Wireless access point

WEP-2L

User manual
Firmware version 1.1.0

IP address: 192.168.1.10

Username: admin

Password: password

Contents

1 Introduction ... 5
1.1 Annotation ... 5
1.2 Symbols ... 5
2 Device description ... 6
2.1 Purpose ... 6
2.2 Device specification ... 6
2.3 The device technical parameters ... 7
2.4 Design ... 9
2.4.1 Device main panel ... 9
2.5 Light indication ... 10
2.6 Reset to the default settings ... 10
2.7 Delivery package ... 10
3 Rules and recommendations for device installation ... 11
3.1 Safety rules ... 11
3.2 Installation recommendations ... 11
3.3 Calculating the number of required access points ... 11
3.4 Channel selection for neighboring access points ... 12
4 Installing WEP-2L ... 14
4.1 Wall mounting ... 14
4.2 Installing to false ceiling ... 15
4.3 Removing the device from the bracket ... 15
5 Device management via the WEB interface ... 16
5.1 Getting started ... 16
5.2 Applying configuration and discarding changes ... 17
5.3 WEB interface basic elements ... 18
5.4 The «Monitoring» menu ... 19
5.4.1 The «Wi-Fi clients» submenu ... 19
5.4.2 The «Traffic Statistics» submenu ... 20
5.4.3 The «Scan Environment» submenu ... 22
5.4.4 The «Events» submenu ... 23
5.4.5 The «Network Information» submenu ... 24
5.4.6 The «Radio Information» submenu ... 26
5.4.7 The «Device Information» submenu ... 27

5.5 The «Radio» menu 28
5.5.1 The «Radio 2.4 GHz» submenu 28
5.5.2 The «Radio 5 GHz» submenu 31
5.5.3 The «Advanced» submenu 35
5.6 The «VAP» menu 36
5.6.1 The «Summary» submenu 36
5.6.2 The «VAP» submenu 37
5.7 The «Network Settings» menu 40
5.7.1 The «System Configuration» submenu 40
5.7.2 The «Access» submenu 41
5.8 The «External Services» menu 42
5.8.1 The «Captive Portal» submenu 42
5.9 The «System» menu 43
5.9.1 The «Device Firmware Upgrade» submenu 43
5.9.2 The «Configuration» submenu 44
5.9.3 The «Reboot» submenu 44
5.9.4 The «Password» submenu 45
5.9.5 The «Log» submenu 45
5.9.6 The «Date and Time» submenu 46
6 Managing the device using the command line 48
6.1 Connection to the device 48
6.2 Network parameters configuration 48
6.3 Virtual Wi-Fi access points (VAP) configuration 49
6.3.1 Configuration of VAP without encryption 49
6.3.2 Configuration of VAP with WPA-Personal security mode 50
6.3.3 Configuration of VAP with Enterprise authorization 51
6.3.4 Configuration of VAP with Captive Portal 52
6.3.5 Advanced VAP settings: 52
6.4 Radio configuration 53
6.4.1 Advanced Radio settings: 54
6.5 System settings 56
6.5.1 Device firmware update 56
6.5.2 Device configuration management 57
6.5.3 Device reboot 57

6.5.4 Setting the date and time 58
6.6 APB service configuration 58
6.7 Monitoring 59
6.7.1 Wi-Fi Clients 59
6.7.2 Device info 60
6.7.3 Network information 61
6.7.4 Wireless interfaces 62
6.7.5 Event logging 62
6.7.6 Spectrum Analyzer 63
7 The list of changes 64

1 Introduction

1.1 Annotation

Modern tendencies of telecommunication development necessitate operators to search for the most optimal technologies, allowing you to satisfy rapidly growing needs of subscribers, maintaining at the same time consistency of business processes, development flexibility and reduction of costs of various services provision. Wireless technologies are spinning up more and more and have paced a huge way for short time from unstable low-speed communication networks of low radius to broadband networks equitable to speed of wired networks with high criteria to the quality of provided services.

WEP-2L is dedicated to be installed inside buildings as an access point and to create a seamless wireless network using several identical access points («Roaming») on a large area.

This manual specifies intended purpose, main technical parameters, design, safe operation rules and installation and configuration recommendations for WEP-2L.

1.2 Symbols

Notes contain important information, tips or recommendations on device operation and setup.

Notes and warnings

Warnings are used to inform the user about harmful situations for the device and the user alike, which could cause malfunction or data loss.

2 Device description

2.1 Purpose

WEP-2L wireless access point is designed for provision of users' access to high-speed safe network.

The device is dedicated to create L2 wireless networks interfacing with a wired network. WEP-2L is connected to a wired network via 10/100/1000M Ethernet interface and arrange high-speed access to the Internet for devices supporting Wi-Fi technology at 2.4 and 5 GHz.

The device has two radio interfaces to organize two physical wireless networks.

WEP-2L supports up-to-date requirements to service quality and allows transmitting more important traffic in higher priorities queues. Prioritization is based on main QoS technologies: CoS (special tags in VLAN packet field) and ToS (tags in IP packet field).

ACL rule creation functionality and support for traffic shaping on each VAP allows you to fully manage access, service quality and restrictions, both for all subscribers and for everyone in particular.

The devices are designed to be installed in offices, state buildings, conference halls, laboratories, hotels, etc. The creation of virtual access points with different types of encryption allows clients to delimit access rights among users and groups of users.

2.2 Device specification

Interfaces:

- 1 port of Ethernet 10/100/1000 Base-T(RJ-45) with PoE+ support;

Functions:

WLAN capabilities:

- Support for IEEE 802.11a/b/g/n/ac standards;
- Data aggregation, including A-MPDU (Tx/Rx) and A-MSDU (Rx);
- WMM-based priorities and packet planning;
- Dynamic frequency selection (DFS);
- Support for hidden SSID;
- 8 virtual access points
- Third-party access point detection;
- Spectrum analyzer;
- Channel autoselection.

Network functions:

- Autonegotiation of speed, duplex mode and switching between MDI and MDI-X modes;
- Support for VLAN;
- Authentication support 802.1X;
- DHCP client;
- ACL;
- NTP;
- Support for Syslog;
- GRE;
- GRE over IPsec;
- Transmission of subscriber traffic out of tunnel.

QoS functions

- Priority and profile-based packet scheduling;
- Bandwidth limitation for each VAP;

- Bandwidth limitation for each client;
- WMM parameters changing.

Security

- Centralized authorization via RADIUS server (WPA Enterprise);
- WPA/WPA2;
- Captive Portal;

The figure below shows WEP-2L application scheme.

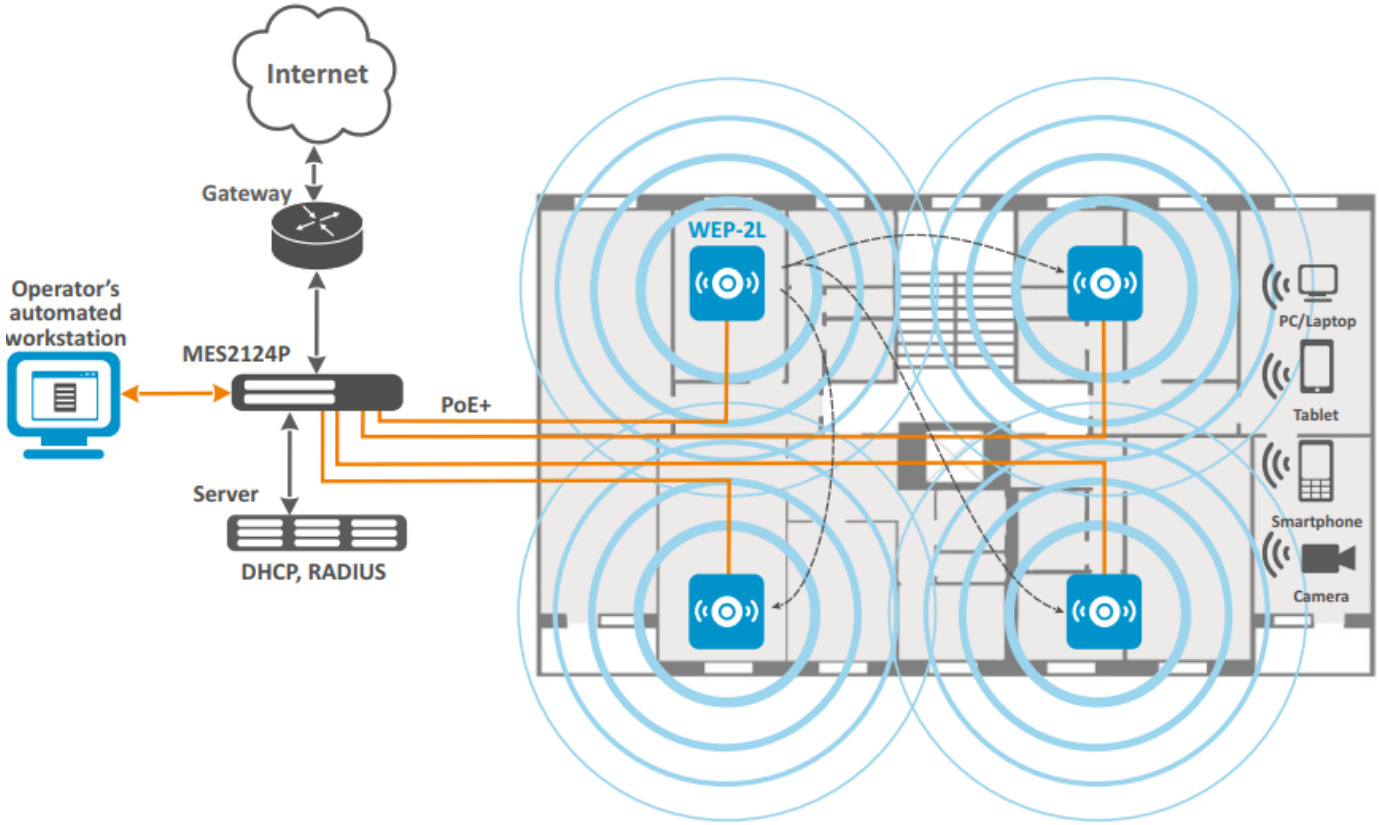


Figure 1 – WEP-2L application scheme

2.3 The device technical parameters

Table 1 – Main Specifications

WAN Ethernet interface parameters	
Number of ports	1
Electrical connector	RJ-45
Data rate, Mbps	10/100/1000, auto-negotiation
Standards	BASE-T
Wireless interface parameters	
Standards	802.11a/b/g/n/ac
Frequency range, MHz	2402–2482 MHz, 5170–5835 MHz
Modulation	DSSS, CCK, BPSK, QPSK, 16QAM, 64QAM, 256QAM

Operating channels	802.11b/g/n: 1–13 (2402–2482 MHz) 802.11a/n/ac: • 36–64 (5170–5320 MHz) • 100–144 (5490–5720 MHz) • 149-165 (5745–5835 MHz)
Data rate, Mbps	802.11a: up to 54 Mbps 802.11b: up to 11 Mbps 802.11g: up to 54 Mbps 802.11n: up to 300 Mbps 802.11ac: up to 867 Mbps
Maximum output power of the transmitter	2.4 GHz: up to 20 dBm 5 GHz: up to 20 dBm
Receiver sensitivity	2.4 GHz: up to -94 dBm 5 GHz: up to -94 dBm
Security	Centralized authorization via RADIUS server (WPA Enterprise) WPA/WPA2 data encryption Captive Portal
Support for 2x2 MIMO	
Two Realtek Wi-Fi chips: RTL8197FS (2.4 GHz) and RTL8812FR (5 GHz).	
Control	
Remote control	Web interface, Telnet, SSH, SNMP (monitoring), NETCONF, EMS management system.
Access restriction	by password
General parameters	
Processor	Realtek RTL8197FS 1 GHz
NAND	32 MB NAND Flash
RAM	128 MB RAM DDR3
Power supply	PoE+ 48V/54V (IEEE 802.3at-2009).
Maximum power consumption	9 W
Range of operation temperatures	from +5 to +40°C
Relative humidity at 25°C	up to 80%
Dimensions (Diameter x Height)	200x40 mm
Weight	0.4 kg

2.4 Design

WEP-2L enclosed in plastic case.

2.4.1 Device main panel

The main panel layout of the device is depicted in Figure 2.

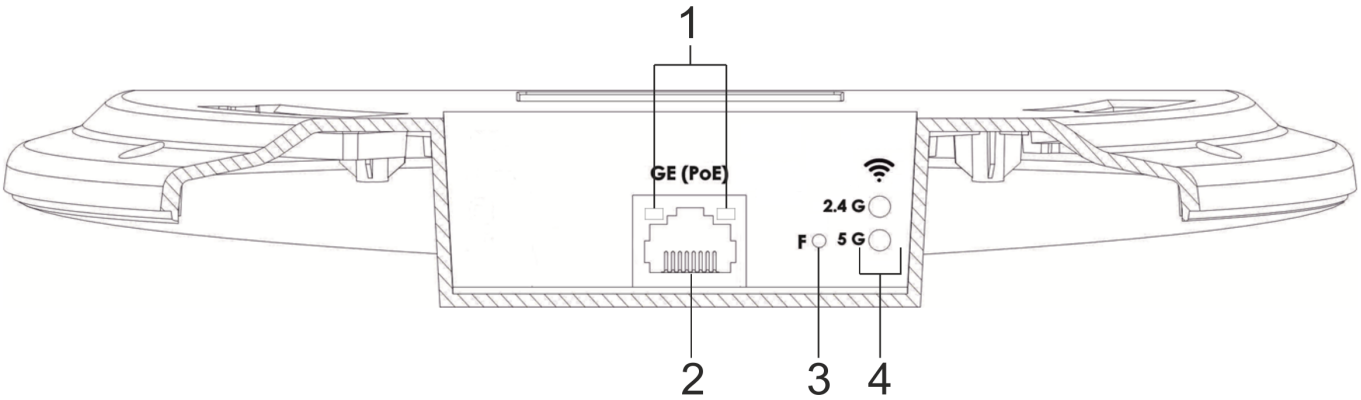


Figure 2 – WEP-2L main panel layout

Connectors and controls located on the device main panel are listed in Table 2.

Table 2 – Description of ports and controls

Main panel element		Description
1	LAN	GE (PoE) port status light indication
2	GE (PoE)	GE port for PoE+ power supply connection
3	F	Button for reseting to factory settings
4	Wi-Fi	Operation indicators of corresponding Wi-Fi modules

2.5 Light indication

The current device state is displayed by **Wi-Fi**, **LAN, Power** indicators. The list of indicators' possible states is given below.

Table 3 – Light indication of device state

LED	LED status	Device state
Wi-Fi	solid green	the Wi-Fi network is active
	flashing green	the process of data transmission trough a wireless network
LAN	solid green (10, 100 Mbps)/ solid orange (1000 Mbps)	the link with the connected network device is established
	flashing green	the process of packet data transmission through LAN interface
Power (on the device top panel)	solid green	the device power on, normal operation
	solid orange	the device is loaded but IP address is not received via DHCP
	solid red	the device is loading

2.6 Reset to the default settings

In order to reset the device to factory settings, press and hold the «F» button until «Power» indicator starts flashing. Device will be rebooted automatically. DHCP client will be launched by default. If the address is not obtained via DHCP, the device will have the default IP address — *192.168.1.10*, and the following netmask — *255.255.255.0*.

2.7 Delivery package

The delivery package includes:

- WEP-2L wireless access point;
- Mounting kit;
- Operating manual (supplied on a CD);
- Conformity certificate;
- Technical passport.

3 Rules and recommendations for device installation

This section defines safety rules, installation recommendations, setup procedure and the device starting procedure.

3.1 Safety rules

1. Do not install the device close to heat sources or in rooms with temperature below 5 °C or above 40 °C.
2. Do not use the device in places with high humidity. Do not expose the device to smoke, dust, water, mechanical vibrations or shocks.
3. Do not open the device case. There are no user serviceable parts inside.

> Do not cover ventilation holes and do not put other objects on the device in order to prevent overheating of device components.

3.2 Installation recommendations

1. The recommended installation: Horizontal, on a ceiling.
2. Before you install and enable device, check the device for visible mechanical defects. If defects are observed, you should stop the device installation, draw up corresponding act and contact the supplier.
3. If the device has been exposed for a long time at a low temperature, it must be left to stand for two hours at room temperature before use. After a long stay of the device in conditions of high humidity, let it stand under normal conditions for at least 12 hours before switching on.
4. During the device installation to provide Wi-Fi coverage area with the best characteristics take into account the following rules:
   a. Install the device at the center of a wireless network;
   b. Minimize the number of obstacles (walls, roof, furniture and etc.) between access point and other wireless network devices;
   c. Do not install the device near (about 2 m) electrical and radio devices;
   d. It is not recommended to use radiophone and other equipment operating on the frequency of 2.4 GHz, 5 GHz in Wi-Fi effective radius;
   e. Obstacles in the form of glass/metal constructions, brick/concrete walls, water cans and mirrors can significantly reduce Wi-Fi action radius. It is not recommended to place the device inside a false ceiling as metal frame causes multipath signal propagation and signal attenuation.
5. During the installation of several access points, cell action radius must overlap with action radius of a neighboring cell at level of -65 ÷ -70 dBm. Decreasing of the signal level on cells borders to -75 dBm is permitted if it involves the use of VoIP, streaming video and other traffic that is sensitive to losses in wireless network.

3.3 Calculating the number of required access points

To calculate the required number of access points, you should evaluate the required coverage zone. For a more accurate assessment, it is necessary to make a radio examination of the room. Approximate radius of coverage area of WEP-2L with a good-quality signal in case of mounting on a ceiling in typical office: 2.4 GHz 40-50 m, 5 GHz: 20-30 m. In the absence of obstacles, the coverage radius: 2.4 GHz up to 100 m; 5 GHz up to 60 m.
The table below describes rough attenuation values.

Table 4 – Attenuation values

Material	Change of signal level, dB	
	2.4 GHz	5 GHz
Organic glass	-0,3	-0,9
Brick	-4,5	-14,6
Glass	-0,5	-1,7
Plaster slab	-0,5	-0,8
Wood laminated plastic	-1,6	-1,9
Plywood	-1,9	-1,8
Plaster with wirecloth	-14,8	-13,2
Breezeblock	-7	-11
Metal lattice (mesh 13*6 mm, metal 2 mm)	-21	-13

3.4 Channel selection for neighboring access points

It is recommended to set nonoverlapping channels to avoid interchannel interference among neighboring access points.

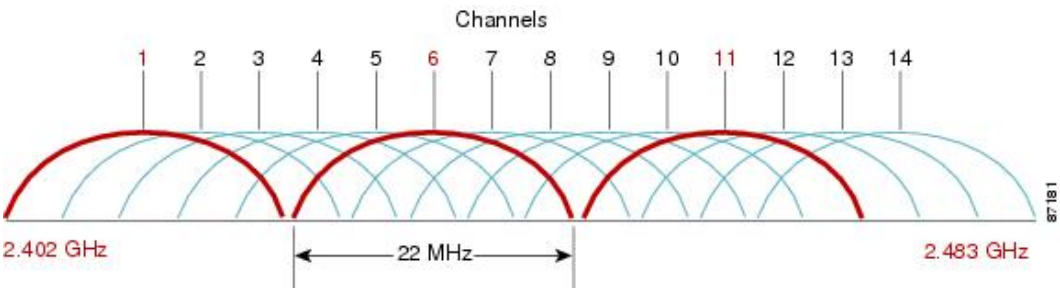


Figure 3 – General diagram of frequency channel closure in the range of 2.4 GHz

For the example of channel allocation scheme among neighboring access points in frequency range of 2.4 GHz when channel width is 20 MHz, see Figure 4.

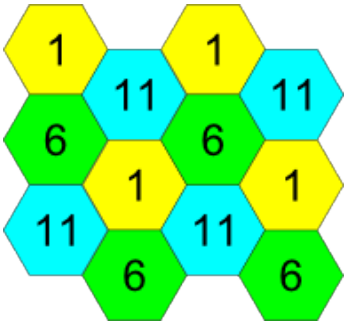


Figure 4 – Scheme of channel allocation among neighboring access points in the frequency range of 2.4 GHz when channel width is 20 MHz

Similarly, the procedure of channel allocation is recommended to save for access point allocation between floors, see Figure 5.

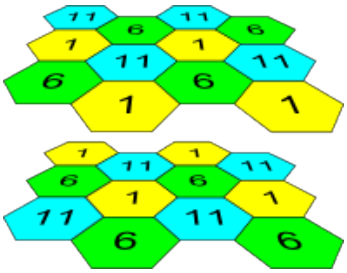


Figure 5 – Scheme of channel allocation between neighboring access points that are located between floors

When width of used channel is 40 MHz there is no non-overlapping channels in frequency range of 2.4 GHz. In such cases, you should select channels maximally separated from each other.

