Wireless access point

WEP-1L

User manual

Firmware version 1.2.2

IP address: 192.168.1.10

Username: admin

Password: password

Contents

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.

The device is dedicated to create L2 wireless networks interfacing with a wired network. WEP-1L 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.

This manual specifies intended purpose, main technical parameters, design, safe operation rules and installation and configuration recommendations for WEP-1L.

1.2 Symbols

Notes and warnings

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

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-1L wireless access point is designed for provision of users' access to high-speed safe network.

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

WEP-1L 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.

WEP-1L is a universal solution for organization of wireless networks with small amount of users and oriented on installation in office or small branch of organization. The ability to create virtual access points with different types of encryption allows to differentiate access rights between ordinary users and dedicated groups of users.

2.2 Device specification

Interfaces:

- 1 port of Ethernet 10/100/1000BASE-T(RJ-45);
- Wi-Fi 2.4 GHz IEEE 802.11b/g/n;
- Wi-Fi 5 GHz IEEE 802.11a/n/ac.

Functions:

WLAN capabilities:

- Support for IEEE 802.11a/b/g/n/ac standards;
- Support for IEEE 802.11r/k/v roaming standards;
- Data aggregation, including A-MPDU (Tx/Rx) and A-MSDU (Rx);
- WMM-based priorities and packet planning;
- Subscriber isolation within one VAP;
- Channel autoselection
- Dynamic frequency selection (DFS);
- Support for hidden SSID;
- 8 virtual access points
- External access point detection;
- Spectrum analyzer.

Network functions:

- Autonegotiation of speed, duplex mode and switching between MDI and MDI-X modes;
- Support for IPv6;
- Support for VLAN;
- Authentication support 802.1X;
- DHCP client;
- GRE;
- GRE over IPsec;
- Transmission of subscriber traffic out of tunnel;
- ACL;
- NTP;
- Syslog.

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 data encryption;
- Support for Captive Portal.

The figure below shows WEP-1L application scheme.

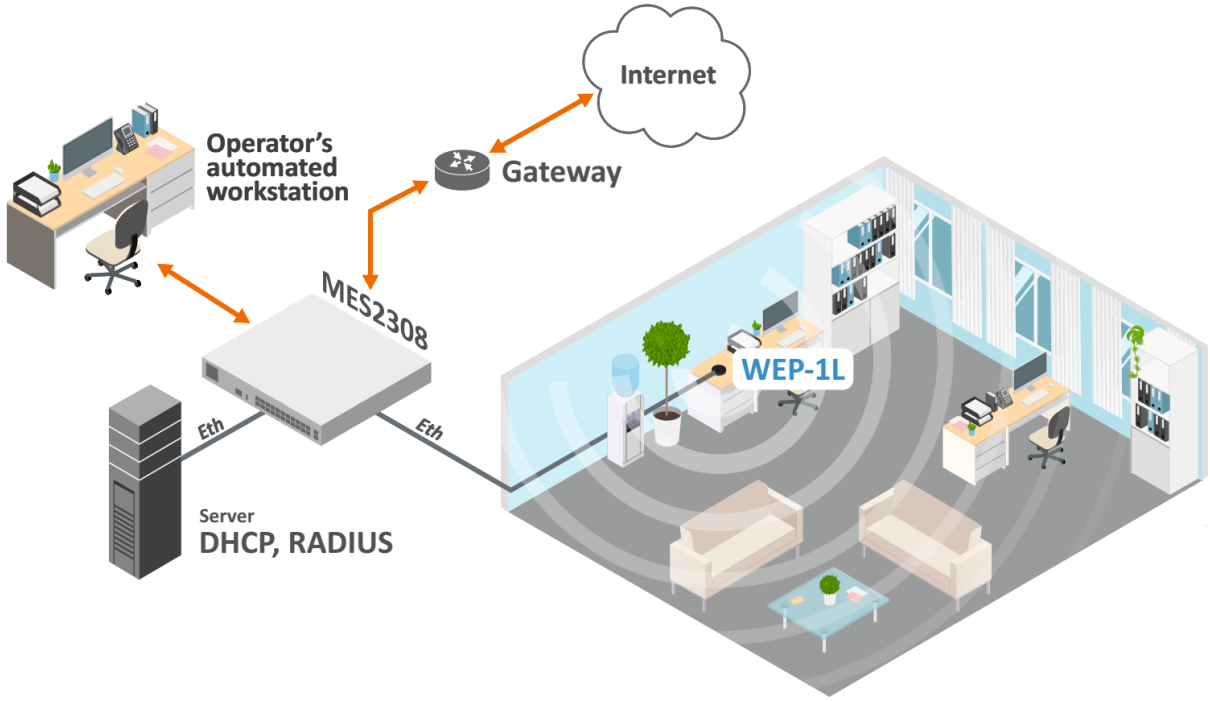


Figure 1 — WEP-1L application scheme

2.3 The device technical parameters

Table 1 — Main Specifications

WAN Ethernet interface parameters	
Number of ports	1
Connector type	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	2400–2483,5 MHz, 5150–5850 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 18 dBm 5 GHz: up to 20 dBm
Built-in antenna gain	2.4 GHz: ~5 dBi 5 GHz: ~5 dBi
Receiver sensitivity	2.4 GHz up to -94 dBm 5 GHz: up to -92 dBm
Security	Centralized authorization via RADIUS server (WPA Enterprise) WPA/WPA2 data encryption Captive Portal
Support for 2x2 MIMO	
Control	
Remote control	Web interface, Telnet, SSH, CLI, SNMP, NETCONF, EMS management system
Access restriction	by password

General parameters	
Flash	32 MB NAND Flash
RAM	128 MB RAM DDR3
Power supply	External power adapter 5.3V DC, 2A
Power consumption	no more than 7 W
range of operation temperatures	from +5°C to +40°C
relative humidity at 25°C	up to 80%
Dimensions (Diameter x Height)	100x23 mm
Weight	85 g

2.4 Design

WEP-1L enclosed in plastic case.

2.4.1 Front panel

The layout of WEP-1L front panel is shown in the figure below.

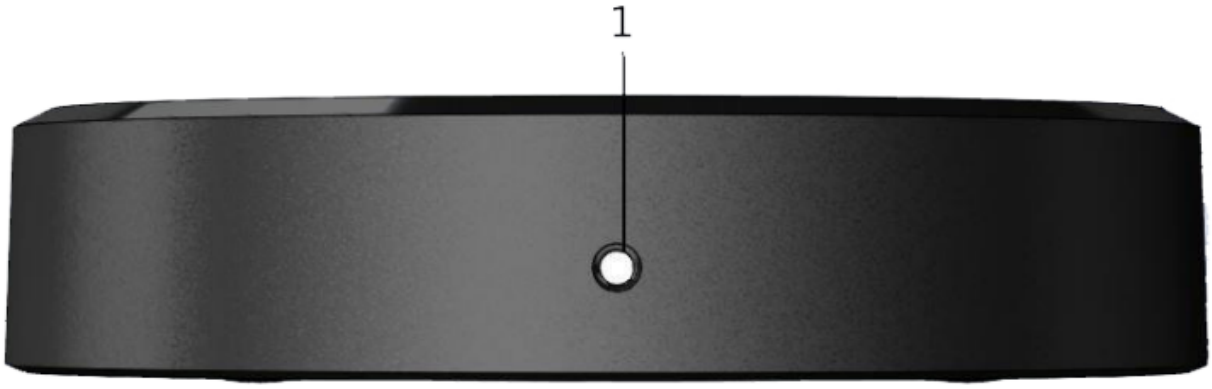


Figure 2 — Front panel of WEP-1L

Table 2 — WEP-1L front panel indicators description

Panel element		Description
1	Power	Device operation LED

2.4.2 Rear panel

The layout of WEP-1L rear panel is shown in the figure below.

