translation function) in the access network.
  - Open: The IP protocol or the associated port number is open for communication (i.e., it is not blocked by a firewall or NAT function) in the access network.
  - Unknown: The exact status is not known. The IP protocol or the associated port number may or may not be open for communication in the access network.

3.6 APController

Layer Two Tunneling Protocol (L2TP) is used to enable the operation of a virtual private network (VPN) for securely managing devices over the Internet using SNMPv3. CHAP (Challenge-Handshake Authentication Protocol) is used to validate the identity of remote clients and provide data channel protection against malicious data insertion.

The APController tab provides access to the following second-level management function tabs:

- AP Controller Page
- SNMPv3 AP to APC Page

3.6.1 AP Controller Page

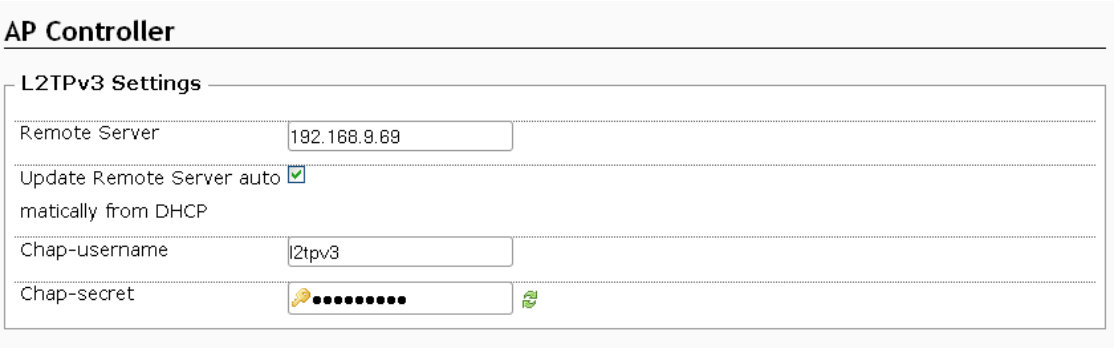


Figure 3-81: APController AP Controller Page

The AP Controller page includes the following sections:

- L2TPv3 Settings
- IPSec

3.6.1.1 L2TPv3 Settings

The L2TPv3 Settings sections includes the following L2TPv3 parameters:

- **Remote Server**: The IP address of the Arena station used for managing the unit.
- **Update Remote Server automatically from DHCP**: Check (the default) to automatically update the IP address of the Arena server using DHCP.

NOTE!

To support automatic update using DHCP the DHCP server should be configured to return the Arena controller's IP address through the Vendor Specific Option Code (option 43) in the DHCP reply.

Option 60 (Vendor Class Identifier) in WBSn units is set to WL_AP.

If the Vendor Class Identifier (VCI) received at the DHCP server is WL_AP, The DHCP server will send back the controller IP addresses (could be more than one address, e.g. a backup server) under option 43, using TLV blocks defined in this way:

- **Type**: 0x33 Hex (=51 Decimal)
- **Length**: A count of the characters of the ASCII string in the Value field. Length must include the commas if there is more than one controller specified, but not a zero-terminator.
- **Value**: A non-zero terminated ASCII string that is a comma-separated list of controllers. No spaces should be embedded in the list.

The encoded hex value is assembled by concatenating the TLV values: **Type + Length + Value**.

Type is always 0x33(hex). Length is the number of controller IP addresses times 4 in hex.

Value is the IP address of the controller listed sequentially in hex.

For example: Assume two controllers with management interface IP addresses, 0.126.126.2 and 10.127.127.2. The type is 0x33(hex). The length is 2*4 = 8 = 08 (hex). The IP addresses translate to 0a7e7e02 and 0a7f7f02. Assembling the string then yields 33080a7e7e020a7f7f02.

- **Chap-Username**: The User Name for Challenge-Handshake Authentication Protocol (CHAP).
- **Chap-secret**: The Chap Secret. The default is abcd12345.

NOTE!

The CHAP settings in the device must match the settings in the controller used for managing it.

3.6.1.2 IPSec

IPSec is not supported in the current release. The **Pre-shared key** parameter is for future use when IPSec will be supported.