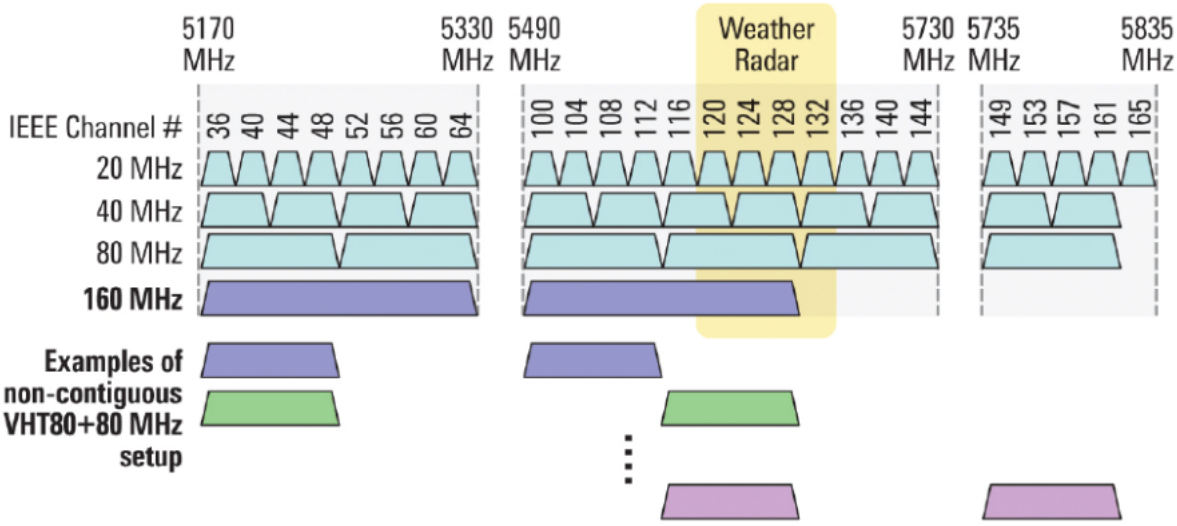


Figure 6 – Channels used in range of 5 GHz when channel width is 20, 40 or 80 MHz

4 Installing WEP-2L

The device should be attached to plain surface (wall or ceiling) in accordance with the safety instruction and recommendations listed above.
The device delivery package includes required mounting kit to attach the device to plain surface.

4.1 Wall mounting

1. Fix the bracket (included in the delivery package) to the wall:

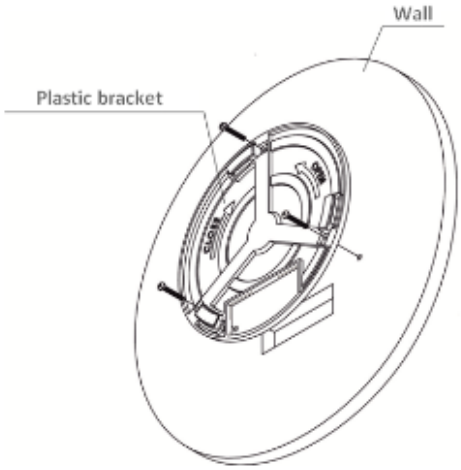


Figure 7 – Attaching the bracket to a wall

a. The figure shows the bracket allocation.
b. When installing the bracket, pass wires through the corresponding channels of the bracket, see figure 7.
c. Pass the wires into the corresponding grooves on the bracket while installing the bracket. Screw the brackets to the device surface by using screwdrive.

2. Install the device

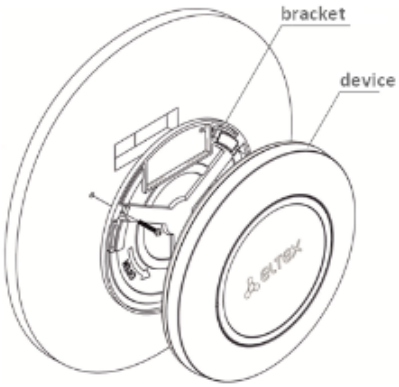
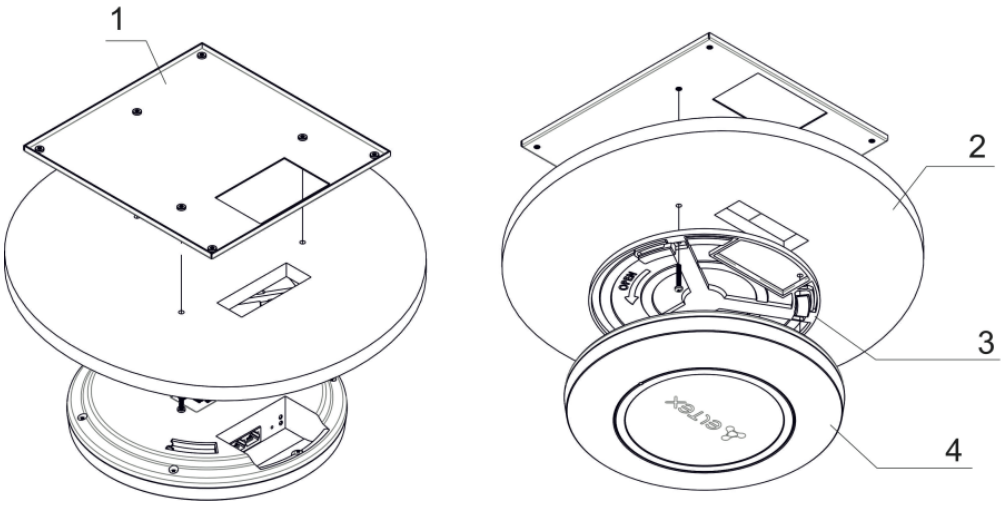


Figure 8 – Device installation (front view)

a. Connect cables to corresponding connector of the device. Description of the connectors is given in section 2.4 Design.
b. Align the device and bracket together, fix the position, turning clockwise.

4.2 Installing to false ceiling

It is not recommended to place the device inside a false ceiling as metal frame causes multipath signal propagation and signal attenuation.



1 – metal bracket; 2 – armstrong panel; 3 – plastic bracket; 4 – device.

Figure 9 – Mounting to a false ceiling

1. Fasten metal and plastic bracket on a ceiling as shown in the figure 9.
    a. The plastic bracket (**3**) should be joined with the metal one (**1**) on the ceiling in the following order: metal bracket -> armstrong panel -> plastic bracket.
    b. Cut the hole in the armstrong panel. The size of the hole should be equal to hole of metal bracket. Conduct wires through the hole.
    c. Align holes in metal bracket with holes of armstrong panel and plastic bracket. Align together three boltholes on the plastic bracket and the boltholes on the metal bracket. Screw the brackets to the device surface by using a screwdrive.
2. Install the device.
    a. Connect cables to corresponding connector of the device. Description of the connectors is given in section 2.4 Design.
    b. Align the device and plastic bracket together, fix the position, turning clockwise.

4.3 Removing the device from the bracket

For removing the device from the bracket:

1. Turn the device counter-clockwise, figure 7.
2. Remove the device.

5 Device management via the WEB interface

5.1 Getting started

In order to start the operation, you should connect to the device via WAN interface using a web browser:

1. Open a web browser, for example, Firefox, Opera, Chrome.
2. Enter the device IP address in the browser address bar.

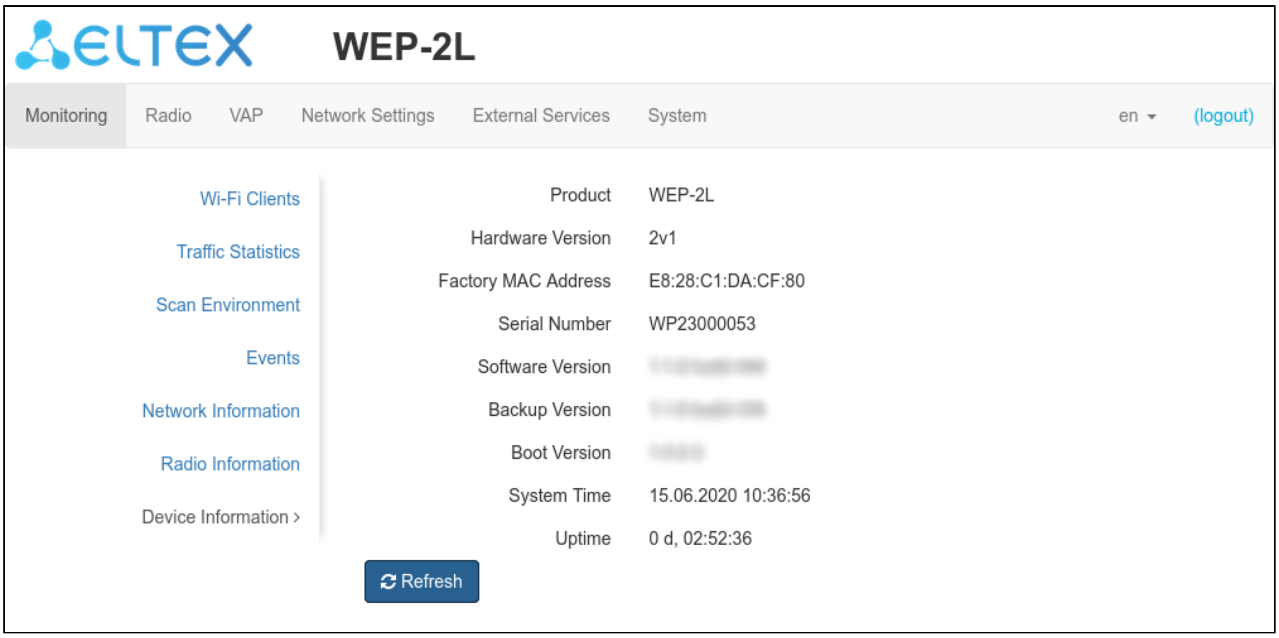
IP address by default: 192.168.1.10, subnet mask: 255.255.255.0. The device is capable to obtain an IP address via DHCP.

When the device is successfully detected, username and password request page will be shown in the browser window

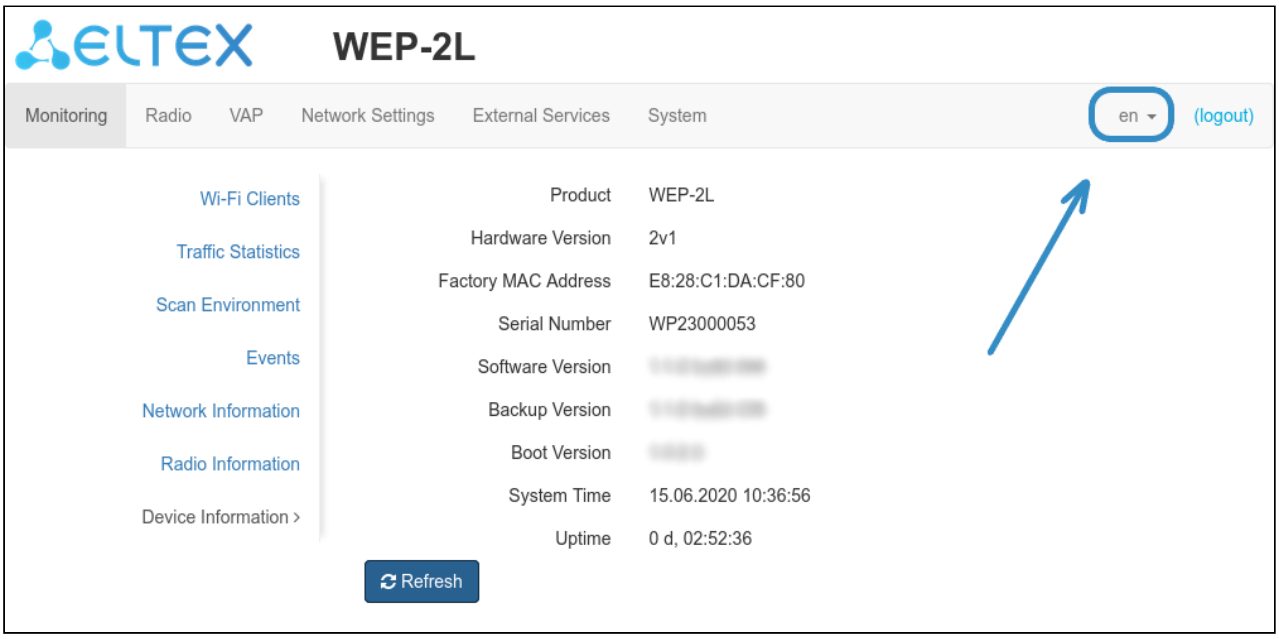
3. Enter your username into «Login» and password into «Password» field.

Factory settings: login: *admin*, password: *password*.

4. Click the «Log in» button. A menu for monitoring the status of the device will open in a browser window.



5. If necessary, you can switch the information display language. Russian and English languages are available for WEB interface.



5.2 Applying configuration and discarding changes

1. Applying configuration

Clicking on the Apply button starts the process of saving the configuration to the device flash memory and applying the new settings. All the settings come into operation without device rebooting.

Visual indication of the process current status of the setting application process is realised in the WEB interface, table 7.

Table 7 – Visual indication of the current status of the setting application process

Image	State description
Apply	After pressing «Apply», the process of settings saving to device memory is launched. This is indicated by the icon in the tab name and on the Apply button.
Apply	Successful settings saving and application are indicated by icon in the tab name.

2. Discarding changes

You can discard changes only before pressing «Apply» button. If you press «Apply» button, all the changed parameters will be applyed and saved to device memory. You will not be able to return to previous configuration after pressing «Apply».

The button for discarding changes appears as follows: Cancel .

5.3 WEB interface basic elements

Navigation elements of the WEB interface are shown on the figure below

User interface window is divided into five general areas:

1. Menu tabs categorize the submenu tabs: **Monitoring, Radio, VAP, Network settings, External Services, System.**
2. Interface language selection and Logout button designed to to end a session in the WEB interface under a given user.
3. Submenu tabs allow you to control settings field.
4. Devcie configuration field displays data and configuration.
5. Information field displays current firmware version.

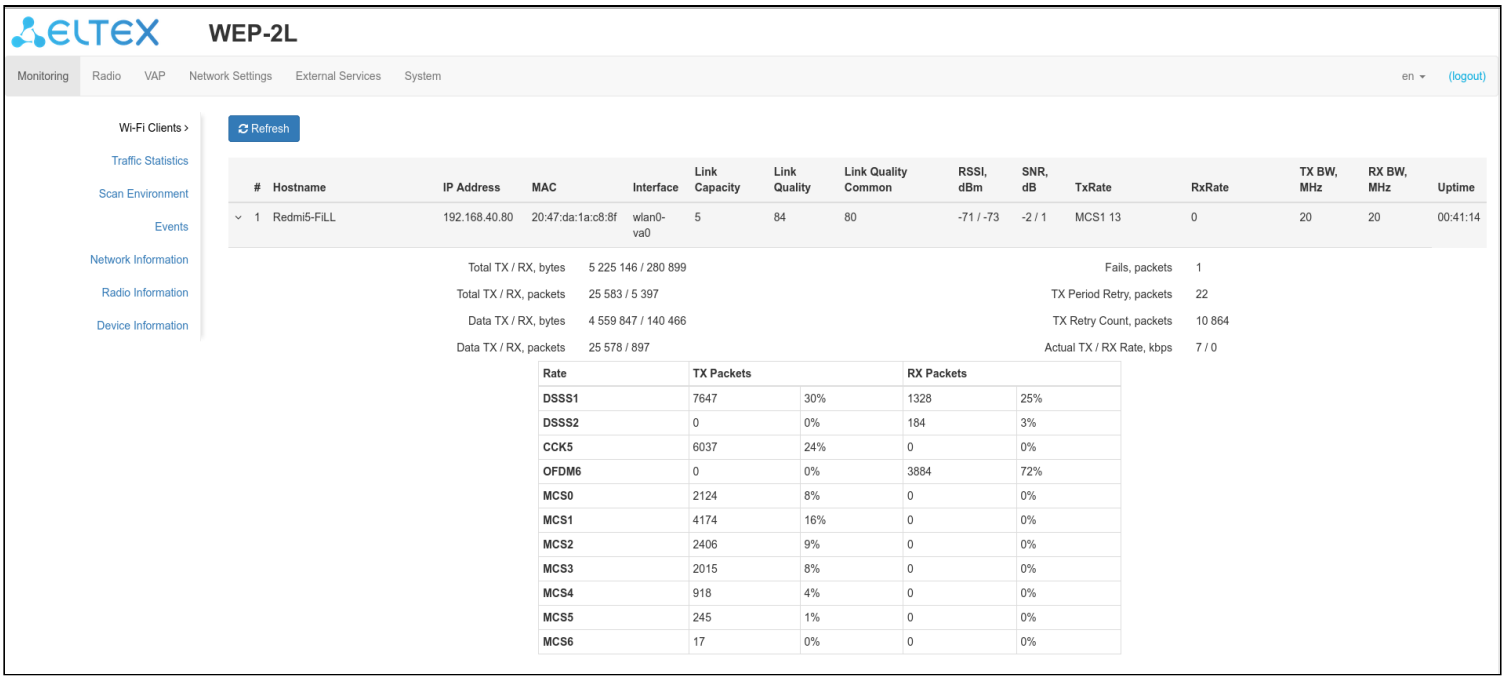
5.4 The «Monitoring» menu

In the «**Monitoring**» menu you can view the current system state.

5.4.1 The «Wi-Fi clients» submenu

The «**Wi-Fi clients**» submenu displays information about the status of connected Wi-Fi clients.

Information on connected clients is not displayed in real time. In order to update the information on the page you should click the «Update» button.



- *№* – number of the connected device in the list;
- *Hostname* – network name of the device;
- *IP address* – IP address of the connected device;
- *MAC address* – MAC address of the connected device;
- *Interface* – interface of WEP-2L communication with the connected device;
- *Link Capacity* – parameter that reflects the effectiveness of the use of a modulation access point on the transmission. It is calculated based on the number of packets transmitted on each modulation to the client, and the reduction factors. The maximum value is 100% (means that all packets are transmitted to the client at maximum modulation for the maximum nss type supported by the client). The minimum value is 2% (in the case when the packets are transmitted to the modulation nss1mcs0 for a client with MIMO 3x3 support). The parameter value is calculated for the last 10 s.
- *Link Quality* – parameter that displays the status of the link to the client, calculated based on the number of retransmit packets sent to the client. The maximum value is 100% (all transmitted packets were sent on the first attempt), the minimum value is 0% (no packets were successfully sent to the client). The parameter value is calculated for the last 10 s.
- *Link Quality Common* – parameter that displays the status of the link to the client, calculated based on the number of retransmit packets sent to the client. The maximum value is 100% (all transmitted packets were sent on the first attempt), the minimum value is 0% (no packets were successfully sent to the client). The parameter value is calculated for the entire client connection time.
- *RSSI* – received signal level, dBm;
- *SNR* – signal/noise ratio, dB;
- *TxRate* – channel data rate of transmission, Mbps;
- *RxRate* – channel data rate of receiving, Mbps;

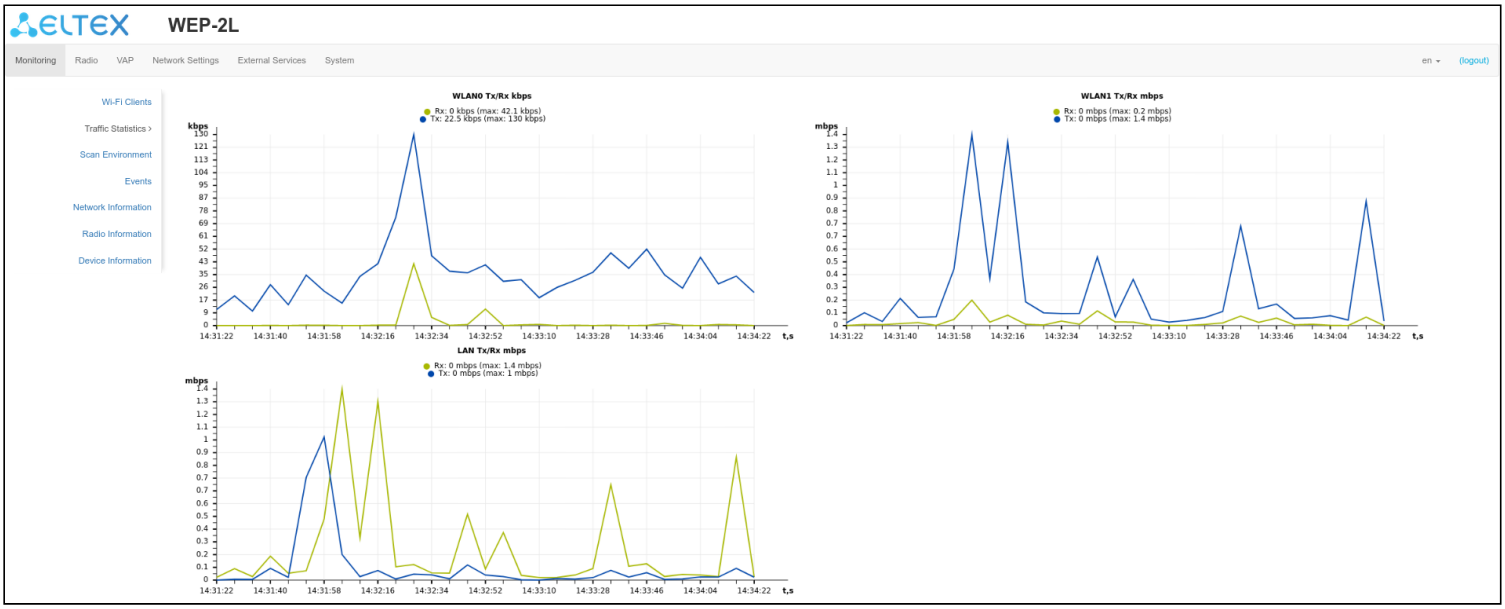
- *Tx BW* – transmission bandwidth, MHz;
- *Rx BW* – reception bandwidth, MHz;
- *Uptime* – Wi-Fi client connection uptime.