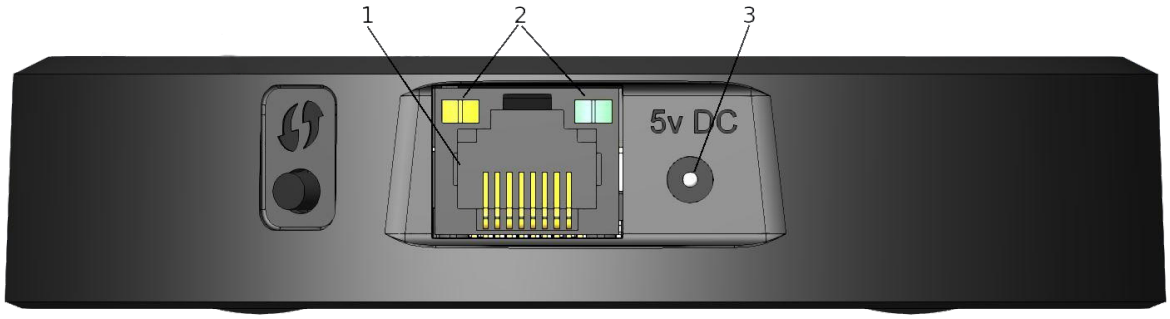


Figure 3 — Rear panel of WEP-1L

LEDs, connectors and controls located on the device main panel are listed in Table 3.

Table 3 — WEP-1L main panel LEDs, ports and controls description

Panel element		Description
1	WAN	10/100/1000BASE-T port (RJ-45 connector) for network connection
2	LEDs	WAN connector indicators
3	5v DC	Power adapter connector

2.4.3 Bottom panel

The layout of WEP-1L bottom panel is shown in the figure below.

Figure 4 — Bottom panel of WEP-1L

Table 4 — WEP-1L bottom panel controls description

Panel element		Description
1	F	Button for resetting to factory settings

2.5 Light indication

The current status of the device is displayed by indicators located on the front and rear panels. The list of indicator states is shown in table 5.

Table 5 — Light indication of device state

Indicator	Indicator's status	Device state
WAN	Only green LED lights	The connection to the connected network device is established at 10/100 Mbps
	Green and orange LEDs light	The connection to the connected network device is established at 1000 Mbps
	Flashing green	Packet data transmission via WAN interface

Indicator	Indicator's status	Device state
Power	solid green	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 the device to the factory settings

To reset the device to the factory settings, press and hold the “F” button until the Power indicator on the front panel flashes orange. There will be an automatic reboot of the device, the indicator will light up in a constant red color.

DHCP client will be launched by default. If the address is not received via DHCP the device will have IP address — 192.168.1.10, subnet mask — 255.255.255.0; User Name/Password to access via web interface: admin/ password.

2.7 Delivery package

The delivery package includes:

- WEP-1L wireless access point;
- 230/5.3V 2.0A power adapter;
- Operations manual on a CD (optional);
- 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.

> In order to avoid components overheating and device malfunctioning, do not place objects on the device.

3.2 Installation recommendations

1. The recommended installation: horizontal, on a table.
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, follow these rules to ensure the best Wi-Fi coverage:
    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.
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-1L with a good-quality signal in case of placing 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 6 — 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 2mm)	-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.

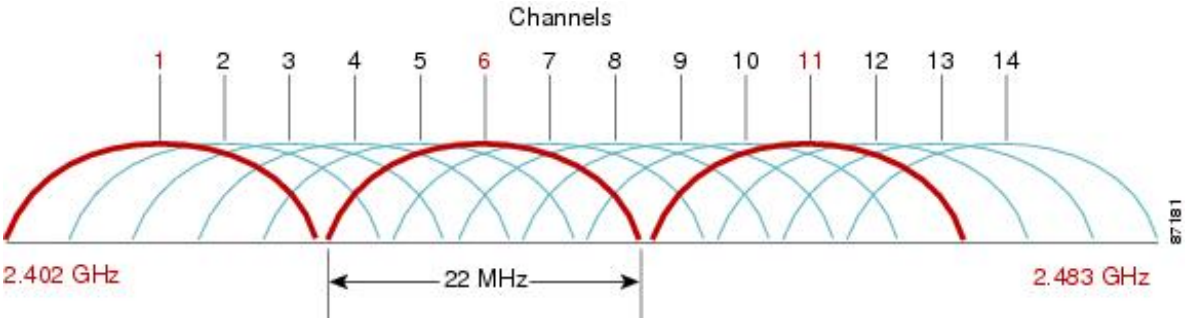


Figure 5 — General diagram of frequency channel closure in the range of 2.4 GHz

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 6.

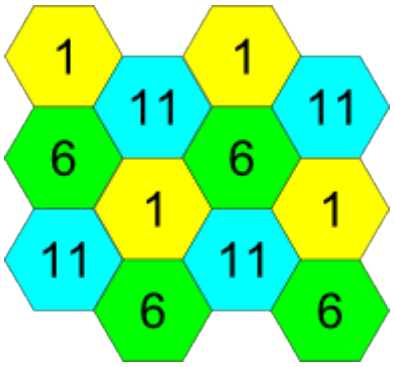


Figure 6 — Scheme of channel allocation among neighboring access points in the frequency range of 2.4 GHz when channel width is 20 MHz

Similarly, the procedure of channel allocation is recommended to save for access point allocation between floors, see Figure 7.

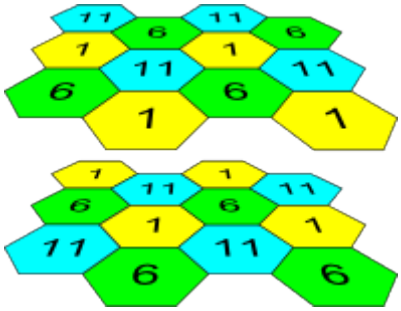


Figure 7 — Scheme of channel allocation between neighboring access points that are located between floors

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.

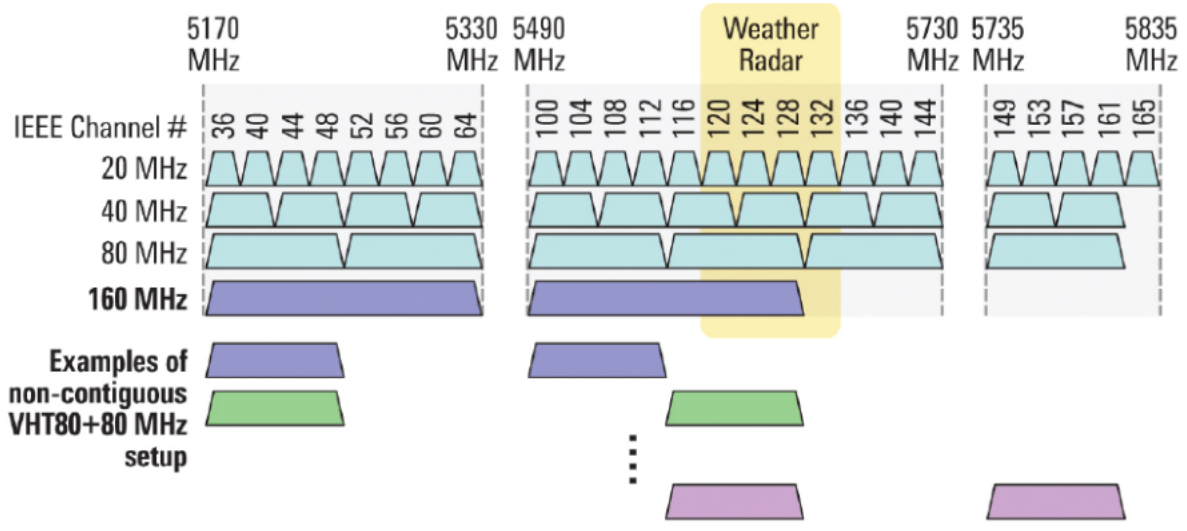


Figure 8 — Channels used in range of 5 GHz when channel width is 20, 40 or 80 MHz

4 Device management via the web interface

4.1 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.