3.6.2 SNMPv3 AP to APC Page

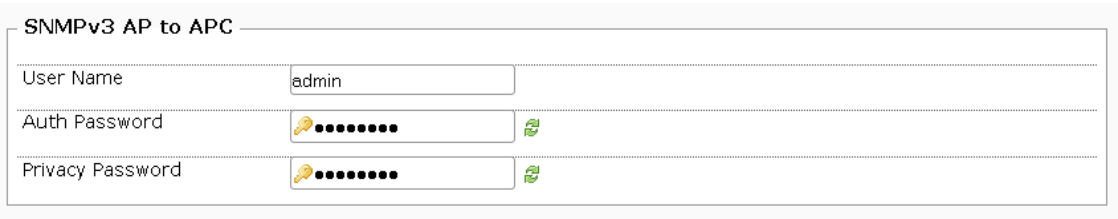


Figure 3-82: APController SNMPv3 AP to APC Page

SNMPv3 AP to APC settings define the SNMPv3 parameters to be used for managing the unit by an Arena controller.

NOTE!

The SNMPv3 AP to APC settings may differ from the settings of the standard SNMPv3 parameters (see "SNMP Page" on page 46) used for any other purpose.

The SNMPv3 AP to APC parameters are:

- **User Name**: The name assigned to the SNMP user. The default is admin.
- **Auth Password**: The password used for authentication using the MD5 protocol. A string of at least 8 characters. The default is password. You can click on the **Reveal/hide password** icon ( ) on the right side of the text field to hide (the default) or reveal the typed string.
- **Privacy Password**: The password used for encrypting the SNMP traffic using the CBC-DES protocol. A string of at least 8 characters. The default is password. You can click on the **Reveal/hide password** icon ( ) on the right side of the text field to hide (the default) or reveal the typed string.

NOTE!

The SNMPv3 AP to APC settings in the device must match the settings in the Arena controller used for managing it.

3.7 Statistics

Click on the Statistics option to open the Graphs third-level tabs, enabling to select an item for viewing relevant performance graph(s).

You can select the time span for which performance graph(s) will be displayed. The available options in the drop down list are 1hour (the default), 1day and 3day. Select the required option and click on the **Display timespan>>** button to view relevant graph(s) for the selected time span.

The Average (Avg) and Last values for each of the relevant performance parameters are displayed below the graph (excluding Interfaces graphs in which calculated Totals for the displayed time span are provided instead of Last values).

NOTE!

For certain graphs in which graphs are displayed for two or more parameters, the graphs display stacked values. For example, in the Wireless Radio Traffic graphs (see "Radio Page" on page 105), the graph for Packets (RX) displays actual values, while the graph for Packets (TX) displays the stacked values [Packets (RX) + Packets (TX)].

The available Statistics pages are:

- CPU Page
- Wireless Pages
- Interfaces Page
- System Load Page
- Memory Page
- Activity Pages
- TCP Connections Pages