To display more detailed information on a particular client, select it from the list. A detailed description includes the following options:

- *Total TX/RX, bytes* – the number of bytes sent/received on the connected device;
- *Total TX/RX, packets* – the number of packets sent/received on the connected device;
- *Data TX/RX, bytes* – the number of data bytes sent/received on the connected device;
- *Data TX/RX, packets* – the number of data packets sent/received on the connected device;
- *Fails, packets* – the number of packets sent with errors on the connected device;
- *TX Period Retry, packets* – the number of retries of transmission to the connected device in the last 10 s;
- *TX Retry Count, packets* – the number of retries of transmission to the connected device during the entire connection;
- *Actual TX/RX Rate, Kbps* – the current traffic transmission rate at the moment.

5.4.2 The «Traffic Statistics» submenu

The «**Traffic Statistics**» section displays the diagrams of the speed of the transmitted/received traffic for last 3 minutes, as well as statistics on the amount of transmitted/received traffic since the access point was turned on.



The LAN Tx/Rx diagram shows the speed of the transmitted/received traffic via the access point's Ethernet interface in the last 3 minutes. The diagram is automatically updated every 6 seconds.

The WLAN0 and WLAN1 Tx/Rx diagrams show the last 3 minutes rate of transmitted/received traffic via Radio 1 and Radio 2 access point interfaces. The diagram is automatically updated every 6 seconds.

Transmit

Interface	Total Packets	Total Bytes	Total Drop	Errors
LAN	536463	76131869	0	0
WLAN0	165963	75366878	341385	140
WLAN1	1525882	1919784608	359381	390
br-mgmt	9493	7749418	0	0
lsw	0	0	0	0
mgmt-gre	9436	7426234	0	57
mgmt-gre.1	9493	7787390	0	0
user-gre	526637	38459019	0	136
wlan0-va0	161849	74195479	51445	123
wlan0-va1	3542	1013363	147020	15
wlan0-va2	572	158036	142627	2
wlan0-va3	0	0	0	0
wlan1-va0	889	149670	147674	30
wlan1-va1	1234	212512	141561	38
wlan1-va2	1523377	1919342058	69904	322
wlan1-va3	0	0	0	0

«Transmit» table description:

- *Interface* – name of the interface;
- *Total packets* – number of successfully sent packets;
- *Total bytes* – number of successfully sent bytes;
- *Total drop* – number of rejected packets;
- *Errors* – number of errors.

Receive

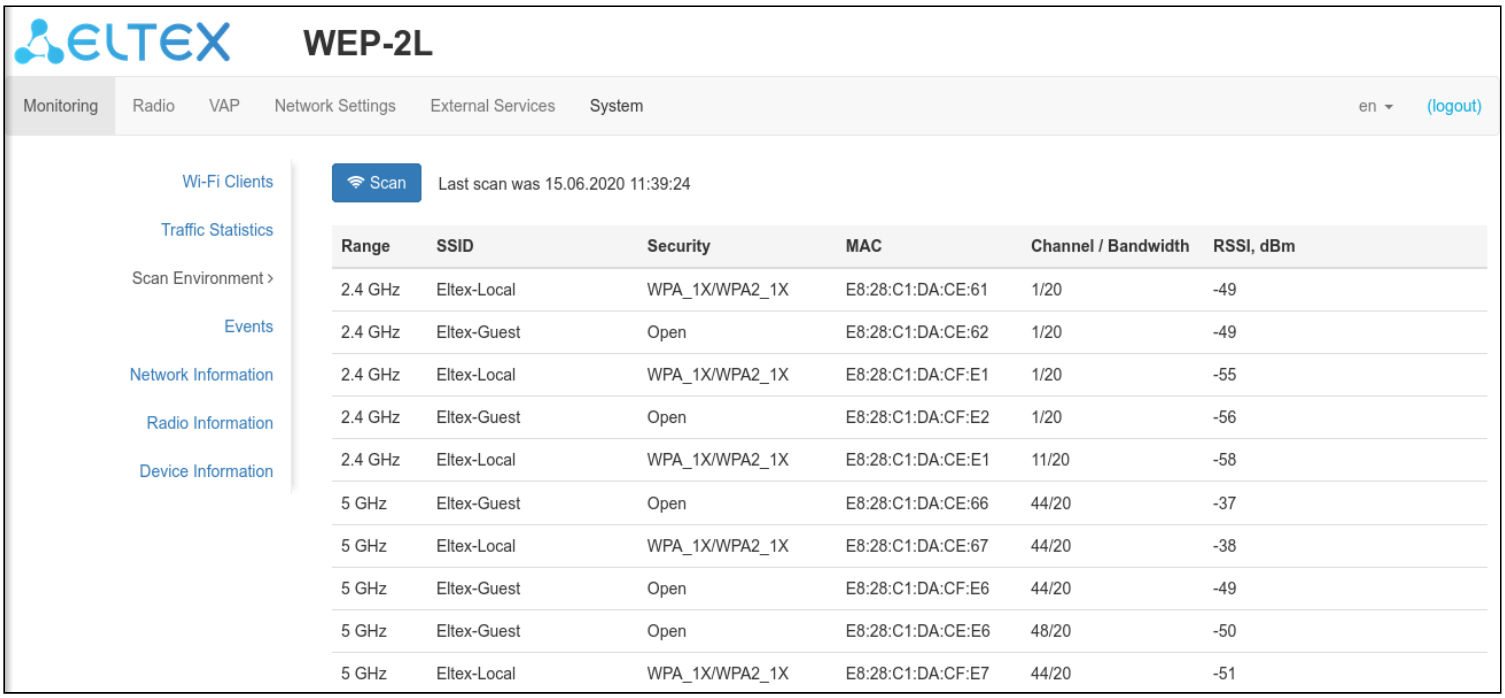
Interface	Total Packets	Total Bytes	Total Drop	Errors
LAN	1511014	2008086705	340	0
WLAN0	28117	4046918	0	0
WLAN1	503014	61464997	1	0
br-mgmt	15672	985394	0	0
lsw	0	0	0	0
mgmt-gre	15743	1053120	0	0
mgmt-gre.1	15743	990148	0	0
user-gre	1494168	1928380794	0	0
wlan0-va0	25758	3470393	0	0
wlan0-va1	1825	477328	0	0
wlan0-va2	534	99197	0	0
wlan0-va3	0	0	0	0
wlan1-va0	92	15957	0	0
wlan1-va1	4	520	0	0
wlan1-va2	502815	61429786	1	0
wlan1-va3	0	0	0	0

«Receive» table description:

- *Interface* — name of the interface;
- *Total packets* – number of successfully received packets;
- *Total bytes* – number of successfully received bytes;
- *Total drop* – number of rejected packets;
- *Errors* – number of errors.

5.4.3 The «Scan Environment» submenu

In the **«Scan Environment»** submenu, scanning of the surrounding radio is carried out and detection of neighboring access points.



Range	SSID	Security	MAC	Channel / Bandwidth	RSSI, dBm
2.4 GHz	Eltex-Local	WPA_1X/WPA2_1X	E8:28:C1:DA:CE:61	1/20	-49
2.4 GHz	Eltex-Guest	Open	E8:28:C1:DA:CE:62	1/20	-49
2.4 GHz	Eltex-Local	WPA_1X/WPA2_1X	E8:28:C1:DA:CF:E1	1/20	-55
2.4 GHz	Eltex-Guest	Open	E8:28:C1:DA:CF:E2	1/20	-56
2.4 GHz	Eltex-Local	WPA_1X/WPA2_1X	E8:28:C1:DA:CE:E1	11/20	-58
5 GHz	Eltex-Guest	Open	E8:28:C1:DA:CE:66	44/20	-37
5 GHz	Eltex-Local	WPA_1X/WPA2_1X	E8:28:C1:DA:CE:67	44/20	-38
5 GHz	Eltex-Guest	Open	E8:28:C1:DA:CF:E6	44/20	-49
5 GHz	Eltex-Guest	Open	E8:28:C1:DA:CE:E6	48/20	-50
5 GHz	Eltex-Local	WPA_1X/WPA2_1X	E8:28:C1:DA:CF:E7	44/20	-51

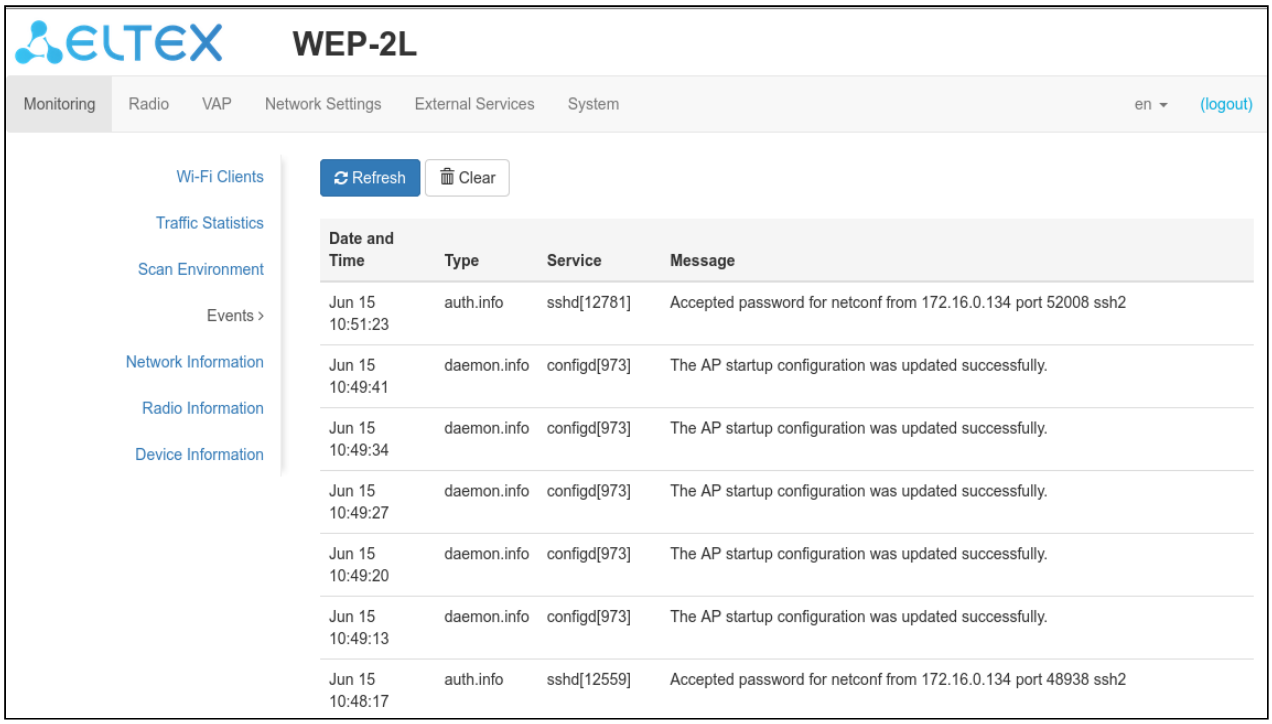
After clicking on the «Scan» button, the process will be launched. After the scan is completed, a list of detected access points and information about them will appear:

- *Range* – specifies the range of 2.4 GHz or 5 GHz to which the access point was detected;
- *SSID* – SSID of the detected access point;
- *Security* – security mode of the detected access point;
- *MAC* – MAC address of the detected access point;
- *Channel/Bandwidth* – radio channel on which the detected access point operates;
- *RSSI* – the level with which the device receives the signal of the detected access point, dBm.

Please note that during the environment scan, the device's radio interface will be disabled, which will make it impossible to transfer data to Wi-Fi clients during the scan.

5.4.4 The «Events» submenu

In this section, you can view a list of real-time informational messages which contains the following information:



- *Date and Time* – time when event was generated;
- *Type* – category and importance level of the event;
- *Service* – name of the process that generated the message;
- *Message* – event description.

Table 7 – event importance categories description

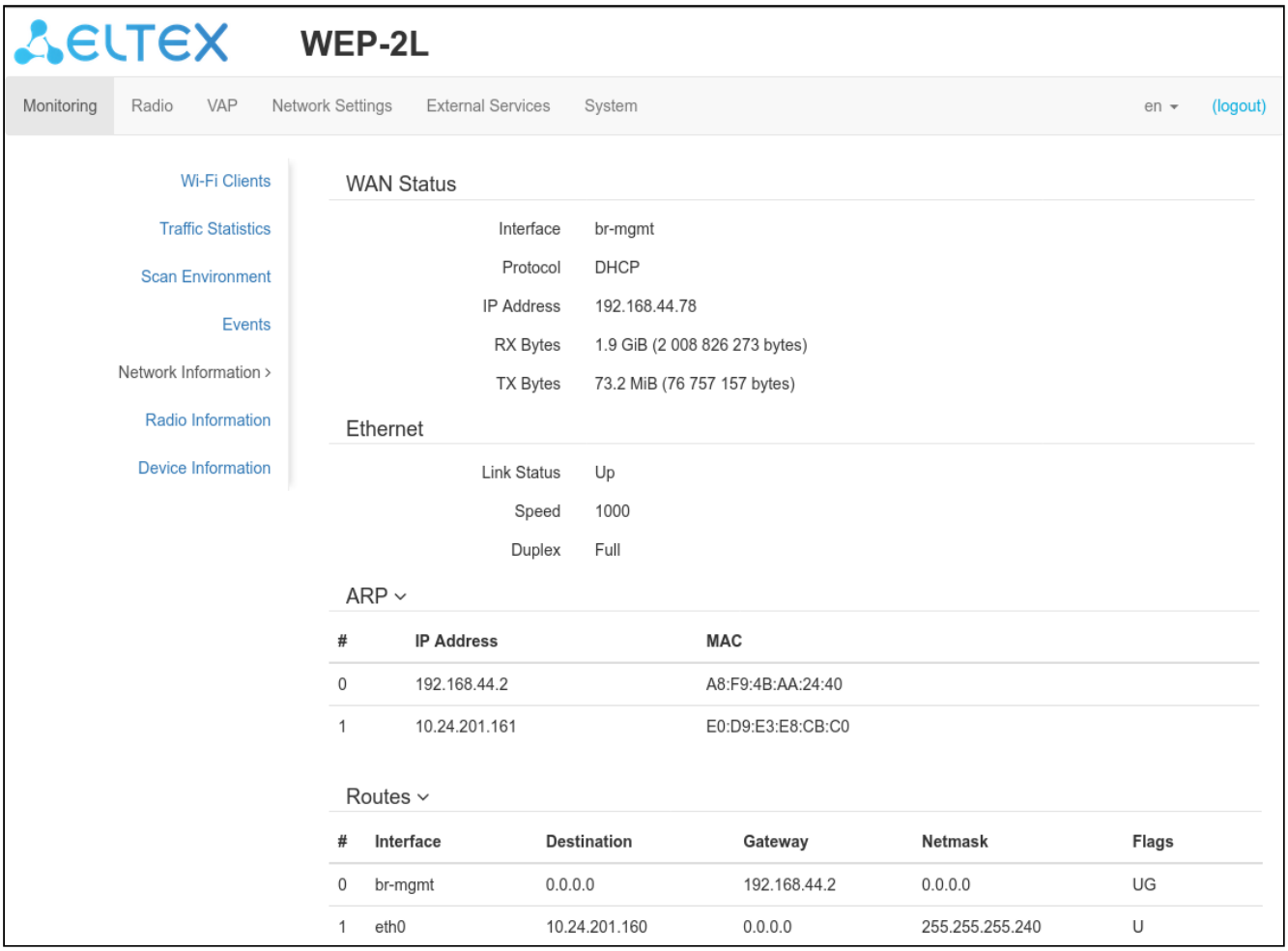
Level	Message importance level	Descritpion
0	Emergency	A critical error has occurred in the system, the system may not work properly.
1	Alert	Immediate intervention is required.
2	Critical	A critical error has occurred on the system.
3	Error	An error has occurred on the system.
4	Warning	Warning, non-emergency message.
5	Notice	System notice, non-emergency message.
6	Informational	Informational system messages.
7	Debug	Debugging messages provide the user with information to correctly configure the system.

To receive new messages in the event log, click the «Update» button.

If necessary, you can delete all old messages from the log by clicking on the «Clear» button.

5.4.5 The «Network Information» submenu

In the «**Network Information**» submenu you can view common network settings of the device.



<u>WAN Status</u>:

- *Interface* – name of the bridge interface;
- *Protocol* – a protocol which is used for access to WAN;
- *IP address* – device IP address in external network;
- *RX Bytes* – number of bytes received on WAN;
- *TX Bytes* – number of bytes sent from WAN.

<u>Ethernet</u>:

- *Link Status* – Ethernet port status;
- *Speed* – Ethernet port connection speed;
- *Duplex* – data transfer mode:
  - *Full* – full duplex;
  - *Half* – half-duplex.

<u>ARP</u>

The ARP table contains information about the alignment between the IP and MAC addresses of neighboring network devices:

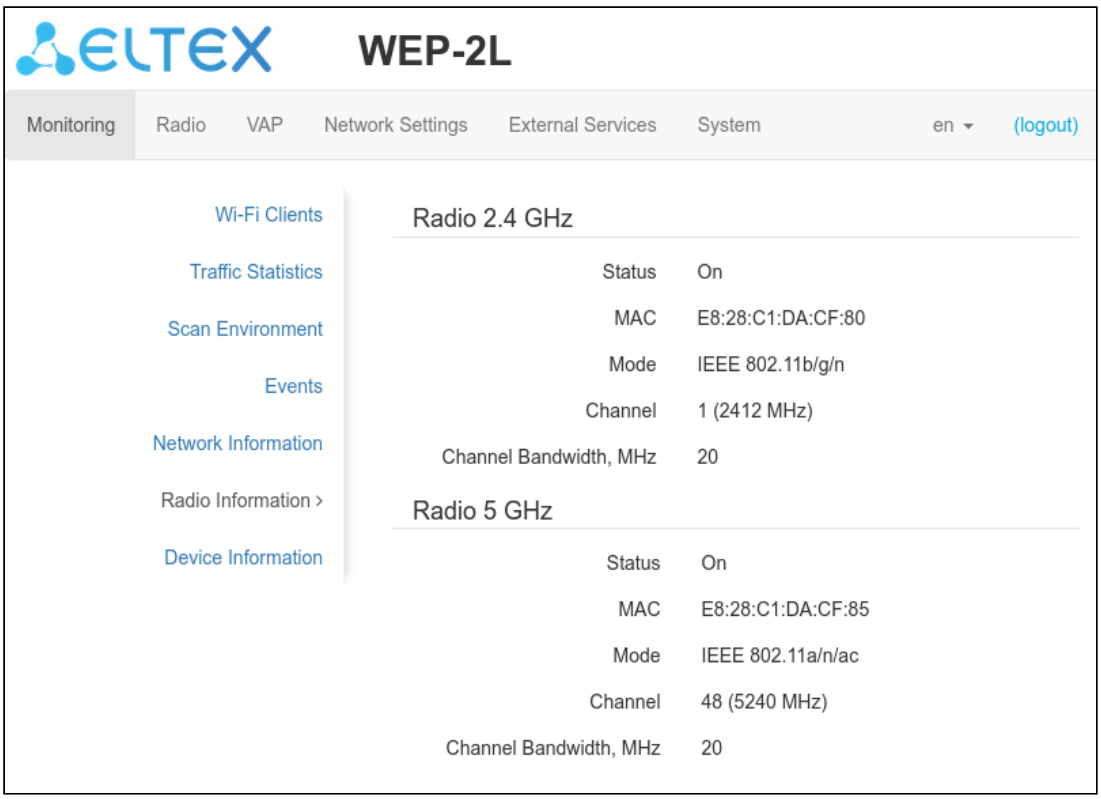
- *IP address* – device IP address;
- *MAC* – device MAC address.