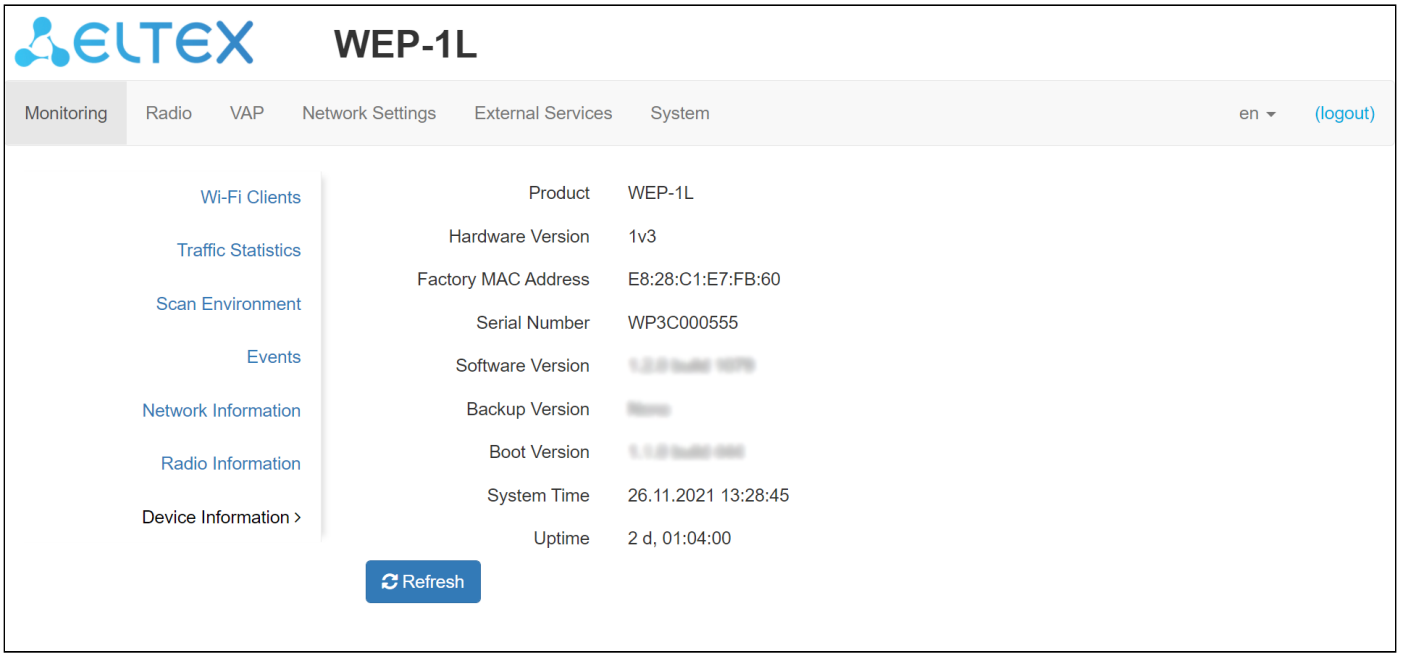
IP address by default: 192.168.1.10, subnet mask: 255.255.255.0. The device is capable to obtain an IP address via DHCP.

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

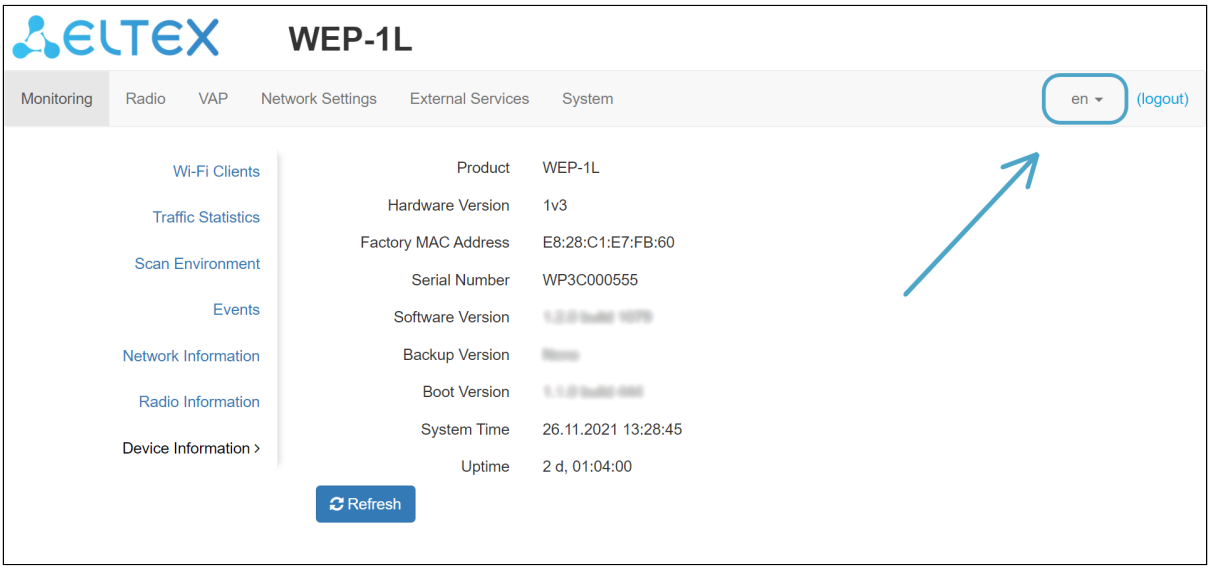
3. Enter your username into “Login” and password into “Password” field.

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.



4.2 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 clicking “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 clicking “Apply” button. If you click “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 clicking “Apply”.

The button for discarding changes appears as follows: Cancel .

4.3 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.

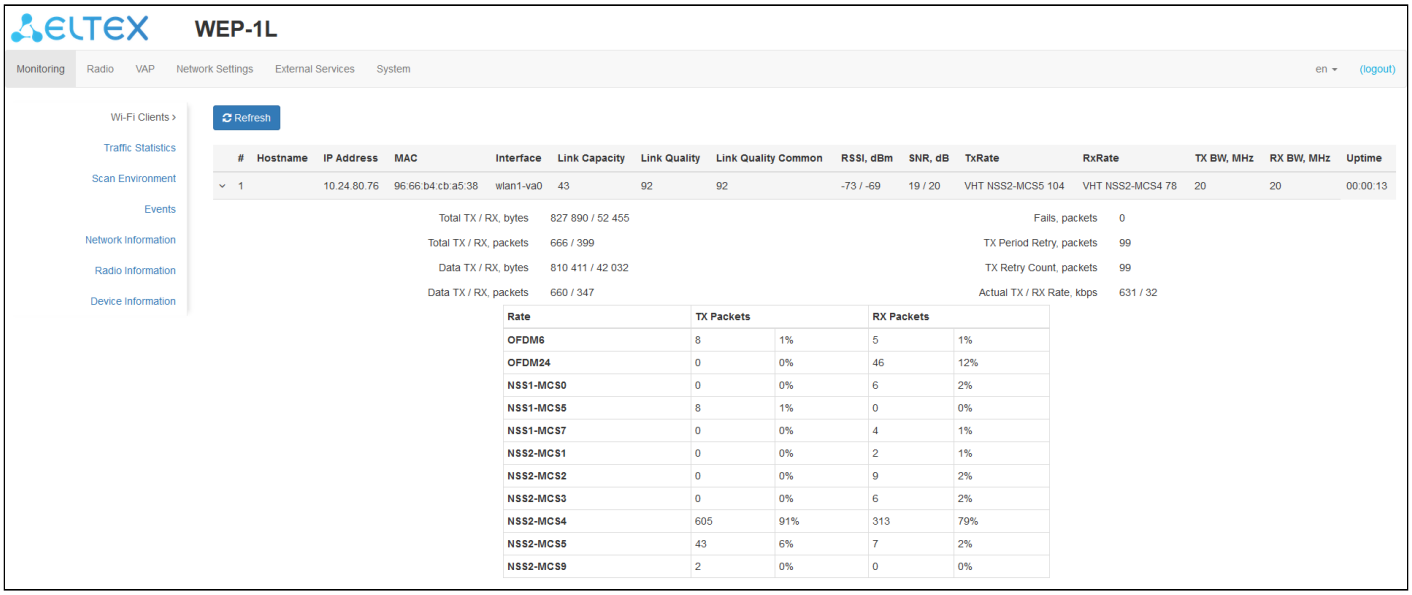
4.4 The “Monitoring” menu

In the “**Monitoring”** menu you can view the current system state.

4.4.1 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-1L 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.

4.4.2 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.