3.7.1 CPU Page

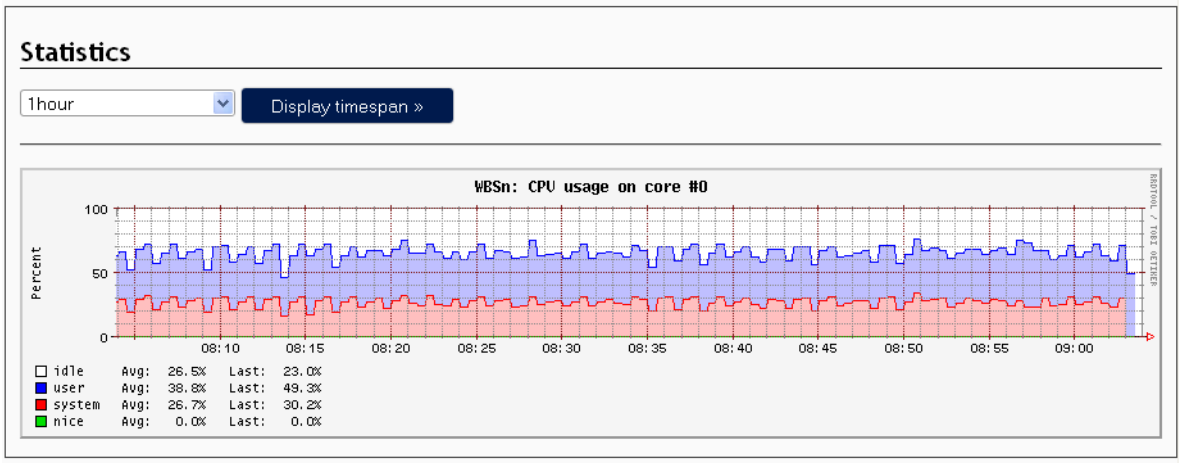


Figure 3-83: Statistics CPU Usage Graph

The CPU page provides a graph displaying CPU utilization (in %) by user, system, nice and idle categories of processes.

3.7.2 Wireless Pages

The Wireless option enables viewing Wireless page as well as the following pages:

- Associations Page
- Radio Page

The Wireless page includes all the graphs available in both the Associations and Radio pages.

3.7.2.1 Associations Page

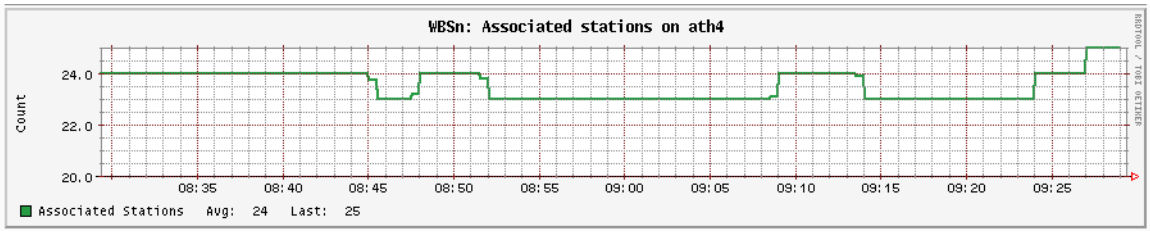


Figure 3-84: Statistics Wireless Associated Stations Graph

The Association page includes a graph for each of the configured wireless networks (identified by the ath# interface). Each graph displays the number of stations associated on this wireless network.