Routes:

- *Interface* – name of the bridge interface;
- *Destination* – IP address of destination host or subnet that the route is established to;
- *Gateway* – gateway IP address that allows for the access to the Destination;
- *Netmask* – subnet mask;
- *Flags* – certain route characteristics. The following flag values exist:
    - **U** – means that the route is created and passable;
    - **H** – identifies the route to the specific host;
    - **G** – means that the route lies through the external gateway. System network interface provides routes in the network with direct connection. All other routes lie through the external gateways. G flag is used for all routes except for the routes in the direct connection networks;
    - **R** - indicates that the route was most likely created by a dynamic routing protocol running on the local system using the reinstate parameter;
    - **D** – indicates that the route was added as a result of receiving an ICMP Redirect Message. When the system learns the route from the ICMP Redirect message, the route will be added into the routing table in order to exclude redirection of the following packets intended for the same destination;
    - **M** – means that the route was modified – likely by a dynamic routing protocol running on a local system with the «mod» parameter applied;
    - **A** - points to a buffered route to which an entry in the ARP table corresponds;
    - **C** – means that the route source is the core routing buffer;
    - **L** – indicates that the destination of the route is one of the addresses of this computer. Such «local routes» exist in the routing buffer only;
    - **B** – means that the route destination is a broadcasting address. Such «broadcast routes» exist in the routing buffer only;
    - **I** – indicates that the route is connected to a ring (loopback) interface for a purpose other than to access the ring network. Such «internal routes» exist in the routing buffer only;
    - **!** – means that datagrams sent to this address will be rejected by the system.

5.4.6 The «Radio Information» submenu

In the **«Radio Information»** submenu the current status of WEP-2L radio interfaces is displayed.



The access point radio interfaces can be in two states: «On» and «Off». The status of each radio interface is shown in the «Status» field.

The Radio status depends on whether the radio interface has virtual access points (VAPs) enabled. In case there is at least one active VAP on the radio interface, Radio will be in «On» status, otherwise - «Off».

Depending on the Radio status, the following information is available for monitoring:

<u>«Off»:</u>

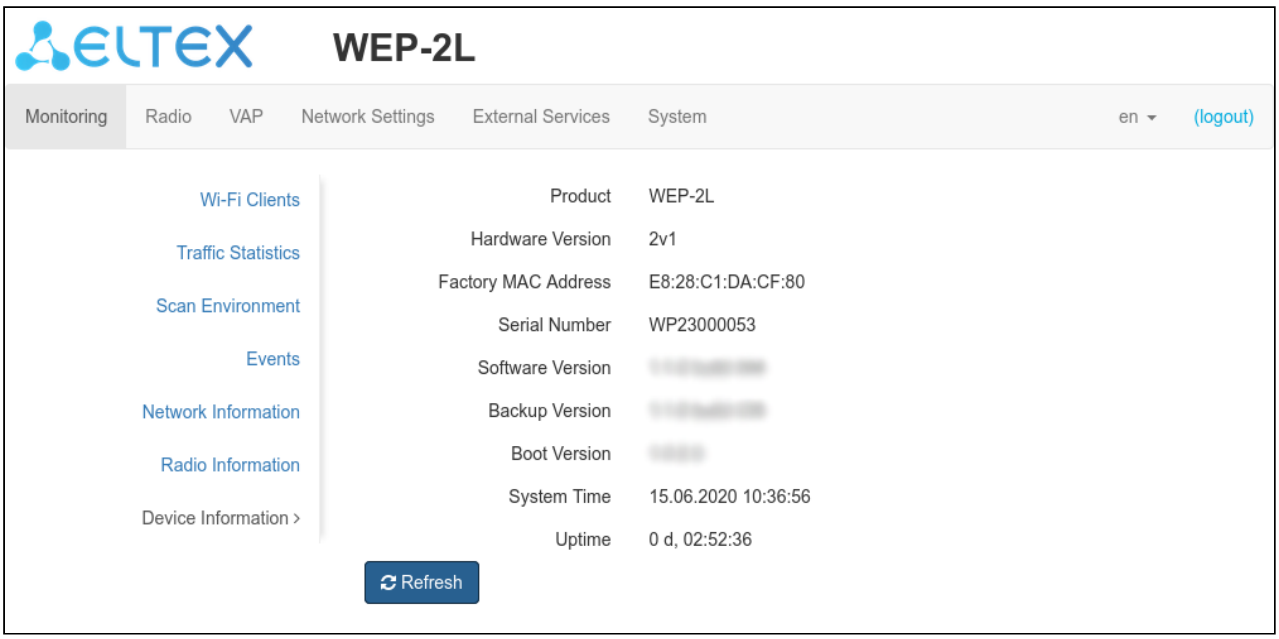
- *Status* – radio interface state;
- *MAC* – radio interface MAC address;
- *Mode* – radio interface operation mode according to IEEE 802.11 standards.

<u>«On»</u>:

- *Status* – radio interface state;
- *MAC* – radio interface MAC address;
- *Mode* – radio interface operation mode according to IEEE 802.11 standards;
- *Channel* – number of the wireless channel on which the radio interface is running;
- *Channel bandwidth* – bandwidth of the channel on which the radio interface is running.

5.4.7 The «Device Information» submenu

The **«Device Information»** submenu displays main WEP-2L parameters.



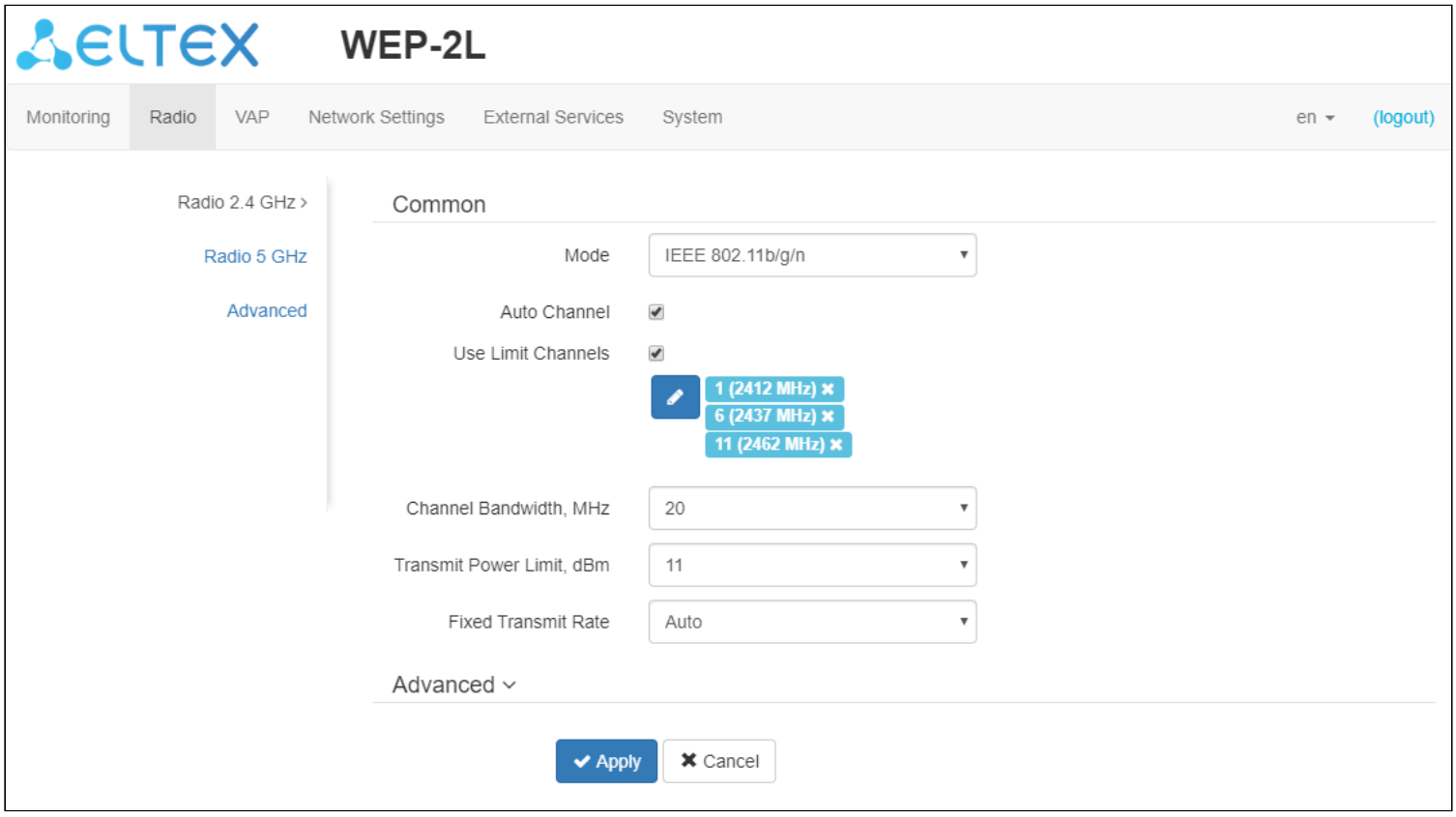
- *Product* – device model name;
- *Hardware Version* – device hardware version;
- *Factory MAC Address* – device WAN interface MAC address, setted by manufacturer;
- *Serial Number* – device serial number, setted by manufacturer;
- *Firmware Version* – device firmware version;
- *Backup Version* – previously installed firmware version;
- *Boot Version* – device firmware boot version;
- *System Time* – current time and date, setted in system;
- *Uptime* – the time since the last turn on or restart the device.

5.5 The «Radio» menu

In the «**Radio**» menu you can configure the wireless interface.

5.5.1 The «Radio 2.4 GHz» submenu

In the «**Radio 2.4 GHz**» submenu you can configure the main parameters of the radio interface of the device operating in the 2.4 GHz band.



- *Mode* – select interface operation mode:
  - IEEE 802.11b/g
  - IEEE 802.11b/g/n
  - IEEE 802.11n
- *Auto Channel* – when checked, the device will automatically select the least loaded radio channel for the Wi-Fi interface. Removing the flag opens the access to install the static operation channel.
- *Channel* – select channel for data transmission;
- *Use Limit Channels* – when checked, the access point will use a user-defined list of channels to work in automatic channel selection mode. If the «Use Limit Channels» flag is not checked or there are no channels in the list, the access point will select the operation channel from all available channels in the given band. 2.4 GHz range channels: 1-13;
- *Channel Bandwidth, MHz* – channel bandwidth, on which the access point operates. The parameter may take values of 20 and 40 MHz;
- *Primary Channel* – the parameter can only be changed if the bandwidth of a statically specified channel is equal to 40 MHz. The 40 MHz channel can be considered as consisting of two 20 MHz channels, which border in the frequency range. These two 20 MHz channels are called primary and secondary channels. The primary channel is used by clients who only support 20 MHz channel bandwidth:
  - *Upper* – the primary channel will be the upper 20 MHz channel in the 40 MHz band;
  - *Lower* – the primary channel will be the lower 20 MHz channel in the 40 MHz band;

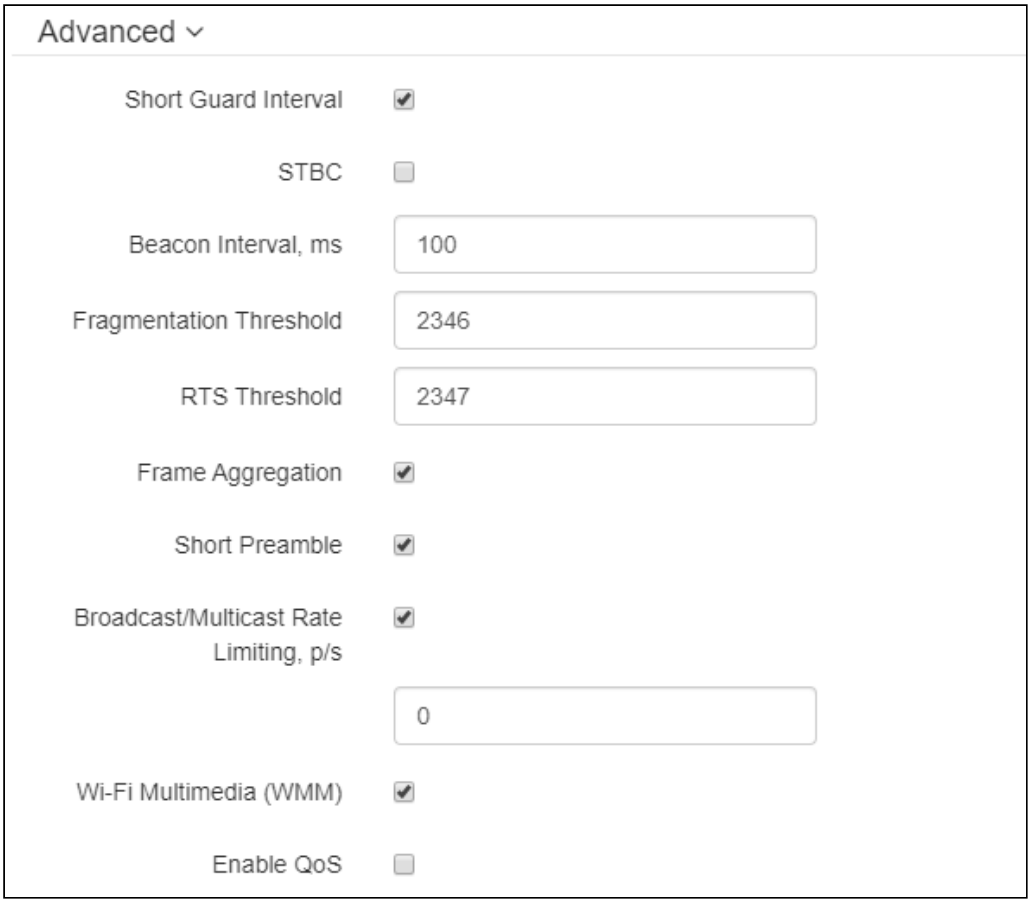
- *Transmission Power Limit, dBm* – transmitting Wi-Fi signal power adjustment, dBm. May take values between 11 and 16 dBm;
- *Fixed Transmit Rate* – fixed wireless data transmission rate which is defined by IEEE 802.11b/g/n standards.

If the «Use Limit Channels» list contains a channel that is not available for selection, it will be marked in grey. In order for the new configuration to be applied to an access point, only available (blue highlighted) channels must be specified in the «Use Limit Channels» list.
Example. No settings have been made on the access point yet, Radio 1 is set to 20 MHz «Channel Bandwidth» by default, and channels are specified in the «Use Limit Channels» list: 1, 6, 11.
Suppose the parameter «Channel Bandwidth» is set to 40 MHz. When you change this parameter from 20 MHz to 40 MHz, the following happens:

- the «Primary channel» parameter becomes available for editing and the default value is «Lower»;
- Channel 11 in the «Use Limit Channels» list changes its color from blue to gray.

If you change the «Channel Bandwidth» parameter to 40 MHz and do not remove the «grey» channels from the list, then when you click on the «Apply» button in the browser an error will appear – «There are errors in data. Changes was not applied». Accordingly, the access point configuration will not be changed. This is due to the fact that channels in the «Use Limit Channels» list that are highlighted in grey do not fit the definition «Primary channel» = Lower.

In the «Advanced» section, you can configure advanced device's radio interface parameters.



- *OBSS Coexistence* – automatic channel bandwidth reduction when the air is loaded. When the flag is set, the mode is enabled;
- *Short Guard interval* – support for Short Guard interval. Access point transmits data using 400 ns Guard interval (instead of 800 ns) to clients which also support Short GI;

- *STBC* – Soace-Time Block Coding method dedicated to improve data transmission reliability. The field is available only if the selected mode of operation of the radio interface includes 802.11n. When checked, the device transmits one data flow through several antennas. When unchecked, the device does not transmit one data flow through several antennas;
- *Beacon Interval, ms* – beacon frames transmission period. The frames are sent to detect access points. The parameter takes values from 20 to 2000 ms, by default – 100 ms;
- *Fragmentation Threshold* – frame fragmentation threshold, bytes. The parameter takes values 256-2346, by default – 2346;
- *RTS Threshold* – after what quantity of bytes the Request to Send will be sent. Decreasing of the parameter's value might improve access point operation when there are a lot of clients connected. However, decreasing of the parameter's value will reduce general bandwidth of wireless network. The parameter takes values from 0 to 2347, by default – 2347;
- *Aggregation* – enable support for AMPDU/AMSDU;
- *Short Preamble* – use of the packet short preamble;
- *Broadcast/Multicast Rate Limiting, p/s* – when the flag is set, transmission of broadcast / multicast traffic over the wireless network is restricted. Specify the limit for broadcast traffic in the popup window (p/s);
- *Wi-Fi Multimedia (WMM)* – WMM support activation (Wi-Fi Multimedia);
- *Enable QoS* – when the flag is set, the setting of Quality of Service functions is available.

The following functions are available for quality assurance configuration:

AP EDCA Parameters

Queue	AIFS	cwMin	cwMax	TXOP Limit
Data 3 (Background)	7	15	1023	0
Data 2 (Best Effort)	3	15	63	0
Data 1 (Video)	1	7	15	94
Data 0 (Voice)	1	3	7	47

Station EDCA Parameters

Queue	AIFS	cwMin	cwMax	TXOP Limit
Data 3 (Background)	7	15	1023	0
Data 2 (Best Effort)	3	15	1023	0
Data 1 (Video)	2	7	15	94
Data 0 (Voice)	2	3	7	47

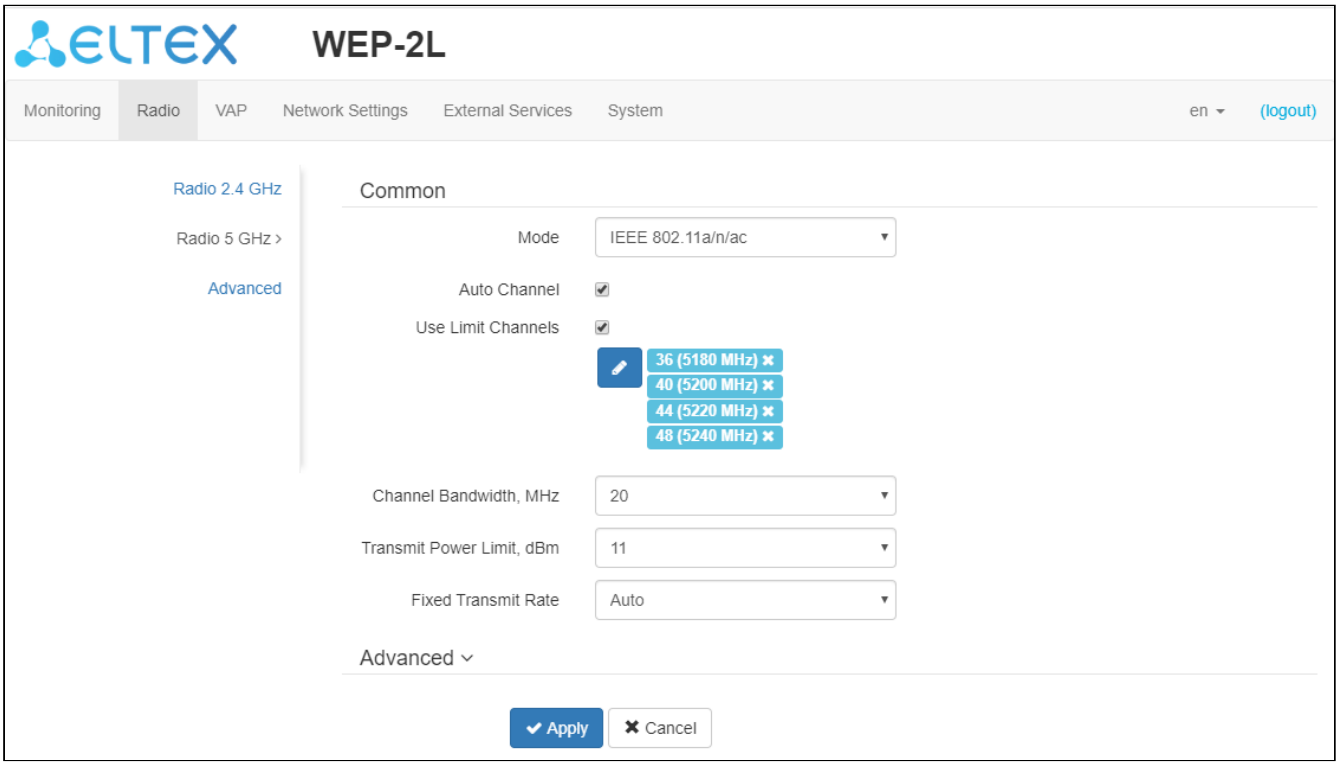
- *AP EDCA parameters* – access point settings table (traffic is transmitted from the access point to the client):
    - *Queue* – predefined queues for various kinds of traffic:
        - *Data 3 (Background)* – low priority queue, high bandwidth (802.1p: cs1, cs2 priorities);

        - *Data 2 (Best Effort)* – middle priority queue, middle bandwidth and delay; Most of the traditional IP data is sent to this queue (802.1p: cs0, cs3 priorities);
        - *Data 1 (Video)* – high priority queue, minimal delay. In this queue, time-sensitive video data is automatically processed (802.1p: cs4, cs5 priorities);
        - *Data 0 (Voice)* – high priority queue, minimal delay. In this queue, time sensitive data is automatically processed, such as: VoIP, streaming video (802.1p: cs6, cs7 priorities).
    - *AIFS* – Arbitration Inter-Frame Spacing, defines the waiting time of data frames, measured in slots, takes values (1-255);
    - *cwMin* – the initial timeout value before resending a frame, specified in milliseconds, takes the values 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023. The value of cwMin cannot exceed the value of cwMax;
    - *cwMax* – the maximum timeout value before resending a frame, specified in milliseconds, takes the values 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023. The value of cwMax must exceed the value of cwMin;
    - *TXOP Limit* – this parameter is used only for data transmitted from the client station to the access point. The transmission capability is the time interval, in milliseconds, when the client WME station has the rights to initiate data transmission over the wireless medium to the access point, the maximum value is 65535 milliseconds;
- *Station EDCA parameters* – table of client station parameter settings (traffic is transmitted from the client station to the access point). For description of table fields, see above.