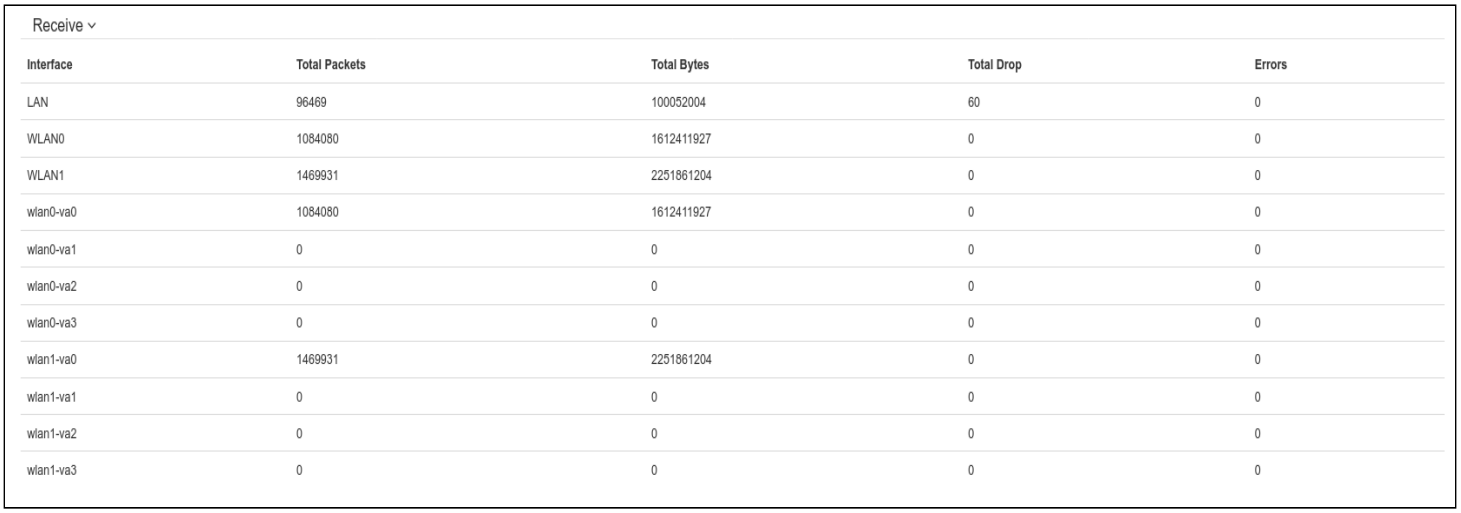
The WLAN0 and WLAN1 Tx/Rx diagrams show the last 3 minutes rate of transmitted/received traffic via Radio 1 and Radio 2 access point interfaces. The diagram is automatically updated every 6 seconds.

Transmit

Interface	Total Packets	Total Bytes	Total Drop	Errors
LAN	2490596	3699981600	0	0
WLAN0	80372	97228761	0	0
WLAN1	781	100913	0	0
wlan0-va0	80372	97228761	371	0
wlan0-va1	0	0	0	0
wlan0-va2	0	0	0	0
wlan0-va3	0	0	0	0
wlan1-va0	781	100913	79	0
wlan1-va1	0	0	154	0
wlan1-va2	0	0	0	0
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

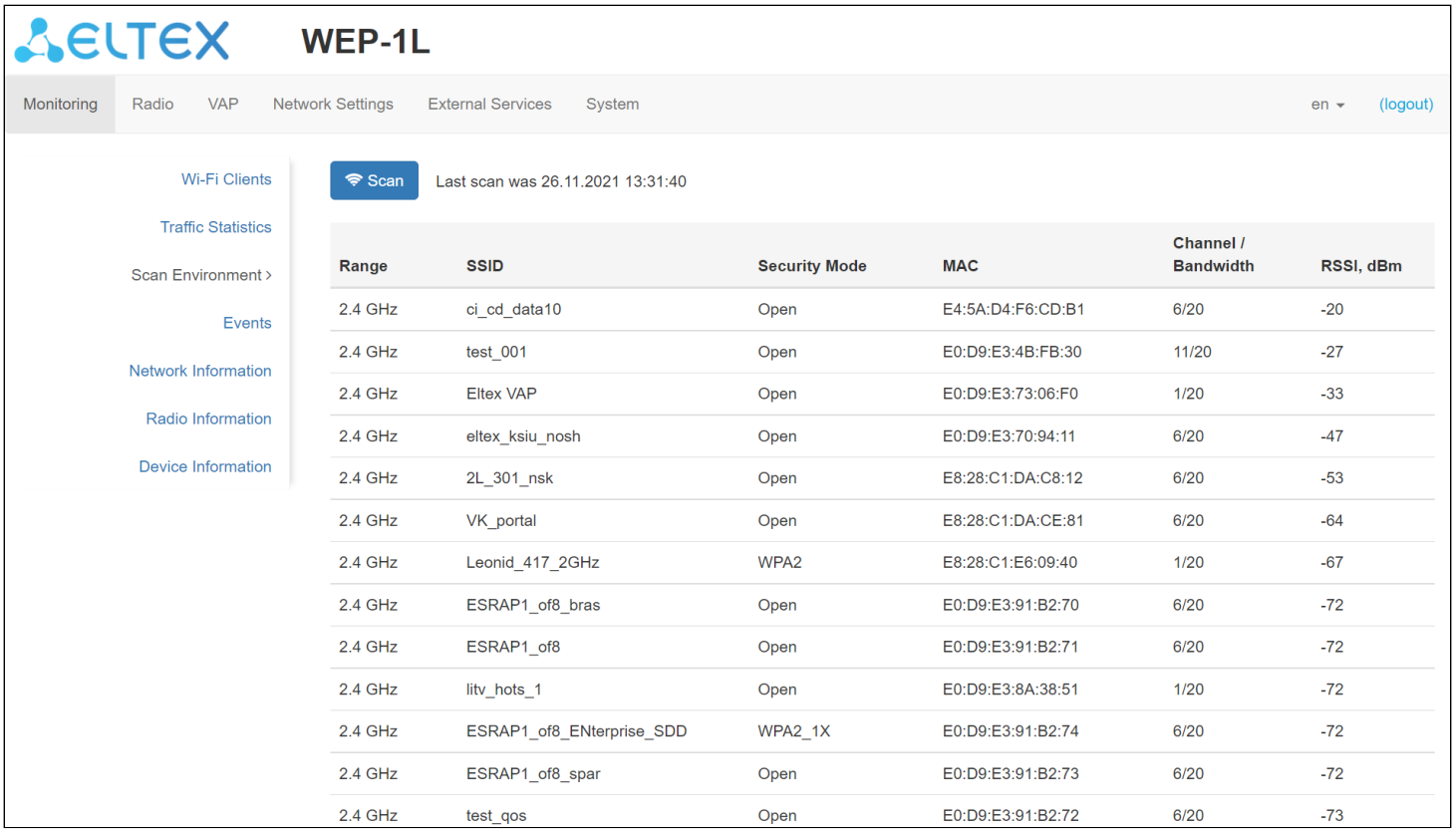
Interface	Total Packets	Total Bytes	Total Drop	Errors
LAN	96469	100052004	60	0
WLAN0	1084080	1612411927	0	0
WLAN1	1469931	2251861204	0	0
wlan0-va0	1084080	1612411927	0	0
wlan0-va1	0	0	0	0
wlan0-va2	0	0	0	0
wlan0-va3	0	0	0	0
wlan1-va0	1469931	2251861204	0	0
wlan1-va1	0	0	0	0
wlan1-va2	0	0	0	0
wlan1-va3	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.