3.7.2.2 Radio Page

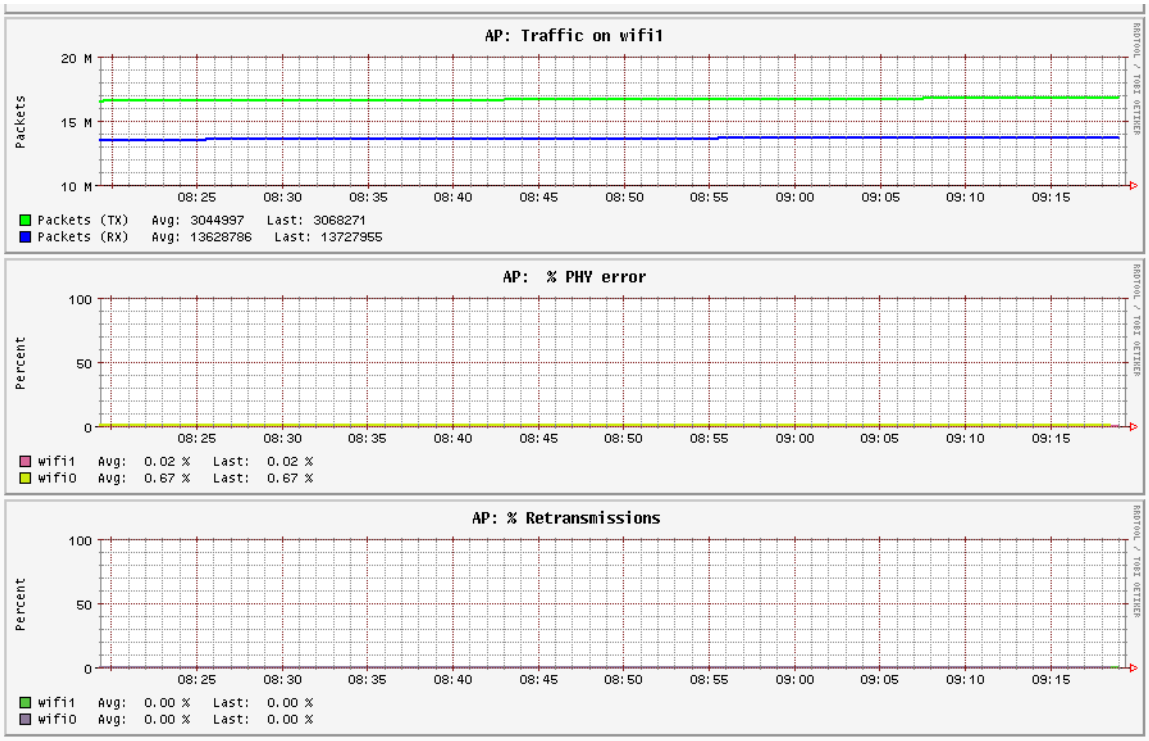


Figure 3-85: Statistics Wireless Radio Page Graphs

The Radio page provides the following graphs:

- **Traffic** graph for each of the supported radios, displaying accumulated numbers of received (RX) and transmitted (TX) Packets.
- **% PHY error** graph, displaying for each of the supported radios the total number of packets received with a PHY error as percentage of total received packets.
- **% Retransmissions** graph, displaying for each of the supported radios the total number of retransmitted packets as percentage of all transmitted packets.

3.7.3 Interfaces Page

The Interfaces page provides the following graphs for each of the relevant interfaces:

- **Traffic**

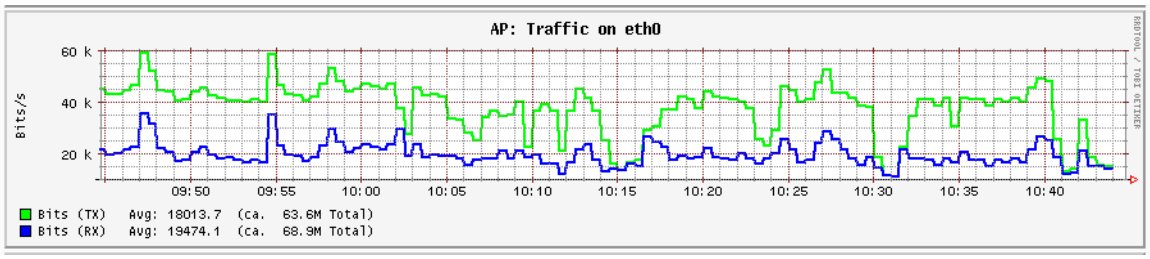


Figure 3-86: Statistics Interfaces Traffic Graph

The Traffic graph displays the following performance parameters on the relevant interface in Bits/second:

- Bits (TX)
- Bits (RX)

Packets

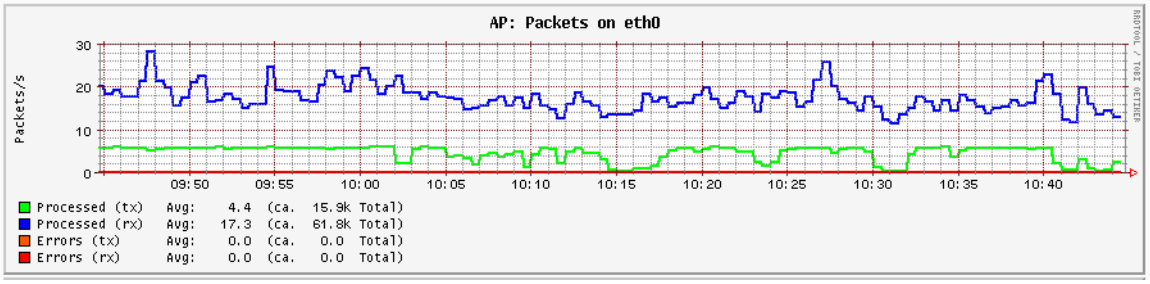


Figure 3-87: Statistics Interfaces Packets Graph

The Packets graph displays the following performance parameters on the relevant interface in Packets/second:

- Processed (tx)
- Processed (rx)
- Errors (tx)
- Errors (rx)