To apply a new configuration and save setting to non-volatile memory, press «Apply». Press «Cancel» to discard the changes.

5.5.2 The «Radio 5 GHz» submenu

In the **«Radio 5 GHz»** submenu you can configure the main parameters of the radio interface of the device operating in the 5 GHz band.



- *Mode* – select interface operation mode:
    - IEEE 802.11a;
    - IEEE 802.11a/n;
    - IEEE 802.11a/n/ac.
- *Auto Channel* – when checked, the device will automatically select the least loaded radio channel for the Wi-Fi interface. Removing the flag opens the access to install the static operation channel;

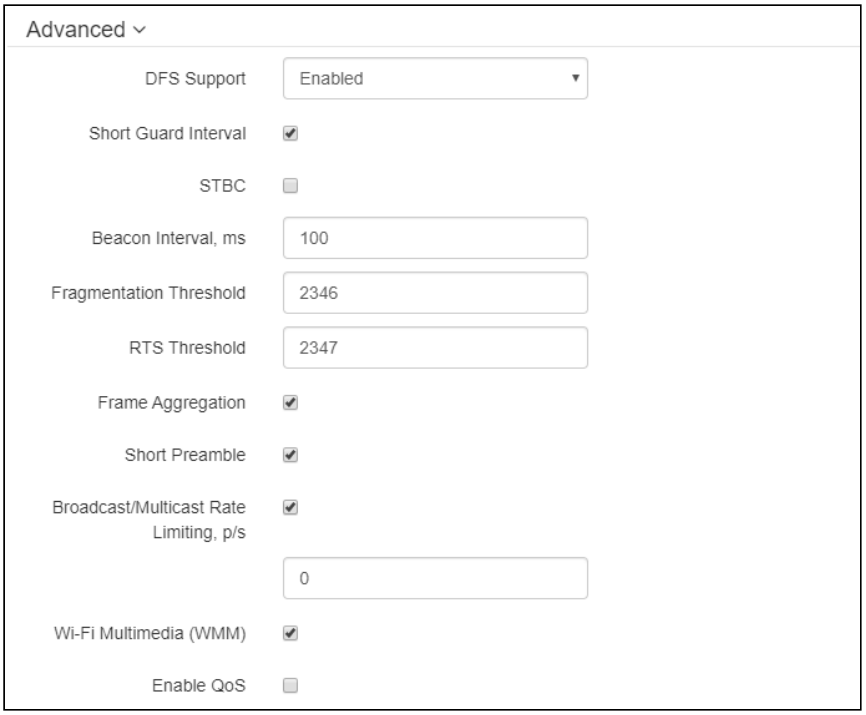
- *Channel* – select channel for data transmission;
- *Use Limit Channels* – when checked, the access point will use a user-defined list of channels to work in automatic channel selection mode. If the «Use Limit Channels» flag is not checked or there are no channels in the list, the access point will select the operation channel from all available channels in the given band. 5 GHz range channels: 36-64, 132-144, 149-165;
- *Channel Bandwidth, MHz* – channel bandwidth, on which the access point operates. The parameter may take values of 20, 40 and 80 MHz;
- *Primary Channel* – the parameter can only be changed if the bandwidth of a statically specified channel is equal to 40 MHz. The 40 MHz channel can be considered as consisting of two 20 MHz channels, which border in the frequency range. These two 20 MHz channels are called primary and secondary channels. The primary channel is used by clients who only support 20 MHz channel bandwidth:
    - *Upper* – the primary channel will be the upper 20 MHz channel in the 40 MHz band;
    - *Lower* – the primary channel will be the lower 20 MHz channel in the 40 MHz band.
- *Transmission Power Limit, dBm* – transmitting Wi-Fi signal power adjustment, dBm. May take values between 11 and 19 dBm;
- *Fixed Transmit Rate* – fixed wireless data transmission rate which is defined by IEEE 802.11a/n/ac standards.

If the «Use Limit Channels» list contains a channel that is not available for selection, it will be marked in grey. In order for the new configuration to be applied to an access point, only available (blue highlighted) channels must be specified in the «Use Limit Channels» list.
Example. No settings have been made on the access point yet, Radio 1 is set to 20 MHz «Channel Bandwidth» by default, and channels are specified in the «Use Limit Channels» list: 36, 40, 44, 48. Suppose the parameter «Channel Bandwidth» is set to 40 MHz. When you change this parameter from 20 MHz to 40 MHz, the following happens:

- the «Primary channel» parameter becomes available for editing and the default value is «Upper»;
- channels 36 and 44 in the «Use Limit Channels» list changes its color from blue to gray.

If you change the «Channel Bandwidth» parameter to 40 MHz and do not remove the «grey» channels from the list, then when you click on the «Apply» button in the browser an error will appear – «There are errors in data. Changes was not applied». Accordingly, the access point configuration will not be changed. This is due to the fact that channels in the «Use Limit Channels» list that are highlighted in grey do not fit the definition «Primary channel» = Upper.

In the «Advanced» section, you can configure advanced device's radio interface parameters.



- *OBSS Coexistence* – automatic channel bandwidth reduction when the air is loaded. When the flag is set, the mode is enabled;
- *DFS Support* – dynamic frequency selection mechanism. The mechanism demands wireless devices to scan environment and avoid using channels which coincide with radiolocation system's channels at 5 GHz:
    - *Disabled* – the mechanism is disabled. DFS channels are not available for selection;
    - *Enabled* – the mechanism is enabled;
    - *Forced* – the mechanism is disabled. DFS channels are available for selection.
- *Short Guard interval* – support for Short Guard interval. Access point transmits data using 400 ns Guard interval (instead of 800 ns) to clients which also support Short GI;
- *STBC* – Soace-Time Block Coding method dedicated to improve data transmission reliability. The field is available only if the selected mode of operation of the radio interface includes 802.11n. When checked, the device transmits one data flow through several antennas. When unchecked, the device does not transmit one data flow through several antennas;
- *Beacon Interval, ms* – beacon frames transmission period. The frames are sent to detect access points. The parameter takes values from 20 to 2000 ms, by default – 100 ms;
- *Fragmentation Threshold* – frame fragmentation threshold, bytes. The parameter takes values 256-2346, by default – 2346;
- *RTS Threshold* – after what quantity of bytes the Request to Send will be sent. Decreasing of the parameter's value might improve access point operation when there are a lot of clients connected. However, decreasing of the parameter's value will reduce general bandwidth of wireless network. The parameter takes values from 0 to 2347, by default – 2347;
- *Aggregation* – enable support for AMPDU/AMSDU;
- *Short Preamble* – use of the packet short preamble;
- *Broadcast/Multicast Rate Limiting, p/s* – when the flag is set, transmission of broadcast / multicast traffic over the wireless network is restricted. Specify the limit for broadcast traffic in the popup window (p/s);
- *Wi-Fi Multimedia (WMM)* – WMM support activation (Wi-Fi Multimedia);
- *Enable QoS* – when the flag is set, the setting of Quality of Service functions is available.

The following functions are available for quality assurance configuration:

AP EDCA Parameters

Queue	AIFS	cwMin	cwMax	TXOP Limit
Data 3 (Background)	7	15	1023	0
Data 2 (Best Effort)	3	15	63	0
Data 1 (Video)	1	7	15	94
Data 0 (Voice)	1	3	7	47

Station EDCA Parameters

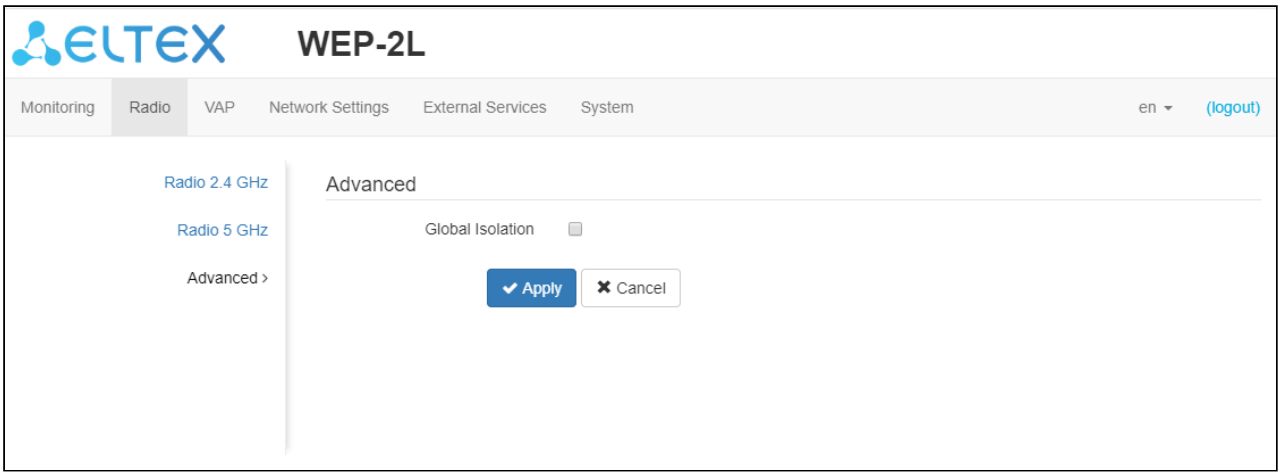
Queue	AIFS	cwMin	cwMax	TXOP Limit
Data 3 (Background)	7	15	1023	0
Data 2 (Best Effort)	3	15	1023	0
Data 1 (Video)	2	7	15	94
Data 0 (Voice)	2	3	7	47

- *AP EDCA parameters* – access point settings table (traffic is transmitted from the access point to the client):
  - *Queue* – predefined queues for various kinds of traffic:
    - *Data 3 (Background)* – low priority queue, high bandwidth (802.1p: cs1, cs2 priorities);
    - *Data 2 (Best Effort)* – middle priority queue, middle bandwidth and delay. Most of the traditional IP data is sent to this queue (802.1p: cs0, cs3 priorities);
    - *Data 1 (Video)* – high priority queue, minimal delay. In this queue, time-sensitive video data is automatically processed (802.1p: cs4, cs5 priorities);
    - *Data 0 (Voice)* – high priority queue, minimal delay. In this queue, time sensitive data is automatically processed, such as: VoIP, streaming video (802.1p: cs6, cs7 priorities).
  - *AIFS* – Arbitration Inter-Frame Spacing, defines the waiting time of data frames, measured in slots, takes values (1-255);
  - *cwMin* – the initial timeout value before resending a frame, specified in milliseconds, takes the values 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023. The value of cwMin cannot exceed the value of cwMax;
  - *cwMax* – the maximum timeout value before resending a frame, specified in milliseconds, takes the values 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023. The value of cwMax must exceed the value of cwMin;
  - *TXOP Limit* – this parameter is used only for data transmitted from the client station to the access point. The transmission capability is the time interval, in milliseconds, when the client WME station has the rights to initiate data transmission over the wireless medium to the access point, the maximum value is 65535 milliseconds;
- *Station EDCA parameters* – table of client station parameter settings (traffic is transmitted from the client station to the access point). For description of table fields, see above.

To apply a new configuration and save setting to non-volatile memory, press «Apply». Press «Cancel» to discard the changes.

5.5.3 The «Advanced» submenu

In the «**Advanced**» section, you can configure advanced device's radio interface parameters.



- *Global Isolation* – when checked, traffic isolation between clients of different VAP and different radio interfaces is enabled.

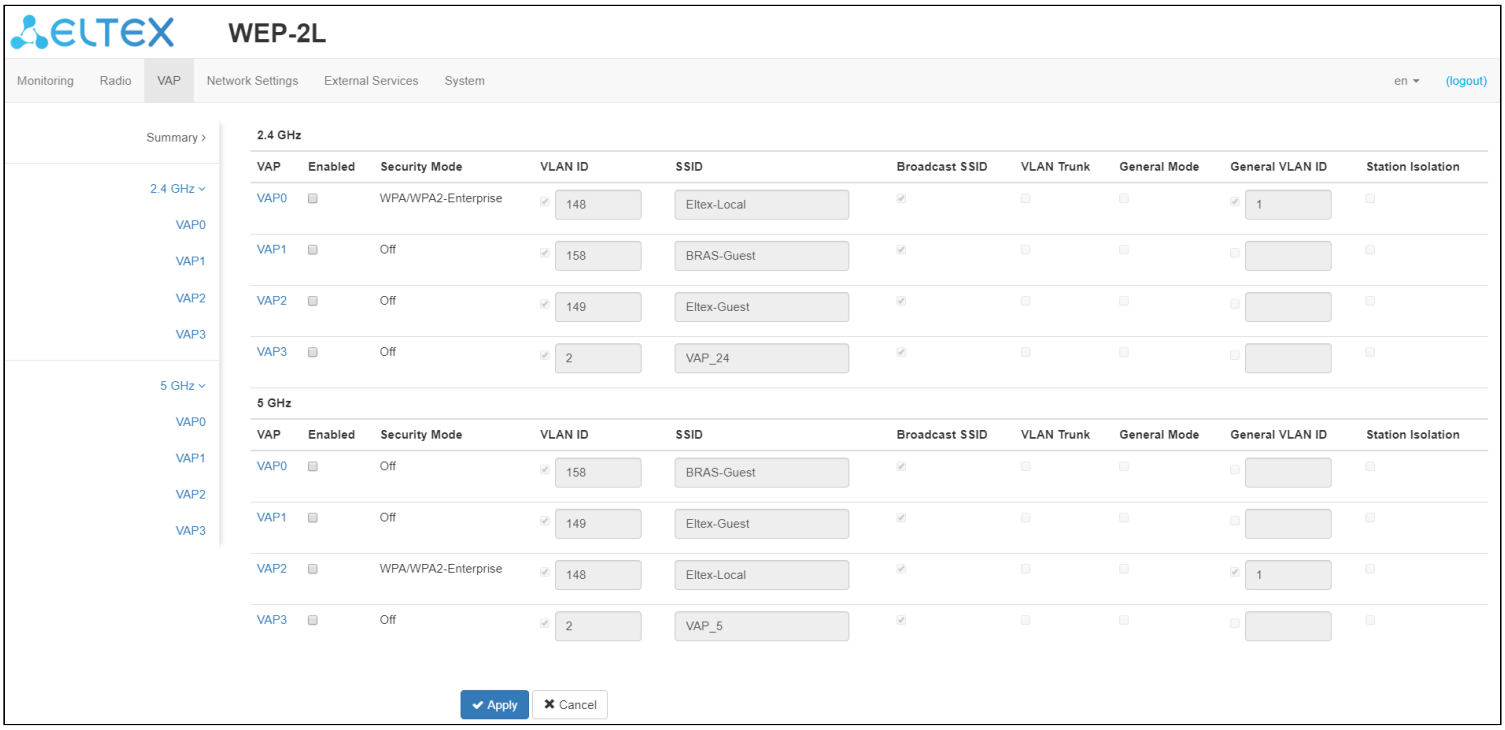
To apply a new configuration and save setting to non-volatile memory, press «Apply». Press «Cancel» to discard the changes.

5.6 The «VAP» menu

In the «**VAP**» menu, you can configure virtual Wi-Fi access points (VAP).

5.6.1 The «Summary» submenu

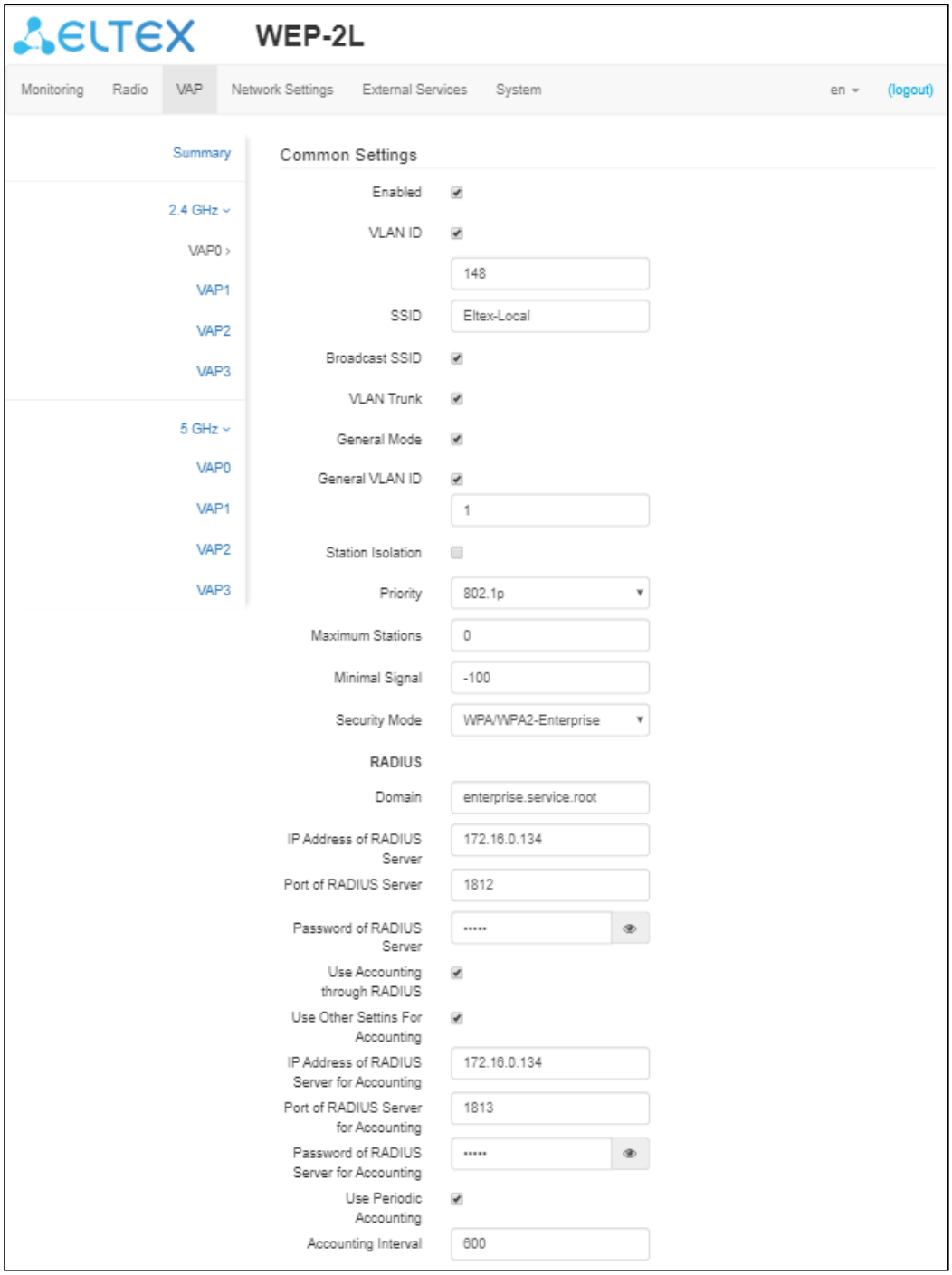
The «**Summary**» submenu displays the settings of all VAPs on Radio 2.4 GHz and Radio 5 GHz radio interfaces. You can see the settings of each virtual access point in sections VAP0..3.