4.4.3 The "Scan Environment" submenu

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



ELTEX WEP-1L

Monitoring | Radio | VAP | Network Settings | External Services | System | en | (logout)

- Wi-Fi Clients
- Traffic Statistics
- Scan Environment
- Events
- Network Information
- Radio Information
- Device Information

Scan — Last scan was 26.11.2021 13:31:40

Range	SSID	Security Mode	MAC	Channel / Bandwidth	RSSI, dBm
2.4 GHz	ci_cd_data10	Open	E4:5A:D4:F6:CD:B1	6/20	-20
2.4 GHz	test_001	Open	E0:D9:E3:4B:FB:30	11/20	-27
2.4 GHz	Eltex VAP	Open	E0:D9:E3:73:06:F0	1/20	-33
2.4 GHz	eltex_ksiu_nosh	Open	E0:D9:E3:70:94:11	6/20	-47
2.4 GHz	2L_301_nsk	Open	E8:28:C1:DA:C8:12	6/20	-53
2.4 GHz	VK_portal	Open	E8:28:C1:DA:CE:81	6/20	-64
2.4 GHz	Leonid_417_2GHz	WPA2	E8:28:C1:E6:09:40	1/20	-67
2.4 GHz	ESRAP1_of8_bras	Open	E0:D9:E3:91:B2:70	6/20	-72
2.4 GHz	ESRAP1_of8	Open	E0:D9:E3:91:B2:71	6/20	-72
2.4 GHz	litv_hots_1	Open	E0:D9:E3:8A:38:51	1/20	-72
2.4 GHz	ESRAP1_of8_ENterprise_SDD	WPA2_1X	E0:D9:E3:91:B2:74	6/20	-72
2.4 GHz	ESRAP1_of8_spar	Open	E0:D9:E3:91:B2:73	6/20	-72
2.4 GHz	test_qos	Open	E0:D9:E3:91:B2:72	6/20	-73

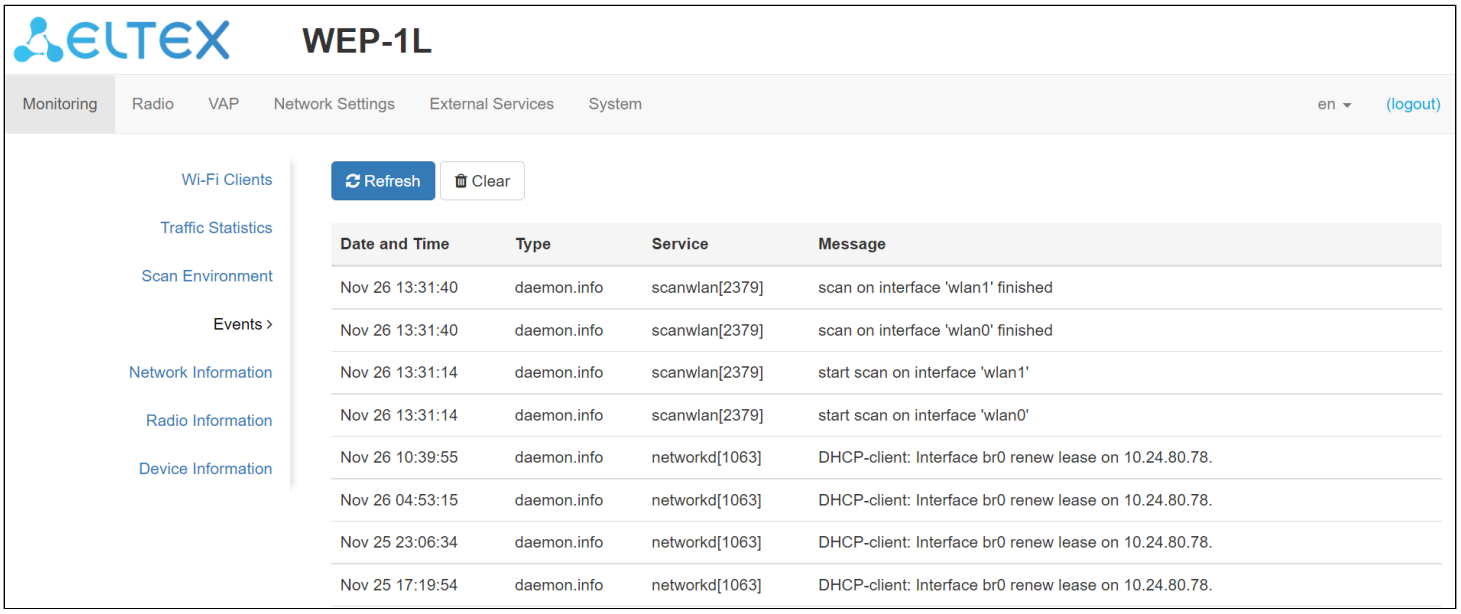
After clicking on the "Scan" button, the process will be launched. After the scan is completed, a list of detected access points and information about them will appear:

- *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 mode* — 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.

4.4.4 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	Description
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.

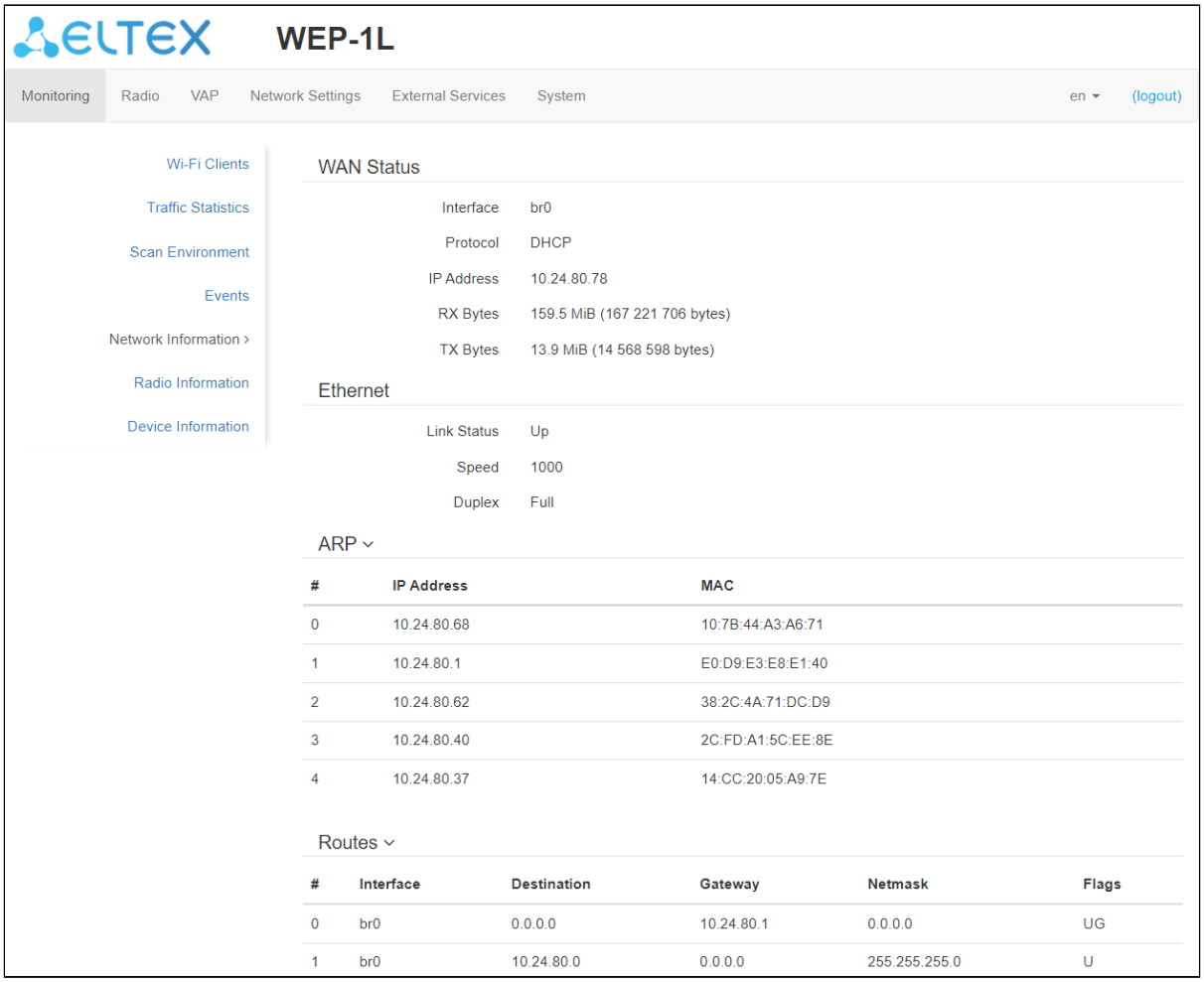
Level	Message importance level	Description
4	Warning	Warning, non-emergency message.
5	Notice	System notice, non-emergency message.
6	Informational	Informational system messages.
7	Debug	Debugging messages provide the user with information to correctly configure the system.