3.7.4 System Load Page

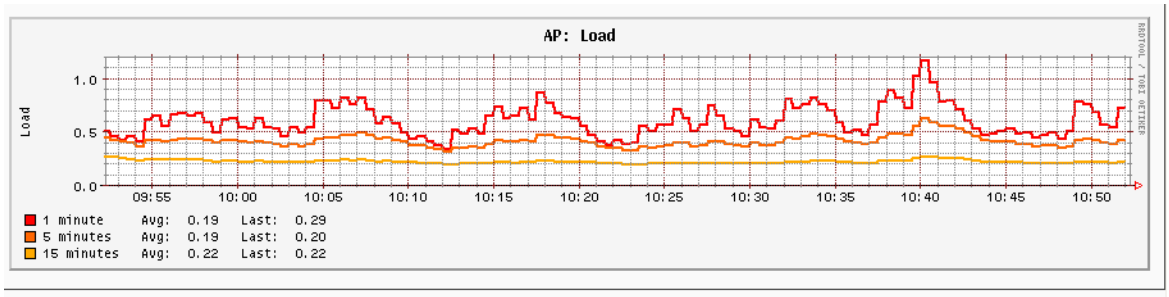


Figure 3-88: Statistics System Load Graph

The System Load page provides a graph displaying the CPU load parameters (1 Minute, 5 Minutes and 15 Minutes).

3.7.5 Memory Page

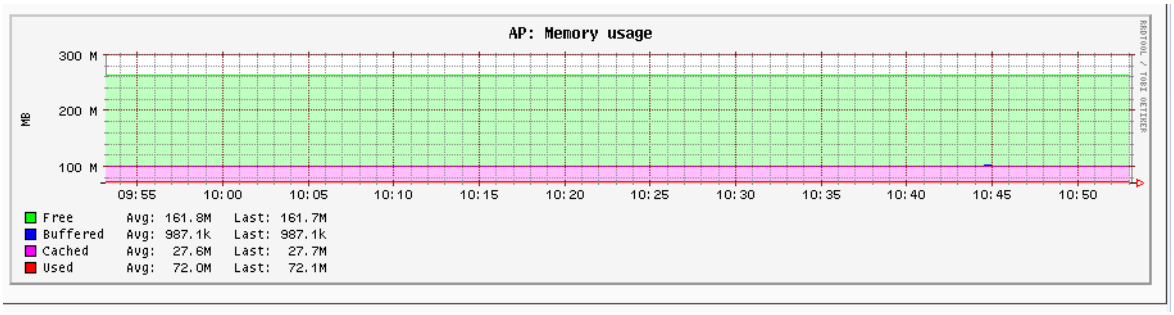


Figure 3-89: Statistics Memory Usage Graph

The Memory page provides a graph displaying memory usage (Free, Buffered, Cached and Used) in MB.