- *VAP0..3* – the sequence number of the virtual access point;
- *Enabled* – when checked, the virtual access point is enabled, otherwise it is disabled;
- *Security Mode* – the type of data encryption used on the virtual access point;
- *VLAN ID* – VLAN number from which the tag will be removed when transmitting Wi-Fi traffic to clients connected to this VAP. When traffic flows in the opposite direction, untagged traffic from clients will be tagged with VLAN ID (when VLAN Trunk mode is disabled);
- *SSID* – virtual wireless network name;
- *Broadcast SSID* – when checked, SSID broadcasting is on, otherwise it is disabled;
- *VLAN Trunk* – when the flag is set, tagged traffic is transmitted to the subscriber;
- *General Mode* – when the flag is set, transmission of untagged traffic jointly with tagged traffic is allowed (available when Trunk VLAN mode is enabled);
- *General VLAN ID* – a tag will be removed from the specified VLAN ID and the traffic of this VLAN will pass to the client without a tag. When traffic passes in the opposite direction, untagged traffic will be tagged with General VLAN ID;
- *Station Isolation*– when checked, traffic isolation between clients in the same VAP is enabled.

To apply a new configuration and save setting to non-volatile memory, press «Apply». Press «Cancel» to discard the changes.

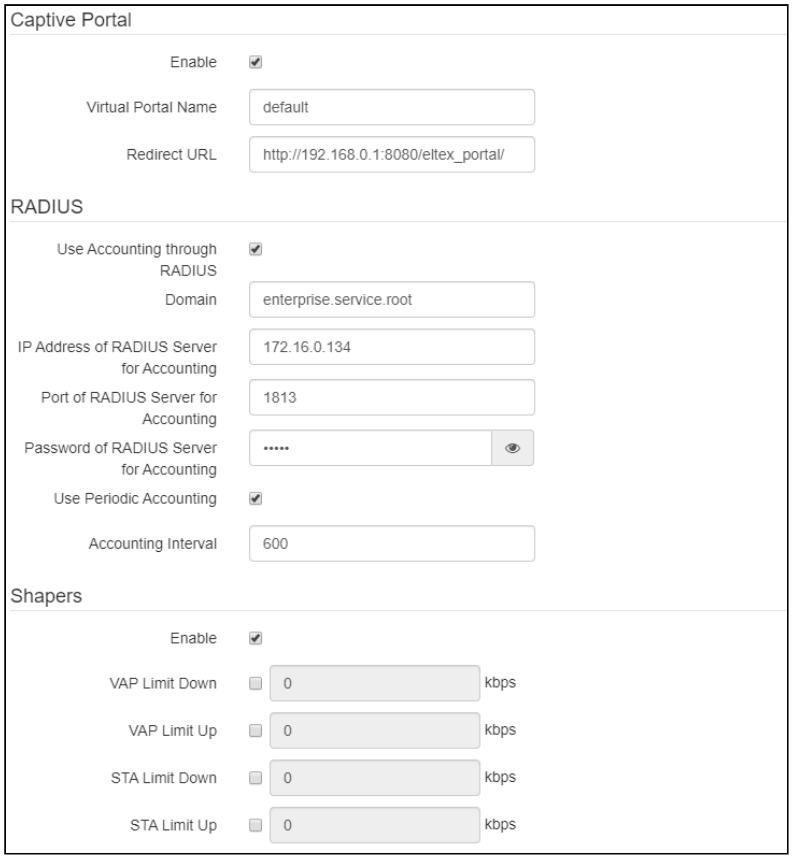
5.6.2 The «VAP» submenu



<u>Common settings</u>

- *Enabled* – when checked, the virtual access point is enabled, otherwise it is disabled;
- *VLAN ID* – VLAN number from which the tag will be removed when transmitting Wi-Fi traffic to clients connected to this VAP. When traffic flows in the opposite direction, untagged traffic from clients will be tagged with VLAN ID (when VLAN Trunk mode is disabled);
- *SSID* – virtual wireless network name;
- *Broadcast SSID* – when checked, SSID broadcasting is on, otherwise it is disabled;
- *VLAN Trunk* – when the flag is set, tagged traffic is transmitted to the subscriber;
- *General Mode* – when the flag is set, transmission of untagged traffic jointly with tagged traffic is allowed (available when Trunk VLAN mode is enabled);

- *General VLAN ID* – a tag will be removed from the specified VLAN ID and the traffic of this VLAN will pass to the client without a tag. When traffic passes in the opposite direction, untagged traffic will be tagged with General VLAN ID;
- *Station Isolation* – when checked, traffic isolation between clients in the same VAP is enabled;
- *Priority* – select prioritization means. Defines the field on the basis of which the traffic transmitted to the radio interface will be distributed in WMM queues:
    - *DSCP* – will analyze the priority from the DSCP field of the IP packet header;
    - *802.1p* – will analyze the priority from the CoS (Class of Service) field of the tagged packets.
- *Maximum Stations* – the maximum number of clients connected to the virtual network;
- *Minimal Signal* – signal level in dBm below which the client equipment is disconnected from the virtual network;
- *Security Mode* – wireless access security mode:
    - *Off* – do not use encryption for data transfer. The access point is available for any subscriber to connect;
    - *WPA, WPA2, WPA/WPA2* – encryption methods, if you select one of the methods, the following setting will be available:
        - *WPA Key* – key/password required to connect to the virtual access point. The length of the key makes from 8 to 63 characters;
    - *WPA-Enterprise, WPA2-Enterprise, WPA/WPA2-Enterprise* – wireless channel encryption mode, in which the client is authorized on the centralized RADIUS server. To configure this security mode, you must specify the parameters of the RADIUS server. You also need to specify a key for the RADIUS server. If you select one of the methods, the following setting will be available:
        - *Domain* – user domain;
        - *IP Address of RADIUS Server* – RADIUS server address;
        - *Port of RADIUS Server*– port of the RADIUS server that used for aithentication and authorization;
        - *Password of RADIUS Server* – password for the RADIUS server used for authentication and authorization;
        - *Use Accounting through RADIUS* – when checked, «Accounting» messages will be sent to the RADIUS server;
        - *Use Other Settings For Accounting:*
            - *IP Address of RADIUS Server for Accounting* – address of the RADIUS server, used for accounting;
            - *Password of RADIUS Server for Accounting*– password for the RADIUS server used for accounting.
        - *Port of RADIUS Server for Accounting* – port that will be used to collect accounts on the RADIUS server:
            - *Use Periodic Accounting* – enable periodic sending of «Accounting» messages to the RADIUS server. You can set the interval for sending messages in the «Accounting Interval» field.



Captive Portal

Under security modes: Off, WPA, WPA2, WPA/WPA2 a portal authorization setting is available on the VAP.

- Enable – when checked, authorization of users in the network will be performed via the virtual portal;
- Virtual Portal Name – name of the virtual portal to which the user will be redirected when connecting to the network;
- Redirect URL – the address of the external virtual portal to which the user will be redirected when connecting to the network.

RADIUS

- *Use Accounting through RADIUS* – when checked, «Accounting» messages will be sent to the RADIUS server;
- *Domain* – user domain;
- *IP Address of RADIUS Server for Accounting* – address of the RADIUS server, used for accounting;
- *Port of RADIUS Server for Accounting* – port that will be used to collect accounts on the RADIUS server;
- *Password of RADIUS Server for Accounting* – password for the RADIUS server used for accounting;
- *Use Periodic Accounting* – enable periodic sending of «Accounting» messages to the RADIUS server. You can set the interval for sending messages in the «Accounting Interval» field.

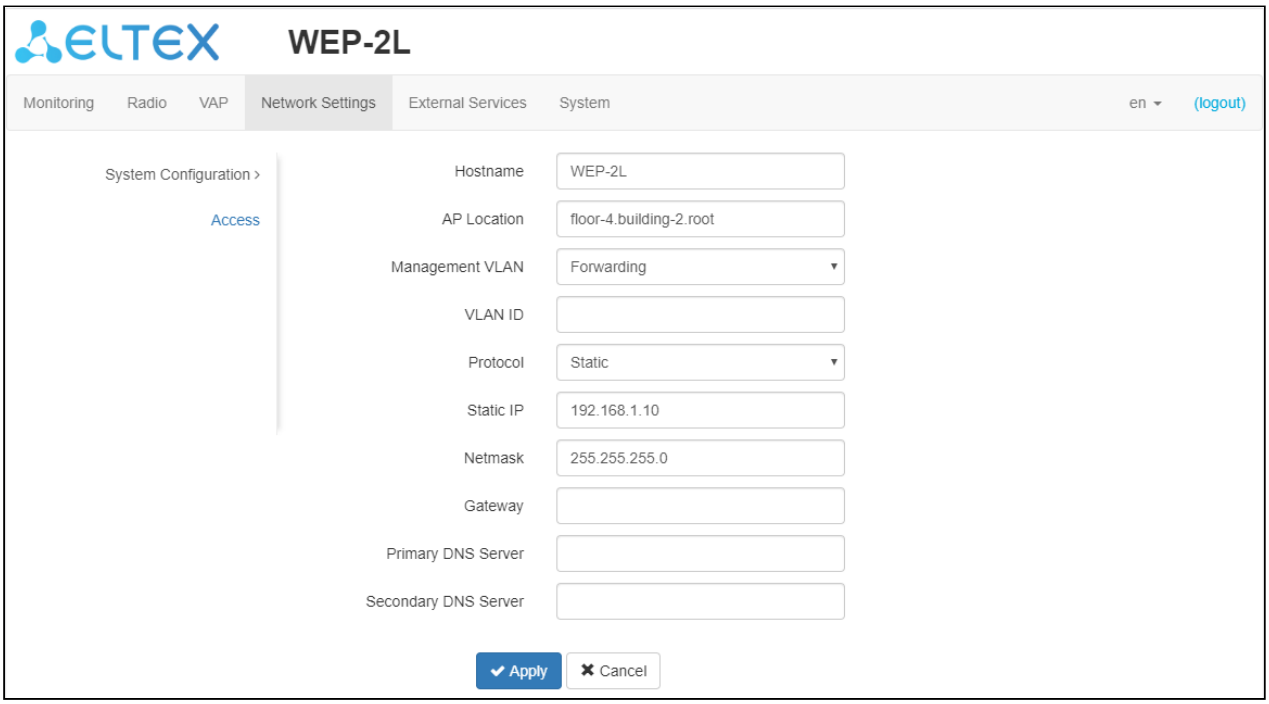
Shapers

- *Show* – display configuration field;
- *VAP Limit Down* – restriction of bandwidth in the direction from the access point to the clients (in total) connected to this VAP, Kbps;
- *VAP Limit Up* – restriction of bandwidth in the direction from the clients (in total) connected to this VAP, to the access point, Kbps;
- *STA Limit Down* – restriction of bandwidth in the direction from the access point to the clients (each separately) connected to this VAP, Kbps;
- *STA Limit Up* – restriction of bandwidth in the direction from the clients (each separately) connected to this VAP, to the access point, Kbps.

To apply a new configuration and save setting to non-volatile memory, press «Apply». Press «Cancel» to discard the changes.

5.7 The «Network Settings» menu

5.7.1 The «System Configuration» submenu

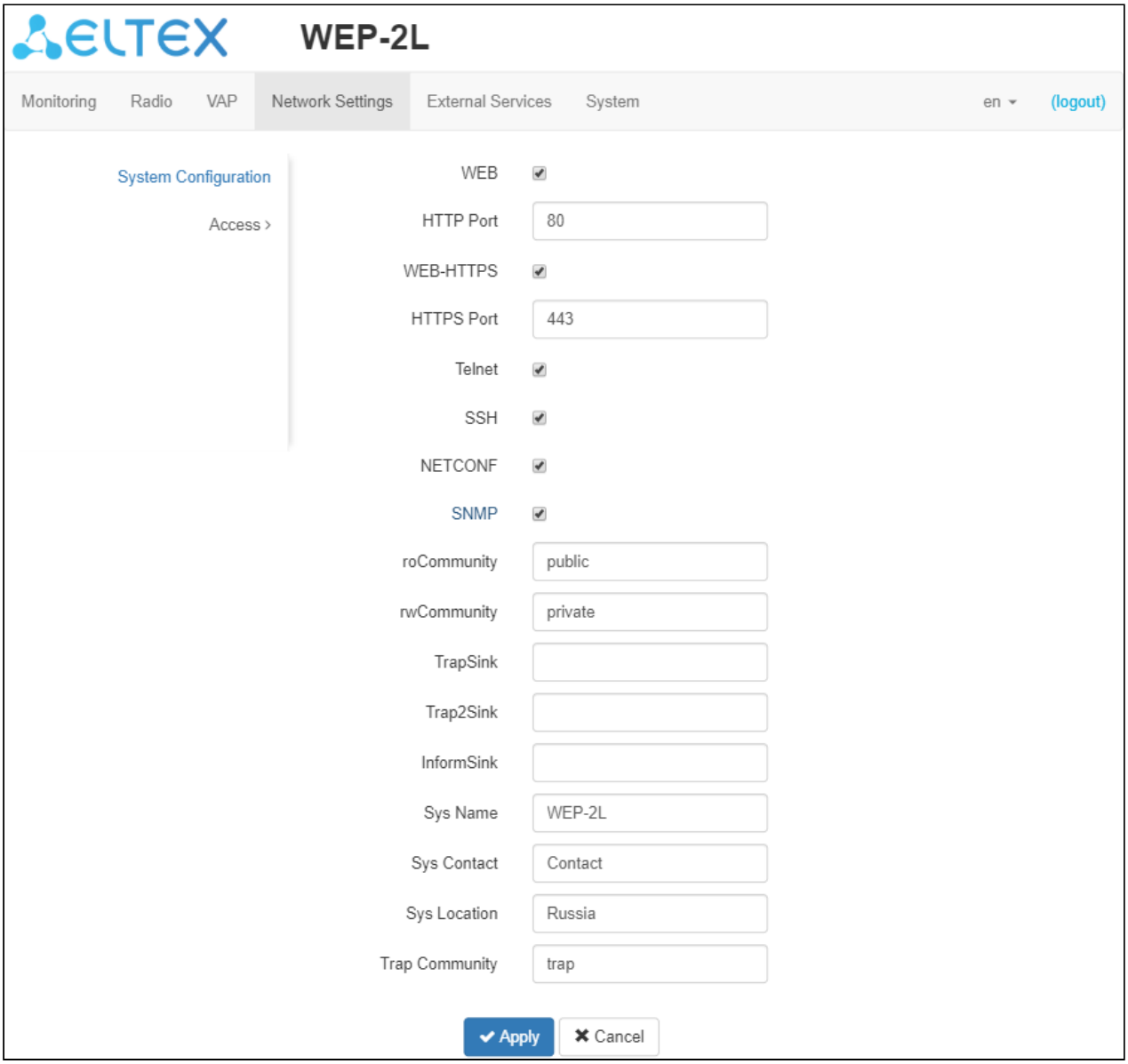


- *Hostname* – nertwork name of the device, specified by string from 1 to 63 characters; latin uppercase and lowercase letters, numbers, hyphen «-» (hyphen can not be the last character in the name);
- *AP Location* – domain of the EMS management system tree host where the access point is located;
- *Management VLAN*:
  - *Disabled* – Management VLAN is not used;
  - *Terminating* – the mode in which the management VLAN is terminated at the access point; in this case, clients connected via the radio interface do not have access to this VLAN;
  - *Forwarding* – the mode in which the management VLAN is also transmitted to the radio interface (with the appropriate VAP configuration).
- *VLAN ID* – the VLAN ID used to access the device, takes values 1-4094;
- *Protocol* – select protocol for connection of the device via Ethernet interface to service provider network:
  - *DHCP* – operation mode, when IP address, subnet mask, DNS server address, defualt gateway and other parameters required for operation are obtained from DHCP server automatically;
  - *Static* – operation mode where IP address and all the necessary parameters for WAN interface are assigned statically. If «Static» is selected, the following parameters will be available to set:
    - *Static IP* – device WAN interface IP address in the provider network;
    - *Netmask* – external subnet mask;
    - *Gateway* – address, to which the packet is sent, if the route in routing table is not found for it.
  - *Primary DNS server, Secondary DNS server* – IP address of DNS servers. If DNS servers' addresses are not allocated automatically via DHCP, set them manually.

To apply a new configuration and save setting to non-volatile memory, press «Apply». Press «Cancel» to discard the changes.

5.7.2 The «Access» submenu

In the «**Access**» submenu, you can configure access to the device via the web interface, Telnet, SSH, NETCONF and SNMP.



- To enable access to the device via the web interface via HTTP protocol, set the flag next to «WEB». In the window that appears, it is possible to change the HTTP port (by default, 80). The range of acceptable values of ports, in addition to the default, from 1025 to 65535 inclusive;
- To enable access to the device via the web interface via HTTPS protocol, set the flag next to «WEB-HTTPS». In the window that appears, it is possible to change the HTTPS port (by default, 443). The range of acceptable values of ports, in addition to the default, from 1025 to 65535 inclusive;

> Note that the ports for the HTTP and HTTPS protocols should not have the same value.

WEP-2L software allows monitoring status of the device and it's sensors via SNMP. In the SNMP submenu, you can configure settings of SNMP agent. The device supports SNMPv1 and SNMPv2 protocol version.

To change the SNMP settings, check the box next to «SNMP», apply the configuration and then go to the SNMP submenu.

- *roCommunity* – a password to read the parameters (by default: *public*);
- *rwCommunity* – a password to configure (write) parameters (by default: *private*);
- *TrapSink* – IP address or domain name of SNMPv1-trap message recipient in HOST [COMMUNITY [PORT]] format;
- *Trap2Sink* – IP address or domain name of SNMPv2-trap message recipient in HOST [COMMUNITY [PORT]] format;
- *InformSink* – IP address or domain name of Inform message recipient in HOST [COMMUNITY [PORT]] format;
- *Sys Name* – device name;
- *Sys Contact* – device vendor contact information;
- *Sys Location* – device location information;
- *Trap community* – password enclosed in traps (default value: trap).

The list of objects which are supported for reading and configuration via SNMP is given below:

- eltexLtd.1.127.1 – monitoring access point parameters and connected client devices;
- eltexLtd.1.127.3 – access point management (reboot).

where eltexLtd – 1.3.6.1.4.1.35265 is Eltex Enterprise ID.

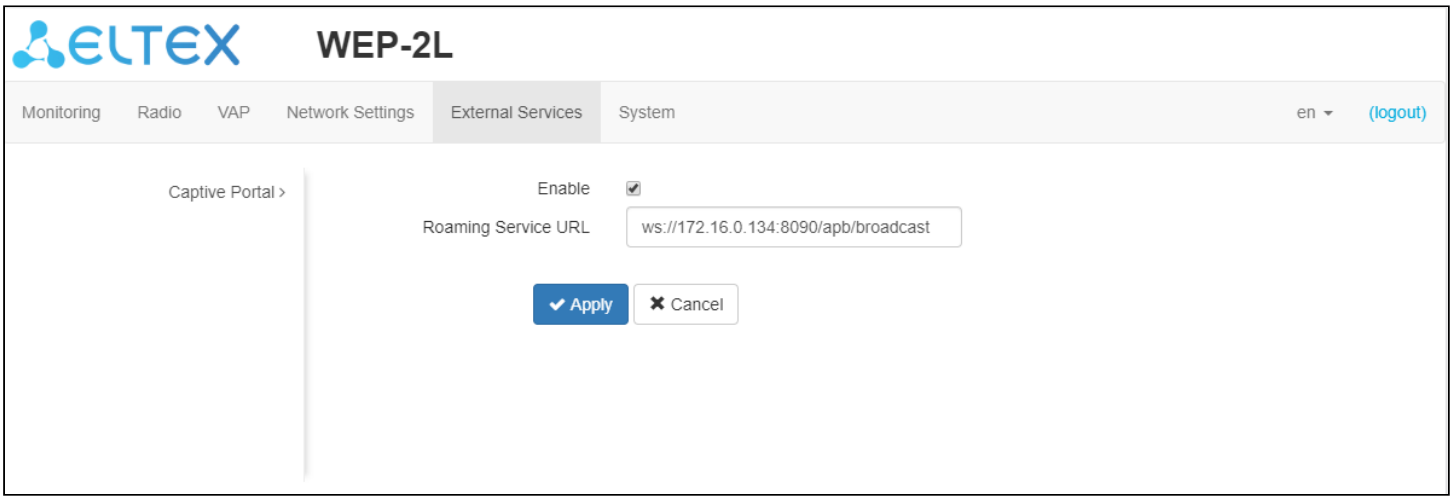
To apply a new configuration and save setting to non-volatile memory, press «Apply». Press «Cancel» to discard the changes.

5.8 The «External Services» menu

5.8.1 The «Captive Portal» submenu

The **«Captive Portal»** submenu is designed to enable and configure the APB service at the access point.

The APB service is used to provide portal roaming of clients between access points connected to the service.