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.

4.4.5 The “Network Information” submenu

In the “**Network Information**” submenu you can view common network settings of the device.



WAN Status

- *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;

Ethernet

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

ARP

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

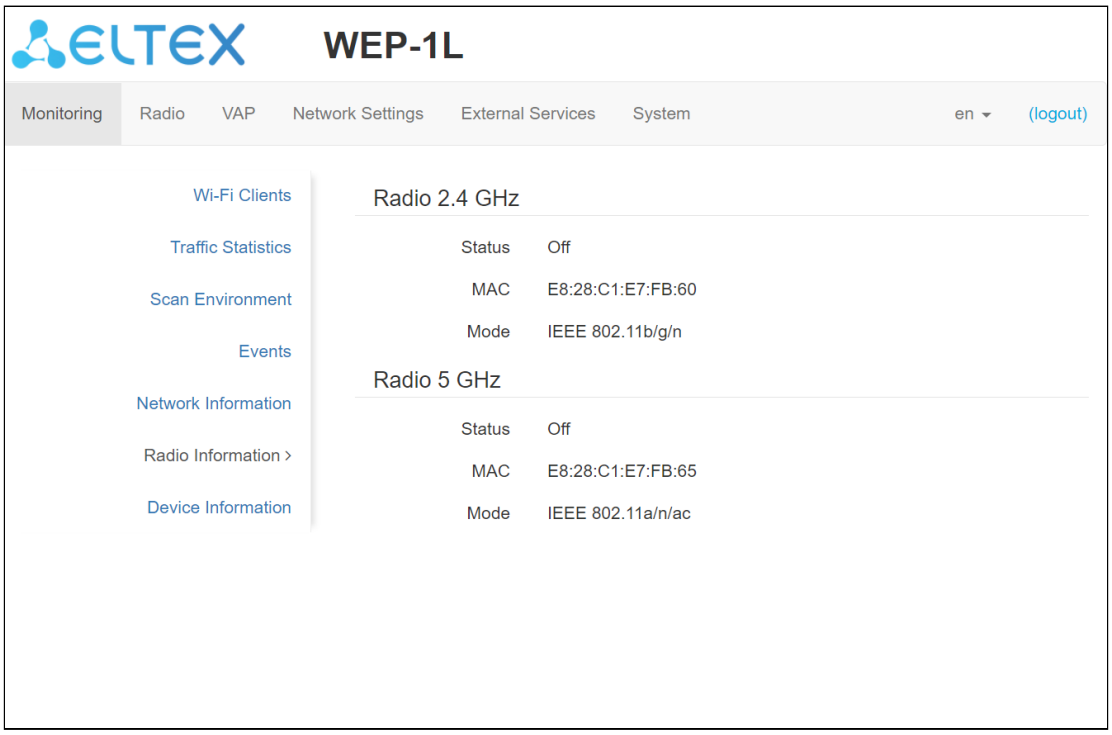
- *IP address* — device IP address;
- *MAC* — device MAC address.

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.

4.4.6 The “Radio Information” submenu

In the **“Radio Information”** submenu the current status of WEP-1L 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:

“Off”

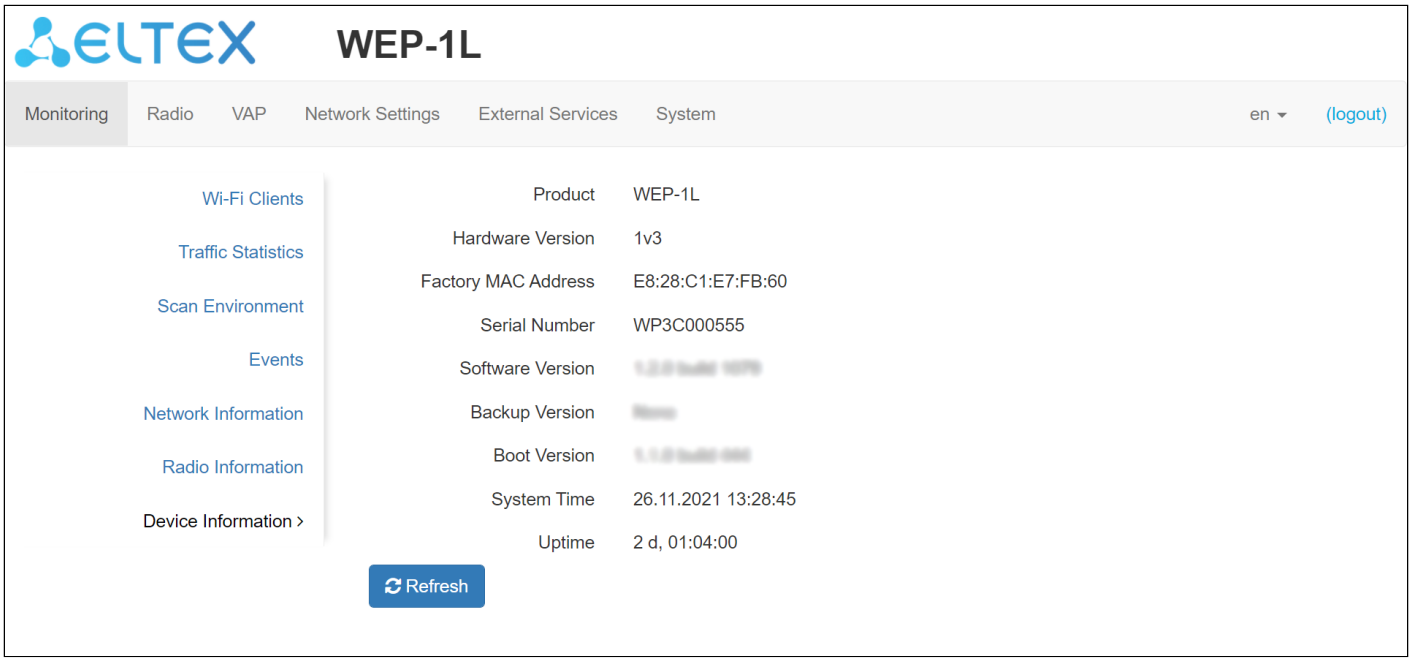
- *Status* — radio interface state;
- *MAC* — radio interface MAC address;
- *Mode* — radio interface operation mode according to IEEE 802.11 standards.

“On”

- *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.

4.4.7 The “Device Information” submenu

The “**Device Information”** submenu displays main WEP-1L parameters.