3.7.6 Activity Pages

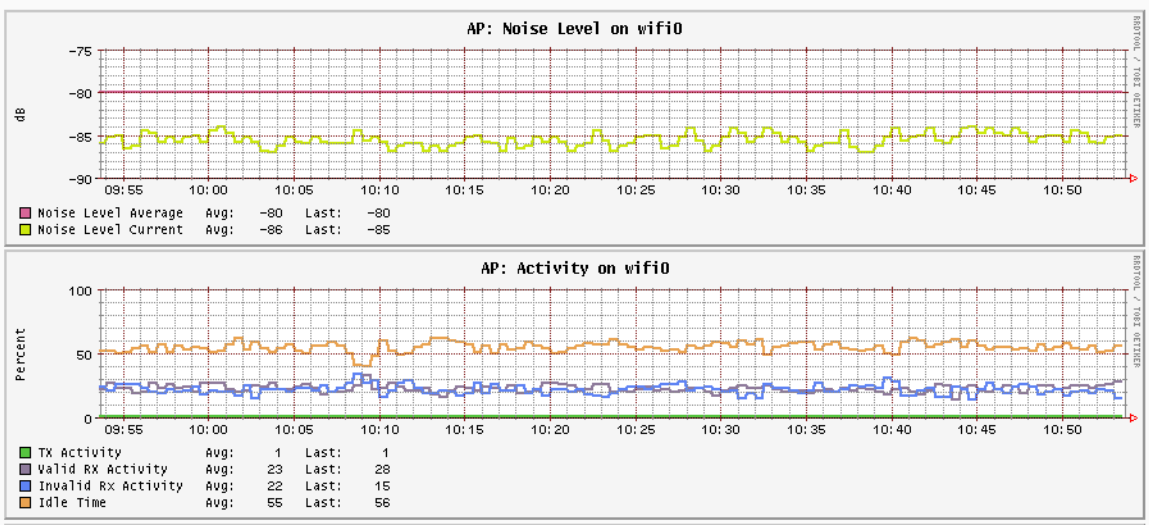


Figure 3-90: Statistics Activity Graphs

The Activity page provides the following graphs for each of the supported radios:

- **Noise Level** graph, displaying the Average and Current Noise Levels in dBm on the radio.
- **Activity** graph, displaying the percentage of time consumed by the following activities:
  - TX Activity
  - Valid RX Activity
  - Invalid RX Activity
  - Idle Time

You can elect to view a per-radio page displaying only the graphs for the selected radio.

3.7.7 TCP Connections Pages

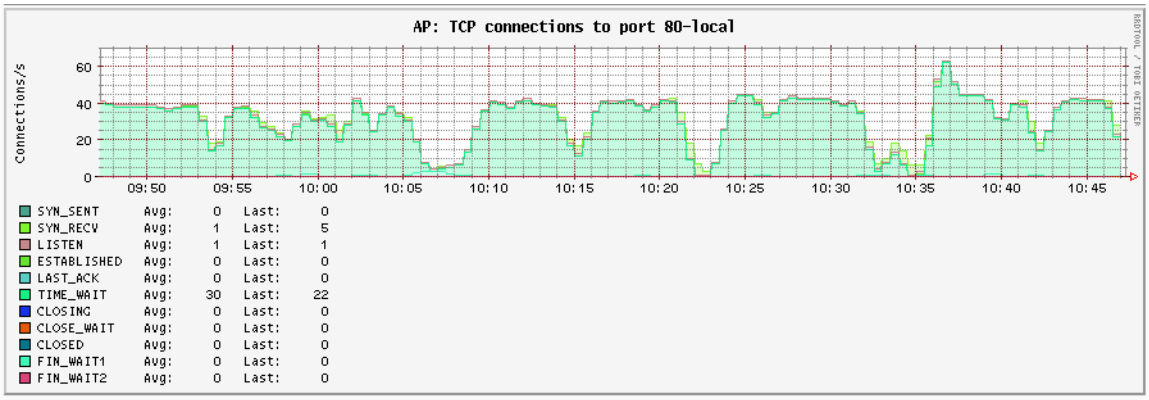


Figure 3-91: Statistics TCP Connections Graph

The TCP Connection provides graphs displaying the number of TCP connections in various states. Graphs are provided for port 80 (HTTP) and port 22 (SSH).

You can elect to view a per-port page displaying only the graph for the selected port.

Appendix A - Troubleshooting

In this Appendix:

A.1 Base Station LEDs Description

Table A-1: Base Station LEDs Description

LED	Description
 Status	Off: No power or start of reboot. Red: Reboot in progress. Blinking Green: Systen Initialization. Solid Green: Normal operation. Orange: Rescue mode is running (see "Restarting the Unit in Rescue Mode" on page 112).
 Wireless	Applicable only during normal operation (Status LED is green). Off: No radio is on. Orange: Only one radio is on Green: Both radios are on
 Ethernet	Off: No Ethernet activity. Blinking Green: Ethernet activity indication.

A.2 Using the Reset Button of the Base Station

The recessed Reset (RST) button is located below the USB button. To use it remove the plastic cap used for sealing the USB connector and the RST button).

CAUTION

After using the Reset button, ensure the button and USB connector are properly sealed with the plastic cap.

The Reset button enables the following actions:

A.2.1 Resetting the Base Station

To reset the unit during normal operation, use a sharp object to press the Reset button for a short time. This will cause a hard-reset operation equivalent to disconnecting/reconnecting power to the unit (Reboot actions executed from the management system cause soft-reset).