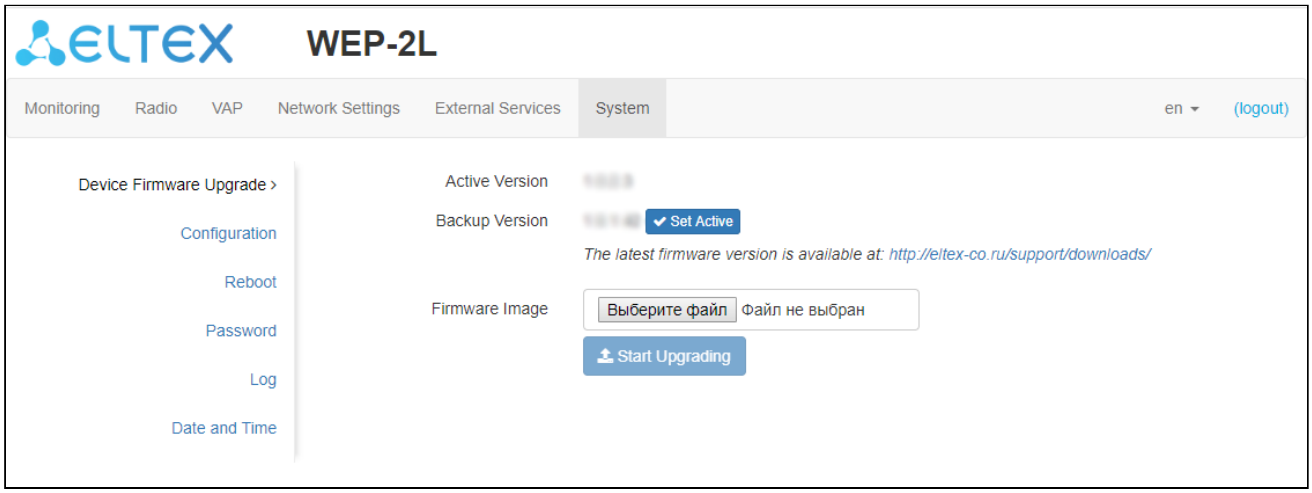
- *Enable* – when checked, the point will connect to the APB service, the address of which is specified in the «Roaming Service URL» field, to provide portal roaming of clients;
- *Roaming Service URL* – APB service address to support roaming in the portal authorization mode. Set in format: "ws://<host>:<port>/apb/broadcast".

5.9 The «System» menu

In the «**System**» menu you can configure system, time, device access via dofferent protocols, change password and update device firmware.

5.9.1 The «Device Firmware Upgrade» submenu

The «**Device Firmware Upgrade**» submenu is intended for upgrading the device's firmware.



- *Active Version* – installed firmware version, which is operating at the moment;
- *Backup version* – installed firmware version which can be used in case of problems with the current active firmware version;
    - *Make active* – a button that allows you to make a backup version of the firmware active, this will require a reboot of the device. The active firmware version will not be set as a backup.

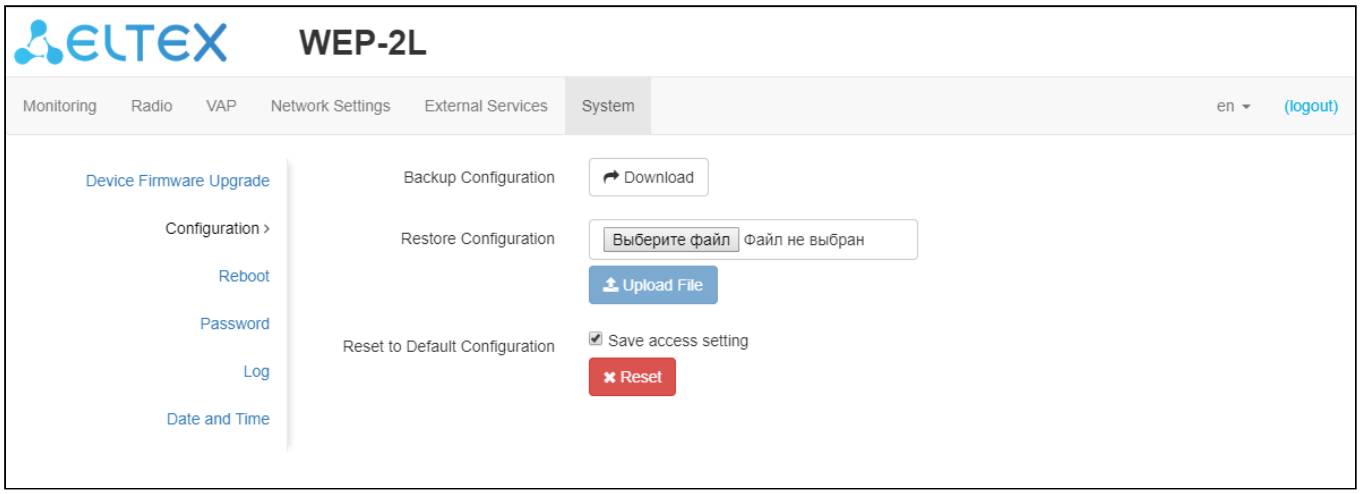
<u>Firmware update</u>

Download the firmware file from *http://eltex-co.com/support/downloads/* and save it on your computer. To do this, click the *«Browse»* button in the Firmware Image field and specify the path to the firmware file in .tar.gz format. To start the update process, you must click the «Start Upgrading» button. The process may take several minutes (its current status will be shown on the page). The device will be automatically rebooted when the update is completed.

Do not switch off or reboot the device during the firmware update.

5.9.2 The «Configuration» submenu

In the **«Configuration»** submenu you can save and update current configuration.



<u>Backup Configuration</u>

To save current device configuration to local computer click on the «Download» button.

<u>Restore Configuration</u>

To download the configuration file saved on the local computer, use the *Restore Configuration* item. To update the device configuration click the «Browse» button, specify a file (in .tar.gz format) and click the «Upload» button. Uploaded configuration will be applied automatically and does not require device reboot.

To change the passwords open the configuration file in text editor and change passwords. Then save the changes in configuration archive. The example of password changing is shown below:

<u>Reset to Default Configuration</u>

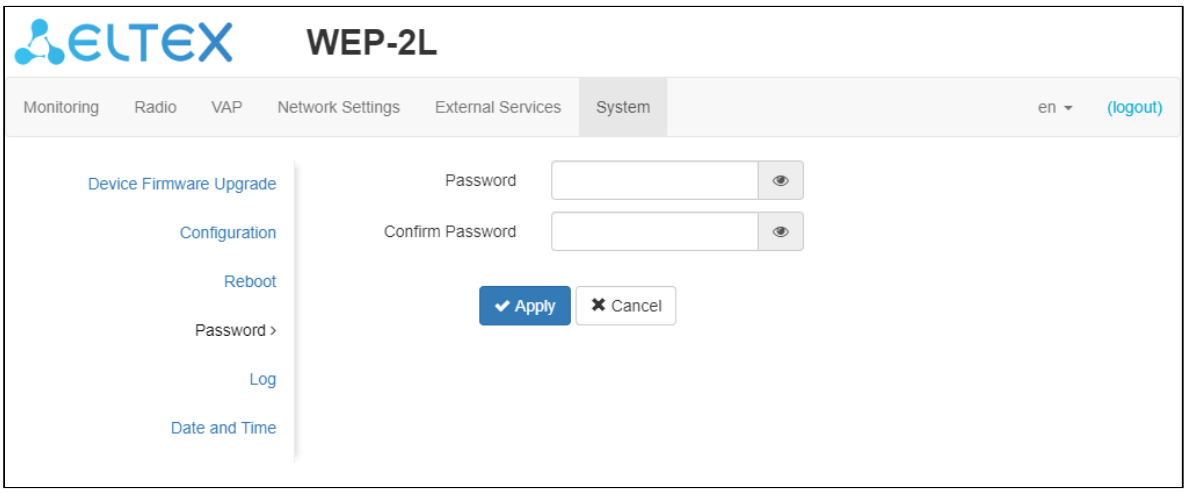
To reset all the settings to default values, press «Reset» button. If the flag «Save access setting» is activated, then those settings, configurations that are responsible for access to the device (IP address settings, Telnet/SSH/SNMP/Netconf/WEB access settings) will be saved

5.9.3 The «Reboot» submenu

To reboot the device, click on the «Reboot» button. The device reboot process takes about 1 minute.

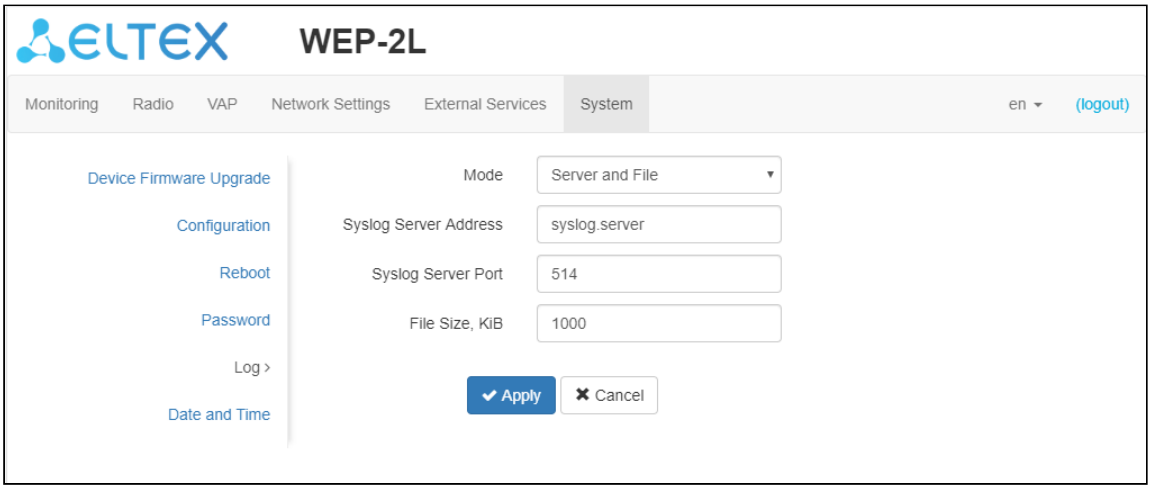
5.9.4 The «Password» submenu

When logging in via WEB interface administrator (default password: **password**) has the full access to the device: read/write any settings, full device status monitoring.
To change the password, enter the new password first in the «Password» field, then in the «Confirm Password» field and click the «Apply» button to save the new password.



5.9.5 The «Log» submenu

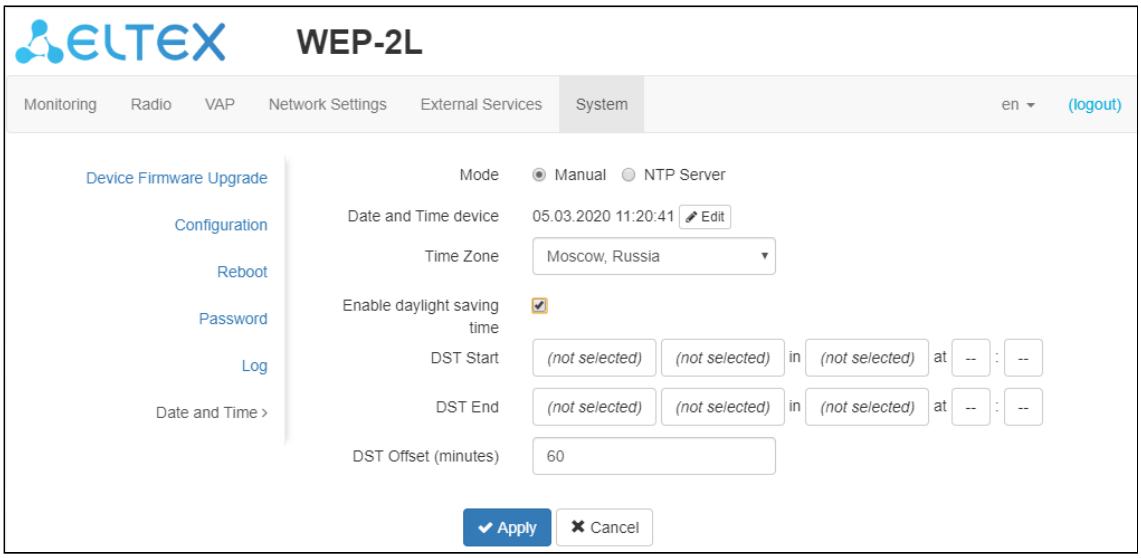
The «Log» submenu is designed to configure the output of various kinds of debugging messages of the system in order to detect the causes of problems in the operation of the device.



- *Mode* – Syslog agent operation mode:
  - *Local File* – log information is stored in a local file and is available in the device's WEB interface on the «Monitoring/Events» tab;
  - *Server and File* – log information is sent to a remote Syslog server and stored in a local file.
- *Syslog Server Address* – IP address or domain name of the Syslog server;
- *Syslog Server Port* – port for incoming Syslog server messages (default: 514, valid values: from 1 to 65535);
- *File Size, KiB* – maximum size of the log file (valid values: 1-1000 kB).

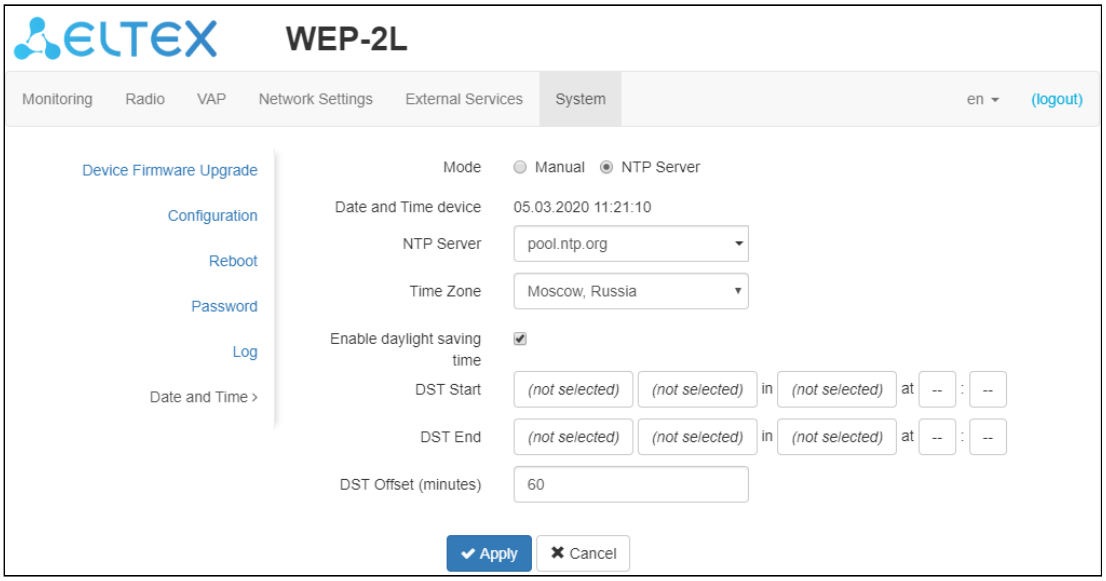
5.9.6 The «Date and Time» submenu

In the «Date and Time» submenu, you can set the time manually or using the time synchronization protocol (NTP). Manual



- *Date and Time device* – date and time set on the device. Click on the «Edit» button if the correction is necessary;
  - *Date, Time* – set the current date and time or click the «Set current date and time» button to synchronize with the device.
- *Time Zone* – allows to set the timezone according to the nearest city for your region from the list;
- *Daylight Saving Time Enable* – when selected, automatic daylight saving change will be performed automatically within the defined time period:
  - *DST Start* – day and time, when daylight saving time is starting;
  - *DST End* – day and time, when daylight saving time is ending;
  - *DST Offset (minutes)* – time period in minutes, on which time offset is performing.

NTP Server



- *Date and Time device* – date and time set on the device;
- *NTP Server* – time synchronization server IP address/domain name. You can specify an address or select from an existing list;
- *Time Zone* – allows to set the timezone according to the nearest city for your region from the list;

To apply a new configuration and store settings into the non-volatile memory, click the *«Apply» button.* To discard changes click the *«Cancel» button.*

6 Managing the device using the command line

To display the existing settings of a particular configuration section, enter the **show-config** command.
Press the key combination (English layout) – **[Shift + ?]** to get a hint of what value this or that configuration parameter can take.
To get a list of options available for editing in this configuration section, press the **Tab** key.
To save the settings, enter the **save** command.
To go back to the previous configuration section, enter the **exit** command.

6.1 Connection to the device

By default, WEP-2L is configured to receive the address via DHCP. If this does not happen, you can connect to the device using the factory IP address.

WEP-2L factory default IP address: **192.168.1.10**, subnet mask: **255.255.255.0**.

Connection to the device is performed via SSH/Telnet:

ssh admin@<IP address of the device>, then enter the password

telnet <IP address of the device>, enter login and password

6.2 Network parameters configuration

Configuration of access point static network parameters

WEP-2L(root):/# **configure**
WEP-2L(config):/# **interface**
WEP-2L(config):/interface# **br0**
WEP-2L(config):/interface/br0# **common**
WEP-2L(config):/interface/br0/common# **static-ip X.X.X.X** (where X.X.X.X - WEP-2L IP address)
WEP-2L(config):/interface/br0/common# **netmask X.X.X.X** (where X.X.X.X - Subnet mask)
WEP-2L(config):/interface/br0/common# **dns-server-1 X.X.X.X** (where X.X.X.X - IP address of the dns server №1)
WEP-2L(config):/interface/br0/common# **dns-server-2 X.X.X.X** (where X.X.X.X - IP address of the dns server №2)
WEP-2L(config):/interface/br0/common# **protocol static-ip** (Change operation mode from DHCP to Static-IP)
WEP-2L(config):/interface/br0/common# **save** (Save configuration)

Configuration of reception of the network parameters via DHCP

WEP-2L(root):/# **configure**
WEP-2L(config):/# **interface**
WEP-2L(config):/interface# **br0**
WEP-2L(config):/interface/br0# **common**
WEP-2L(config):/interface/br0/common# **protocol dhcp**
WEP-2L(config):/interface/br0/common# **save** (Save changes)

6.3 Virtual Wi-Fi access points (VAP) configuration

When configuring a VAP, remember that the interface names in the 2.4 GHz range start with wlan0, in the 5 GHz range with wlan1.

Table 8 – Commands for configuration of security mode on VAP

Security mode	**Command to set the security mode**
Without password	security-mode off
WPA	security-mode WPA
WPA2	security-mode WPA2
WPA/WPA2	security-mode WPA_WPA2
WPA-Enterprise	security-mode WPA_1X
WPA2-Enterprise	security-mode WPA2_1X
WPA/WPA2-Enterprise	security-mode WPA_WPA2_1X

Below are examples of VAP configuration with different security modes for Radio 5 GHz (wlan1).