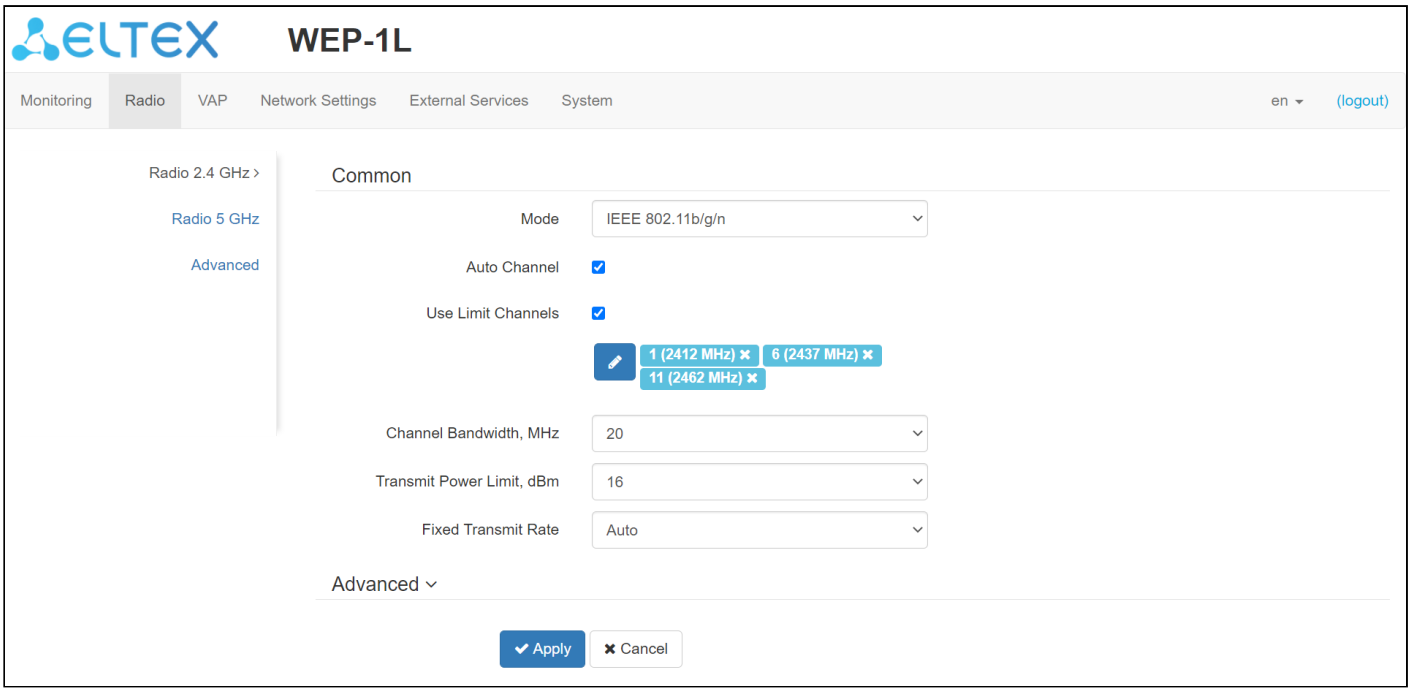
- *Product* — device model name;
- *Hardware Version* — device hardware version;
- *Factory MAC Address* — device WAN interface MAC address, setted by manufacturer;
- *Serial Number* — device serial number, setted by manufacturer;
- *Firmware Version* — device firmware version;
- *Backup Version* — previously 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.

4.5 The “Radio” menu

In the “**Radio**” menu you can configure the wireless interface.

4.5.1 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 2.4 GHz 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.

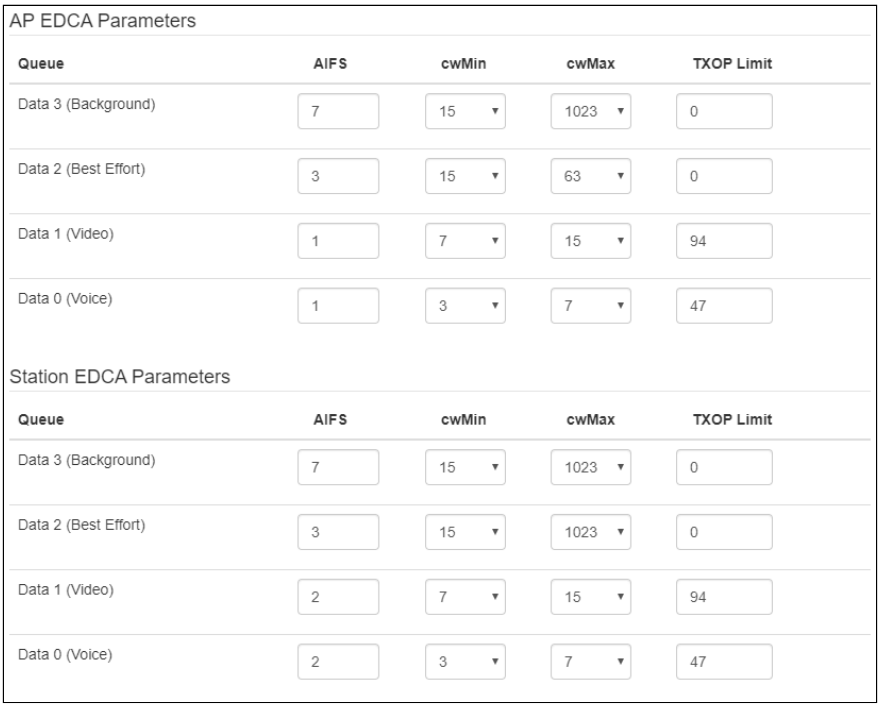
If you change the “Channel Bandwidth” parameter to 40 MHz and do not remove the “grey” channels from the list, then when you click on the “Apply” button in the browser an error will appear — “There are errors in data. Changes was not applied”. Accordingly, the access point configuration will not be changed. 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:

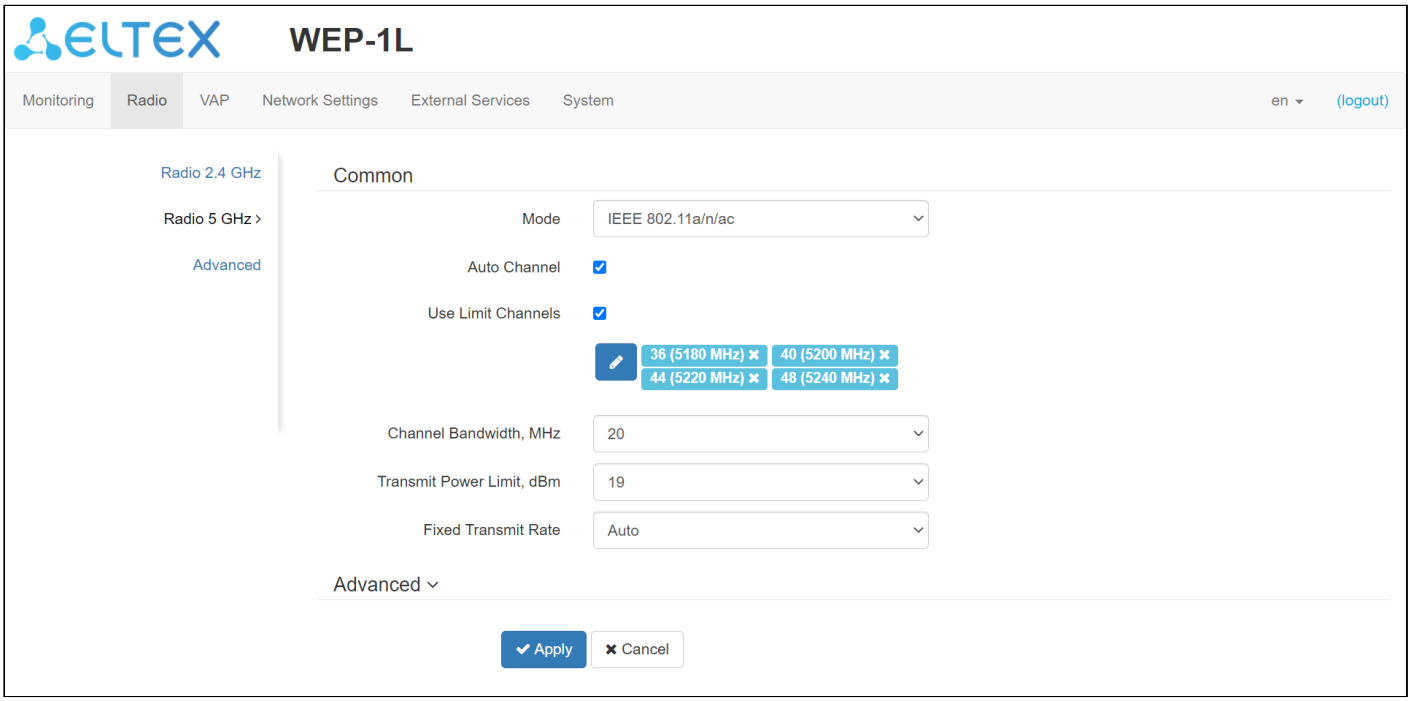


- *AP EDCA parameters* — access point settings table (traffic is transmitted from the access point to the client):
  - *Queue* — predefined queues for various kinds of traffic:
    - *Data 3 (Background)* — low priority queue, high bandwidth (802.1p: cs1, cs2 priorities);
    - *Data 2 (Best Effort)* — 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, click “Apply”. click “Cancel” to discard the changes.

4.5.2 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.