A.2.2 Returning the Base Station to Factory Default Configuration

To return to factory default configuration press the Reset button continuously for at least 20 seconds (but less than 40 seconds). The unit will reset and restart using the factory default configuration (including management IP parameters).

A.2.3 Restarting the Unit in Rescue Mode

Rescue Mode is a special operation mode allowing to access the unit when it does not operate properly for one of the following reasons:

1. Frequent power interruptions - when the power disconnects/reconnects on several concurrent occasions within a few minutes.
2. Inability to manage the unit due to a configuration problem.
3. The firmware files in both banks are corrupted.

Under the above conditions it is impossible the access the unit using the management applications or perform a reset.

To restart the unit in rescue mode press the Reset button continuously for at least 40 seconds. The unit will reset and restart in rescue mode, allowing access through a simplified web interface using the default IP address (192.168.1.1), regardless of the regular operational IP address:

Figure A-1: Rescue Mode Entry Screen

NOTE!

If you do not login to the system through the simplified web interface within ten minutes of entering Rescue Mode, the system will automatically reboot and try to load the regular operational version. If you log in through this interface, the system will stay in rescue mode until rebooted manually.

If the reason you entered Rescue Mode is repeated power interruptions (reason 1 above), click on the **Reboot** button. The unit should restart in normal operation.

If the reason you entered Rescue Mode is because the device does not operate properly and you are not able to access the EMS utility even after reboot, try solving the problem by to uploading a correct firmware file without changing the current configuration:

1. Click on the **Choose File** button and navigate to the location of the appropriate dlv file (should be a firmware file known to be good) and select it. The name to the selected file will be displayed.
2. Select the firmware bank (0 or 1) to which the selected file will be loaded.
3. Click on the **Upload** button. The progress of the upload process is displayed. At the end of the process the result is indicated.

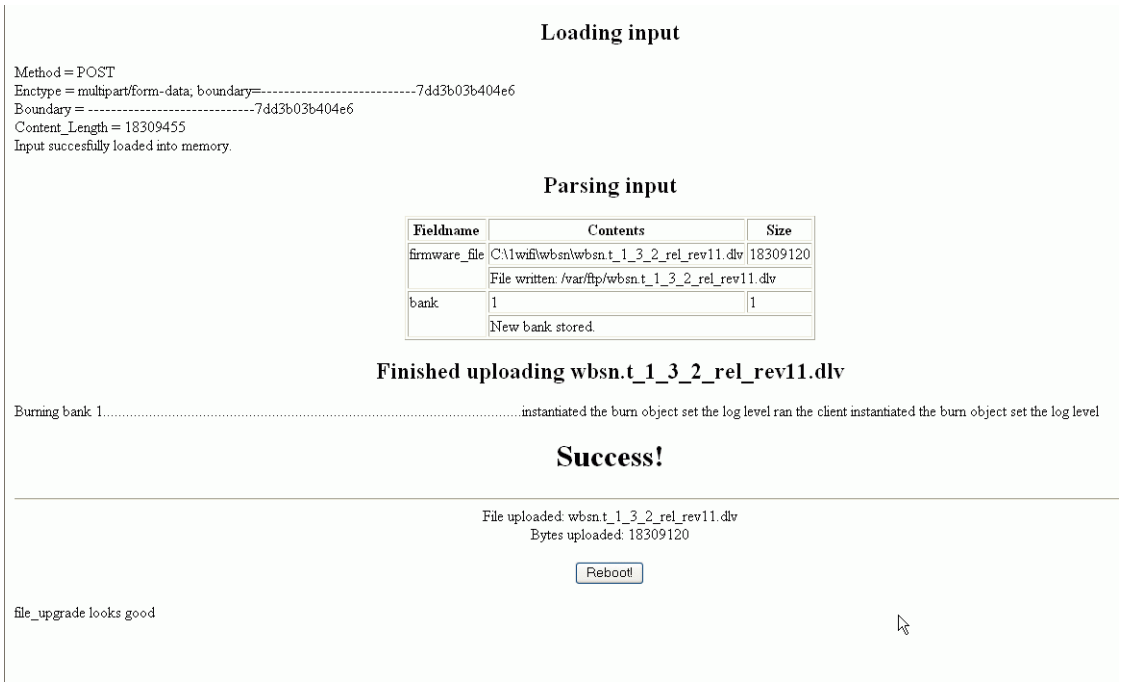


Figure A-2: Rescue Mode - Upgrade Progress Screen

NOTE!