6.3.1 Configuration of VAP without encryption

Creation of VAP without encryption

WEP-2L(root):/# **configure**
WEP-2L(config):/# **interface**
WEP-2L(config):/interface# **wlan1-va0**
WEP-2L(config):/interface/wlan1-va0# **common**
WEP-2L(config):/interface/wlan1-va0/common# **enabled true** (Enable VAP)
WEP-2L(config):/interface/wlan1-va0/common# **exit**
WEP-2L(config):/interface/wlan1-va0# **vap**
WEP-2L(config):/interface/wlan1-va0/vap# **ssid 'SSID_WEP-2L_open'** (Change SSID name)
WEP-2L(config):/interface/wlan1-va0/vap# **security-mode off** (Encryption mode off - Without password)
WEP-2L(config):/interface/wlan1-va0/vap# **save**

6.3.2 Configuration of VAP with WPA-Personal security mode

Creation of VAP with WPA-Personal security mode

WEP-2L(root):/# **configure**
WEP-2L(config):/# **interface**
WEP-2L(config):/interface# **wlan1-va0**
WEP-2L(config):/interface/wlan1-va0# **common**
WEP-2L(config):/interface/wlan1-va0/common# **enabled true** (Enable VAP)
WEP-2L(config):/interface/wlan1-va0/common# **exit**
WEP-2L(config):/interface/wlan1-va0# **vap**
WEP-2L(config):/interface/wlan1-va0/vap# **ssid 'SSID_WEP-2L_Wpa2'** (Change SSID name)
WEP-2L(config):/interface/wlan1-va0/vap# **security-mode WPA_WPA2** (Encryption mode - WPA/WPA2)
WEP-2L(config):/interface/wlan1-va0/vap# **key-wpa password123** (Key/password required to connect to the virtual access point. The key must be between 8 and 63 characters long.)
WEP-2L(config):/interface/wlan1-va0/vap# **save**

6.3.3 Configuration of VAP with Enterprise authorization

Creation of VAP with WPA2-Enterprise security mode with periodic accounting to RADIUS server

WEP-2L(root):/# **configure**
WEP-2L(config):/# **interface**
WEP-2L(config):/interface# **wlan1-va0**
WEP-2L(config):/interface/wlan1-va0# **common**
WEP-2L(config):/interface/wlan1-va0/common# **enabled true** (Enable VAP)
WEP-2L(config):/interface/wlan1-va0/common# **exit**
WEP-2L(config):/interface/wlan1-va0# **vap**
WEP-2L(config):/interface/wlan1-va0/vap# **ssid 'SSID_WEP-2L_enterprise'** (Change SSID name)
WEP-2L(config):/interface/wlan1-va0/vap# **security-mode WPA_WPA2_1X** (Encryption mode - WPA/WPA2-Enterprise)
WEP-2L(config):/interface/wlan1-va0/vap# **radius**
WEP-2L(config):/interface/wlan1-va0/vap/radius# **domain root** (where root - User domain)
WEP-2L(config):/interface/wlan1-va0/vap/radius# **auth-address X.X.X.X** (where X.X.X.X - RADIUS server IP address)
WEP-2L(config):/interface/wlan1-va0/vap/radius# **auth-port X** (where X - RADIUS server port, used for authentication and authorization. By default: 1812)
WEP-2L(config):/interface/wlan1-va0/vap/radius# **auth-password secret** (where secret - Password for RADIUS server, used for authentication and authorization)
WEP-2L(config):/interface/wlan1-va0/vap/radius# **acct-enable true** (Enable the sending of «Accounting» messages to the RADIUS server. By default: false)
WEP-2L(config):/interface/wlan1-va0/vap/radius# **acct-address X.X.X.X** (where X.X.X.X - RADIUS server IP address, used for accounting)
WEP-2L(config):/interface/wlan1-va0/vap/radius# **acct-password secret** (where secret - Password for RADIUS server, used for accounting)
WEP-2L(config):/interface/wlan1-va0/vap/radius# **acct-periodic true** (Enable the periodic sending of «Accounting» messages to the RADIUS server. By default: false)
WEP-2L(config):/interface/wlan1-va0/vap/radius# **acct-interval 600** (Interval of sending of «Accounting» messages to the RADIUS server)
WEP-2L(config):/interface/wlan1-va0/vap# **save**

6.3.4 Configuration of VAP with Captive Portal

Commands to configure portal authorization by sending your account to the Radius server

WEP-2L(root):/# **configure**
WEP-2L(config):/# **interface**
WEP-2L(config):/interface# **wlan1-va0**
WEP-2L(config):/interface/wlan1-va0# **common**
WEP-2L(config):/interface/wlan1-va0/common# **enabled true**
WEP-2L(config):/interface/wlan1-va0/common# **exit**
WEP-2L(config):/interface/wlan1-va0# **vap**
WEP-2L(config):/interface/wlan1-va0/vap# **vlan-id X** (where X - VLAN-ID on VAP)
WEP-2L(config):/interface/wlan1-va0/vap# **security-mode off** (Encryption mode off - Without password)
WEP-2L(config):/interface/wlan1-va0/vap# **ssid 'Portal_WEP-2L'** (Change SSID name)
WEP-2L(config):/interface/wlan1-va0/vap# **captive-portal**
WEP-2L(config):/interface/wlan1-va0/vap/captive-portal# **scenarios**
WEP-2L(config):/interface/wlan1-va0/vap/captive-portal/scenarios# **scenario-redirect**
WEP-2L(config):/interface/wlan1-va0/vap/captive-portal/scenarios/scenario-redirect# **redirect-url http://<IP>:<PORT>/eltex_portal/** (Specify virtual portal URL)
WEP-2L(config):/interface/wlan1-va0/vap/captive-portal/scenarios/scenario-redirect# **index 1**
WEP-2L(config):/interface/wlan1-va0/vap/captive-portal/scenarios/scenario-redirect# **virtual-portal-name default** (Specify portal name. By default: default)
WEP-2L(config):/interface/wlan1-va0/vap/captive-portal/scenarios/scenario-redirect# **exit**
WEP-2L(config):/interface/wlan1-va0/vap/captive-portal/scenarios# **exit**
WEP-2L(config):/interface/wlan1-va0/vap/captive-portal# **enabled true**
WEP-2L(config):/interface/wlan1-va0/vap/captive-portal# **exit**
WEP-2L(config):/interface/wlan1-va0/vap# **radius**
WEP-2L(config):/interface/wlan1-va0/vap/radius# **domain root** (where root - User domain)
WEP-2L(config):/interface/wlan1-va0/vap/radius# **acct-enable true** (Enable the sending of «Accounting» messages to the RADIUS server. By default: false)
WEP-2L(config):/interface/wlan1-va0/vap/radius# **acct-address X.X.X.X** (where X.X.X.X - RADIUS server IP address, used for accounting)
WEP-2L(config):/interface/wlan1-va0/vap/radius# **acct-password secret** (where secret - Password for RADIUS server, used for accounting)
WEP-2L(config):/interface/wlan1-va0/vap/radius# **acct-periodic true** (Enable the periodic sending of «Accounting» messages to the RADIUS server. By default: false)
WEP-2L(config):/interface/wlan1-va0/vap/radius# **acct-interval 600** (Interval of sending of «Accounting» messages to the RADIUS server)
WEP-2L(config):/interface/wlan1-va0/vap/radius# **save**

6.3.5 Advanced VAP settings:

Enabling VLAN trunk on VAP

WEP-2L(config):/interface/wlan1-va0/vap# **vlan-trunk true** (Enabling VLAN trunk on VAP. To disable, enter **false**)

Enabling General VLAN on VAP

WEP-2L(config):/interface/wlan1-va0/vap# **general-vlan-mode true** (Enabling General VLAN on SSID. To disable, enter **false**)
WEP-2L(config):/interface/wlan1-va0/vap# **general-vlan-id X** (where X – General VLAN number)

Enabling hidden SSID

WEP-2L(config):/interface/wlan1-va0/vap# **hidden true** (Enabling hidden SSID. To disable, enter **false**)

Client limitation on VAP

WEP-2L(config):/interface/wlan1-va0/vap# **sta-limit X** (where X is the maximum allowable number of clients connected to the virtual network)

Enabling client isolation on VAP

WEP-2L(config):/interface/wlan1-va0/vap# **station-isolation true** (Enable traffic isolation between clients within a single VAP. To disable, enter **false**)

Enabling minimal signal

WEP-2L(config):/interface/wlan1-va0/vap# **minimal-signal -X** (where X - RSSI threshold, when reached, the point will disconnect the client from the VAP. The parameter can take values from -100 to 0.)

Enabling TLS usage during authorization

WEP-2L(config):/interface/wlan1-va0/vap/radius# **tls-enable true** (Use TLS during authorization. To disable enter **false**)

6.4 Radio configuration

In the Radio section, automatic selection of the working channel is used by default. To set the channel manually and change the power, use the following commands:

Change of operation channel and radio interface power

WEP-2L(root):/# **configure**
WEP-2L(config):/# **interface**
WEP-2L(config):/interface# **wlan0**
WEP-2L(config):/interface/wlan0# **wlan**
WEP-2L(config):/interface/wlan0/wlan# **radio-2g**
WEP-2L(config):/interface/wlan0/wlan/radio-2g# **tx-power X** (where X - power level, dBm. Parameter can take the following value: for Radio 1: 11-16 dBm; for Radio 2: 11-19 dBm)
WEP-2L(config):/interface/wlan0/wlan/radio-2g#**auto-channel false** (Disable Auto Channel. To enable, enter **true**)
WEP-2L(config):/interface/wlan0/wlan/radio-2g# **use-limit-channels false** (Disable Use Limit Channels. To enable, enter **true**)
WEP-2L(config):/interface/wlan0/wlan/radio-2g# **channel X** (where X - number of the static channel on which the point will operate)

6.4.1 Advanced Radio settings:

Changing the channel bandwidth

WEP-2L(config):/interface/wlan0/wlan/radio-2g# **bandwidth X** (where X - bandwidth. Parameter can take the following value: for Radio 1: 20, 40; Radio 2: 20, 40, 80.)

Changing the primary channel

WEP-2L(config):/interface/wlan0/wlan/radio-2g# **control-sideband lower** (Parameter may take values: lower, upper. By default: for Radio 1: lower; for Radio 2: upper)

Changing a limited list of channels

WEP-2L(config):/interface/wlan0/wlan/radio-2g# **limit-channels '1 6 11'** (where 1, 6, 11 are channels of the range in which the tunable radio interface can operate)

Enabling the use of Short Guard Interval

WEP-2L(config):/interface/wlan0/wlan/radio-2g# **sgi true** (Enabling the use of a Short Guard Interval for data transmission of 400 ns instead of 800 ns. To disable, enter **false**)

Enabling STBC

WEP-2L(config):/interface/wlan0/wlan/radio-2g# **stbc true** (Enabling the Spatial-Time Block Coding (STBC) method, aimed at improving the reliability of data transmission... To disable, enter **false**)

Enabling aggregation

WEP-2L(config):/interface/wlan0/wlan/radio-2g# **aggregation true** (Enabling aggregation on Radio - support for AMPDU/AMSDU. To disable, enter **false**)

Enabling the short preamble

WEP-2L(config):/interface/wlan0/wlan/radio-2g# **short-preamble true** (Enabling the short packet preamble. To disable, enter **false**)

Enabling the Wi-Fi Multimedia (WMM)

WEP-2L(config):/interface/wlan0/wlan/radio-2g# **wmm true** (Enabling the support for WMM (Wi-Fi Multimedia) To disable, enter **false**)

Enabling Broadcast/Multicast shaper

WEP-2L(config):/interface/wlan0/wlan/radio-2g# **tx-broadcast-limit X** (where X - Restricting broadcast/multicast traffic over the wireless network, specify a limit for broadcast traffic per packet/s)

Enabling QoS and parameter changes

WEP-2L(config):/interface/wlan0/wlan/radio-2g# **qos**
WEP-2L(config):/interface/wlan0/wlan/radio-2g/qos# **enable true** (Enabling the use of Quality of Service functions.) To disable, enter **false**)
WEP-2L(config):/interface/wlan0/wlan/radio-2g/qos# **edca-ap** (Configuring the access point's QoS parameters (traffic is transmitted from the access point to the client))
WEP-2L(config):/interface/wlan0/wlan/radio-2g/qos/edca-ap# **bk** (Configure QoS parameters for low-priority high-bandwidth queues (802.1p priorities: cs1, cs2))
WEP-2L(config):/interface/wlan0/wlan/radio-2g/qos/edca-ap/bk# **aifs X** (where X - the time frame(s) of data measured in slots. Takes the values: 1-255)
WEP-2L(config):/interface/wlan0/wlan/radio-2g/qos/edca-ap/bk# **cwmin X** (X - The initial value of the waiting time before sending the frame again is set in milliseconds. Takes the following values: 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023. The value of cwMin may not exceed the value of cwMax)
WEP-2L(config):/interface/wlan0/wlan/radio-2g/qos/edca-ap/bk# **cwmax X** (where X - The maximum waiting time before resending a frame is set in milliseconds. Takes the following values: 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023. The value of cwMax must be greater than the value of cwMin)
WEP-2L(config):/interface/wlan0/wlan/radio-2g/qos/edca-ap/bk# **txop X** (where X - The time interval, in milliseconds, in which the client WME station is allowed to initiate data transmission over the wireless environment to the access point. Max value – 65535 ms)
WEP-2L(config):/interface/wlan0/wlan/radio-2g/qos/edca-ap/bk# **exit**
WEP-2L(config):/interface/wlan0/wlan/radio-2g/qos/edca-ap# **exit**
WEP-2L(config):/interface/wlan0/wlan/radio-2g/qos# **edca-sta** (Configuring the client station QoS parameters (traffic is transmitted from the client station to the access point))

The configuration method of **edca-sta** is the same as that of **edca-ap**.
Parameters configuration for queues **be**, **vi**, **vo** is similar to parameters configuration for queue **bk**.

6.5 System settings

6.5.1 Device firmware update

Device firmware update via tftp

WEP-2L(root):/# **firmware upload tftp <tftp server IP address> <Firmware image name>** (Example: firmware upload tftp 192.168.1.15 WEP-2L-1.1.0_build_444.tar.gz)
WEP-2L(root):/# **firmware upgrade**

Device firmware update via http

WEP-2L(root):/# **firmware upload http <URL to download Firmware image>** (Example: firmware upload http http://192.168.1.100:8080/files/WEP-2L-1.1.0_build_444.tar.gz)
WEP-2L(root):/# **firmware upgrade**

6.5.2 Device configuration management

Resetting the device configuration to a default state without saving the access parameters
WEP-2L(root):/# **manage-config reset-to-default**

Resetting the device configuration to a default state with saving the access parameters
WEP-2L(root):/# **manage-config reset-to-default-without-management**

Download the device configuration file to tftp server
WEP-2L(root):/# **manage-config download tftp <tftp server IP address>** (Example: manage-config download tftp 192.168.1.15)

Download configuration file from tftp server to the device
WEP-2L(root):/# **manage-config upload tftp <tftp server IP address> <Configuration file name>** (Example: manage-config upload tftp 192.168.1.15 config.json) WEP-2L(root):/# **manage-config apply** (Apply configuration to the access point)

6.5.3 Device reboot

The command for rebooting the device.
WEP-2L(root):/# **reboot**

6.5.4 Setting the date and time

Commands to configure NTP server time synchronization

WEP-2L(root):/# **configure**
WEP-2L(config):/# **date-time**
WEP-2L(config):/date-time# **mode ntp** (Enable NTP operation mode)
WEP-2L(config):/date-time# **ntp**
WEP-2L(config):/date-time/ntp# **server <NTP server IP address>** (NTP server configuration)
WEP-2L(config):/date-time/ntp# **exit**
WEP-2L(config):/date-time# **common**
WEP-2L(config):/date-time/common# **timezone 'Asia/Novosibirsk (Novosibirsk)'** (Timezone configuration)
WEP-2L(config):/date-time/common# **save**

6.6 APB service configuration

The APB service is used to provide portal roaming of clients between access points connected to the service.

Commands for APB service configuration

WEP-2L(root):/# **configure**
WEP-2L(config):/# **captive-portal**
WEP-2L(config):/captive-portal# **apbd**
WEP-2L(config):/captive-portal/apbd# **roam_service_url <APB service address>** (Example: roam_service_url ws://192.168.1.100:8090/apb/broadcast)
WEP-2L(config):/captive-portal/apbd# **enabled true** (Enabling APB service. To disable it, enter **false**)
WEP-2L(config):captive-portal/apbd# **save**

6.7 Monitoring

6.7.1 Wi-Fi Clients

WEP-2L(root):/# **monitoring clients**

```
 index                     | 0
 interface                 | wlan0-va3
 state                     | ASSOC AUTH_SUCCESS
 hw-addr                   | e0:d9:e3:49:c1:80
 ip-addr                   | 192.168.0.25
 hostname                  | WB-2P-LR2
 authorized                | true
 captive-portal-vap        | false
 enterprise-vap            | false
 rx-retry-count            | 2
 tx-fails                  | 0
 tx-period-retry           | 0
 tx-retry-count            | 2
 rssi-1                    | -36
 rssi-2                    | -28
 snr-1                     | 22
 snr-2                     | 25
 tx-rate                   | OFDM 48
 rx-rate                   | OFDM 36
 rx-bw                     | 20M
 rx-bw-all                 | 20M
 tx-bw                     | 20M
 uptime                    | 00:00:24
 multicast-groups-count    | 0
 wireless-mode             | g
 eltex-serial-number       | WP36000037
 link-capacity             | 48 (not changed)
 link-quality              | 75 (not changed)
 link-quality-common       | 75
 actual-tx-rate            | 0
 actual-rx-rate            | 0
 actual-tx-pps             | 0
 actual-rx-pps             | 0
 name                      | 0

 Rate                   Transmitted            Received
-----------------------------------------------------------------
 Total Packets:        | 12                   | 13                   |
 TX success:           | 100                  |                      |
 Total Bytes:          | 740                  | 1486                 |
 Data Packets:         | 5                    | 7                    |
 Data Bytes:           | 330                  | 932                  |
 Mgmt Packets:         | 7                    | 6                    |
 Mgmt Bytes:           | 280                  | 372                  |
-----------------------------------------------------------------
```

```
 Rate       Transmitted        Received
-------------------------------------------------
 dsss1     | 7          |  58%|          6 |  50%|
 ofdm6     | 0          |   0%|          3 |  25%|
 ofdm24    | 0          |   0%|          3 |  25%|
 ofdm48    | 1          |   8%|          0 |   0%|
 ofdm54    | 4          |  33%|          0 |   0%|
-------------------------------------------------


Multicast groups: none
```

6.7.2 Device info

WEP-2L(root):/# **monitoring information**

```
system-time: 13:17:13 16.06.2020
uptime: 1 d 02:34:03
software-version: 1.1.0 build 444
secondary-software-version: 1.0.3.6
boot-version: 1.1.0 build 444
memory-usage: 70
memory-free: 32
memory-used: 76
memory-total: 108
cpu: 3.43
is-default-config: false
board-type: WEP-2L
hw-platform: WEP-2L
factory-wan-mac: E8:28:C1:xx:xx:xx
factory-lan-mac: E8:28:C1:xx:xx:xx
factory-serial-number: WP39000026
hw-revision: 1v0
session-password-initialized: false
ott-mode: false
test-changes-mode: false
```

6.7.3 Network information

WEP-2L(root):/# **monitoring wan-status**

```
interface: br0
protocol: dhcp
ip-address: 192.168.1.15
mac: e8:28:c1:xx:xx:xx
mask: 255.255.255.0
gateway: 192.168.1.1
DNS-1: 192.168.1.100
DNS-2:
rx-bytes: 4864149
rx-packets: 13751
tx-bytes: 2462399
tx-packets: 20753
```

WEP-2L(root):/# **monitoring ethernet**

```
link: up
speed: 1000
duplex: enabled
rx-bytes: 4872597
rx-packets: 13844
tx-bytes: 2477091
tx-packets: 20923
```

WEP-2L(root):/# **monitoring arp**

```
#        ip                mac
-------------------------------------------
0        192.168.1.1       02:00:48:xx:xx:xx
1        192.168.1.151     2c:fd:a1:xx:xx:xx
```

WEP-2L(root):/# **monitoring route**

```
Destination       Gateway           Mask              Flags      Interface
-----------------------------------------------------------------------------
0.0.0.0           192.168.1.1       0.0.0.0           UG         br0
192.168.1.0       0.0.0.0           255.255.255.0     U          br0
```

6.7.4 Wireless interfaces

WEP-2L(root):/# **monitoring radio-2**

```
hwaddr: E8:28:C1:xx:xx:xx
status: on
noise-1: -100
noise-2: -100
utilization: 21
channel: 11
thermal: 30
bandwidth: 20
frequency: 2462
```

WEP-2L(root):/# **monitoring radio-5**

```
hwaddr: E8:28:C1:xx:xx:xx
status: on
noise-1: -100
noise-2: -100
utilization: 0
channel: 132
thermal: 31
bandwidth: 20
frequency: 5660
```

6.7.5 Event logging

WEP-2L(root):/# **monitoring events**

```
Jan  23 00:00:07 WEP-2L daemon.info syslogd[925]: started: BusyBox v1.21.1

Jan  23 00:00:09 WEP-2L daemon.info configd[955]: The AP startup configuration was loaded
successfully.

Jan  1 03:00:14 WEP-2L daemon.info networkd[987]: Networkd started

Jan  1 03:01:17 WEP-2L daemon.info networkd[987]: DHCP-client: Interface br0 obtained lease on
192.168.1.15.

Jan 23 07:17:14 WEP-2L daemon.info monitord[1055]: event: 'associated' mac: E4:0E:EE:BD:AE:6B
ssid: 'WEP-2L_2.4GHz' int0
```

6.7.6 Spectrum Analyzer

The spectrum analyzer provides information on channel utilization in the 2.4 and 5 GHz bands. The result is displayed as a percentage.

WEP-2L(root):/# **monitoring spectrum-analyzer**

```
Channel| CCA
      1|  81%
      2|  40%
      3|  14%
      4|  10%
      5|  36%
      6|  60%
      7|  40%
      8|   8%
      9|  14%
     10|  38%
     11|  75%
     12|  37%
     13|  18%
     36|  14%
     40|  12%
     44|  10%
     48|  18%
     52|   3%
     56|   5%
     60|   8%
     64|   6%
    132|   0%
    136|   0%
    140|   0%
    144|   1%
    149|  30%
    153|   1%
    157|   3%
    161|   2%
    165|   1%
```

Please note that all clients will disconnect from the access point during spectrum analyzer operation. Clients will be connected again only when the spectrum analyzer finishes its work.
The analysis time for all the radio channels in two ranges is approximately 5 minutes.

7 The list of changes

Document version	Issue date	Revisions
Version 1.1	30.06.2020	Syncronization with firmware version 1.1.0
Version 1.0	16.03.2020	First issue.
Firmware version 1.1.0		

TECHNICAL SUPPORT

To get technical support regarding our products, please, contact ELTEX Service Center:

29 Okruzhnaya Str., Novosibirsk, Russian Federation, 630020

E-mail: techsupp@eltex-co.ru

You are welcome to visit ELTEX official website to get the relevant technical documentation and software for ELTEX products or consult a Service Center Specialist on our technical forum.

https://eltex-co.com/

https://eltex-co.com/support/downloads/

http://forum.eltex-co.ru/