It is highly recommended to upload the firmware file to both banks before rebooting the unit, regardless of the order in which they are loaded.

4 After successful completion of the upload process, click on the **Reboot** button. After reset the unit should resume normal operation using the uploaded firmware.

If normal operation is not resumed after uploading a good firmware file, then most probably there is a configuration problem. Click on the **Default Configuration** button. After a few minutes the unit should restart using the factory default configuration.

INFORMATION

Click on the **Flash State** button if you wish to verify which software files are installed in the base station.

Appendix B - Preparing Ethernet Cables

In this Appendix:

B.1 Preparing the Base Station's Ethernet Cable

NOTE!

Use only Category 5e (or higher) outdoors Ethernet cable.

Use only shielded RJ-45 8-pin modular plugs.

Make sure that the length of the Ethernet cable is sufficient for reaching from the intended location of the base station to the intended location of the indoor equipment.

The combined length of the outdoor Ethernet cable (from the base station to the PoE Injector) and the Ethernet cable connecting the PoE Injector to the data networking equipment should not exceed 100 meters.

1 The unit is supplied with the sealing gland attached to the Ethernet (ETH) connector.

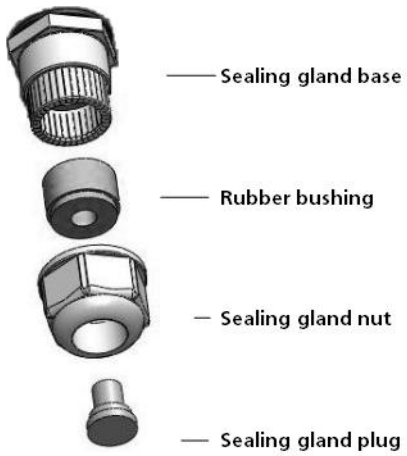


Figure B-1: Ethernet Sealing Gland Components

CAUTION

Do not attempt to remove the sealing gland base from the unit.

The USB port is for engineering purposes only. Ensure that the USB port is always properly sealed with the plastic cap.

2 Unscrew the nut (use the extraction key supplied with the unit or an equivalent tool) and remove it from the base.

3 Remove the rubber bushing (inner sleeve) from the base of the gland.

4 Remove the plug from the nut and feed the Ethernet cable through the nut and rubber bushing.

Figure B-2: Ethernet Cable Routed Through Nut and Bushing

5 Insert and crimp the shielded RJ-45 connector. 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. All 8 pins must be connected (see details in Table B-1 below). 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 gland 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 provide a good connection with the connector's shield after crimping. To ensure a good shielding connection solder the shield wire to the connector's shield after crimping.

6 Connect the cable to the Ethernet connector.

7 Firmly push the rubber bushing back into place inside the base of the gland.

8 Close the nut using the extraction key supplied with the unit or an equivalent tool and tighten it firmly to ensure proper sealing.

The PoE Injector provides power over 1Gbps Ethernet, meaning that there are no spare wires. All wires are used for power and data concurrently:

Table B-1: Base Station Ethernet Cable - RJ-45 PoE Pins

Pin	Signal	Wire Color	Description
1	BI_DA+	Orange-White	Bi-directional pair A +, PoE GND
2	BI_DA-	Orange	Bi-directional pair A -, PoE GND
3	BI_DB+	Green-White	Bi-directional pair B +, PoE +55V
4	BI_DC+	Blue	Bi-directional pair C +, PoE +55V
5	BI_DC-	Blue-White	Bi-directional pair C -, PoE +55V
6	BI_DB-	Green	Bi-directional pair B -, PoE +55V
7	BI_DD+	Brown-White	Bi-directional pair D +, PoE GND
8	BI_DD-	Brown	Bi-directional pair D -, PoE GND