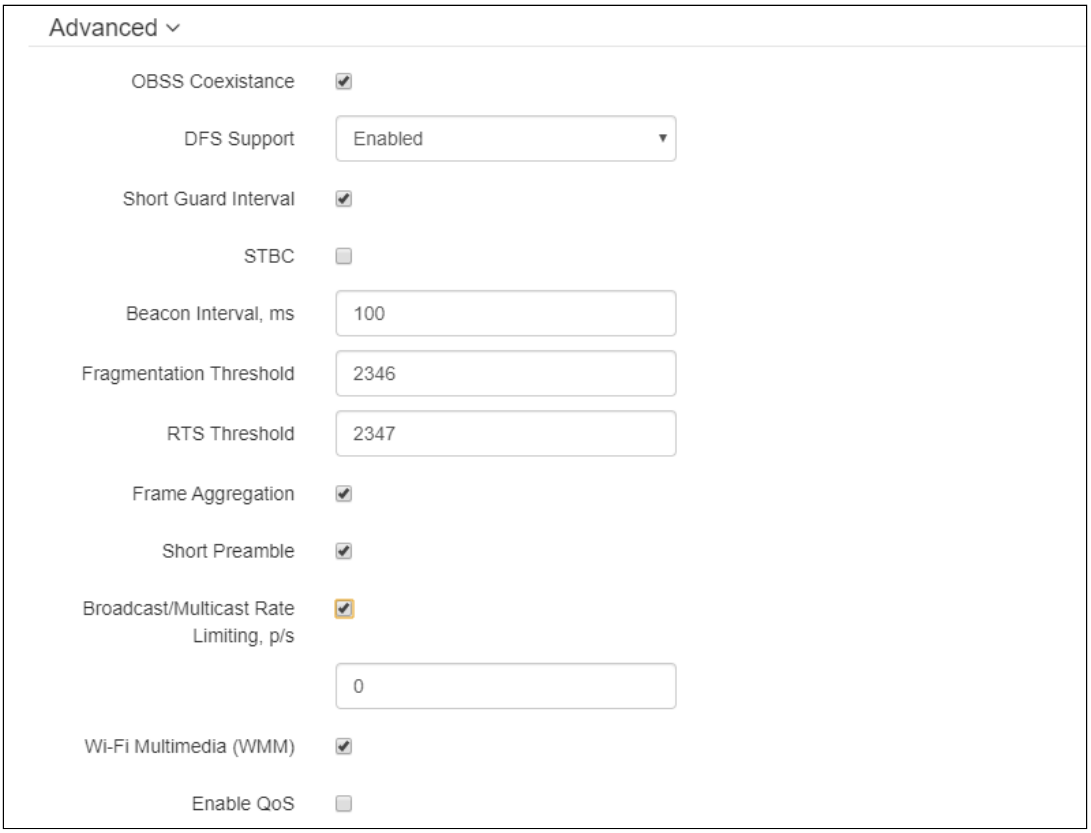
- *Mode* — select interface operation mode:
  - IEEE 802.11a
  - IEEE 802.11a/n
  - IEEE 802.11a/n/ac
- *Auto Channel* — when checked, the device will automatically select the least loaded radio channel for the Wi-Fi interface. Removing the flag opens the access to install the static operation channel.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

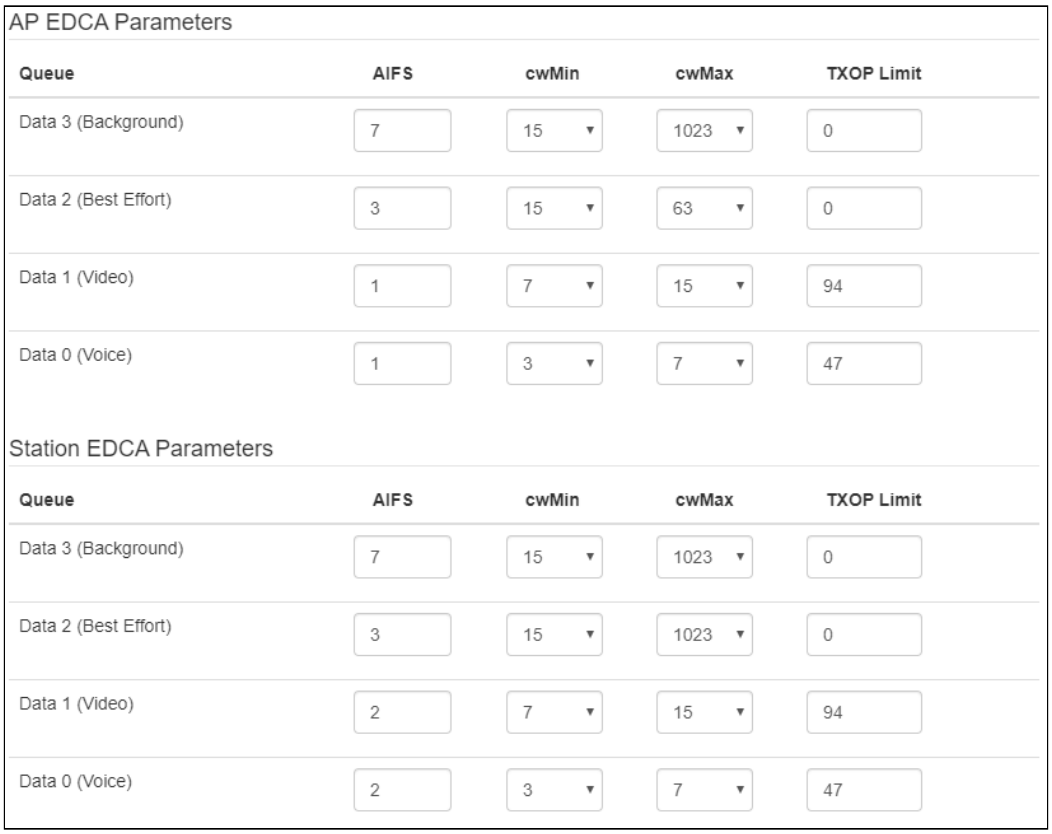


- *OBSS Coexistence* — automatic channel bandwidth reduction when the air is loaded. When the flag is set, the mode is enabled;
- *DFS Support* — dynamic frequency selection mechanism. The mechanism demands wireless devices to scan environment and avoid using channels which coincide with radiolocation 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* — 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).

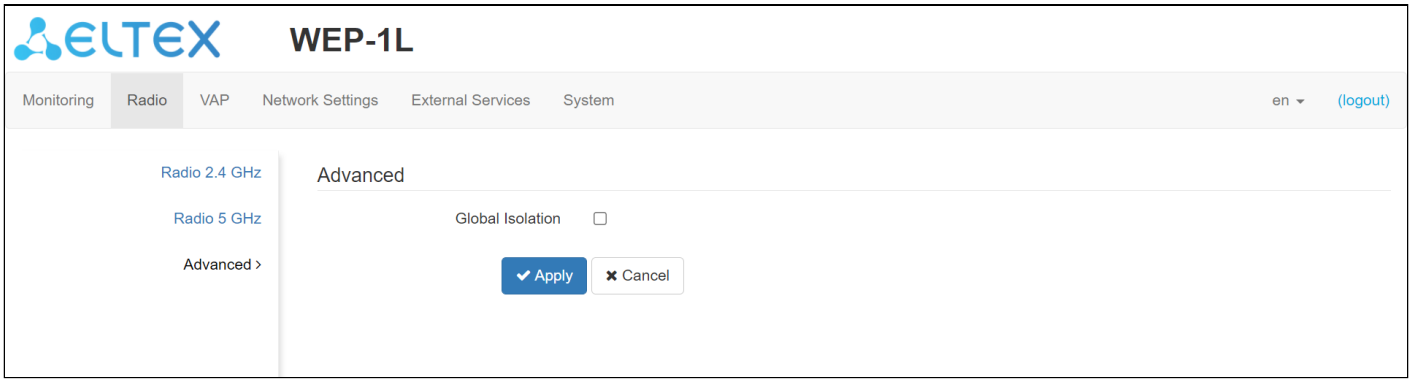
- *AIFS* — Arbitration Inter-Frame Spacing, defines the waiting time of data frames, measured in slots, takes values (1-255);
- *cwMin* — the initial timeout value before resending a frame, specified in milliseconds, takes the values 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023. The value of cwMin cannot 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, click “Apply”. click “Cancel” to discard the changes.

4.5.3 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.

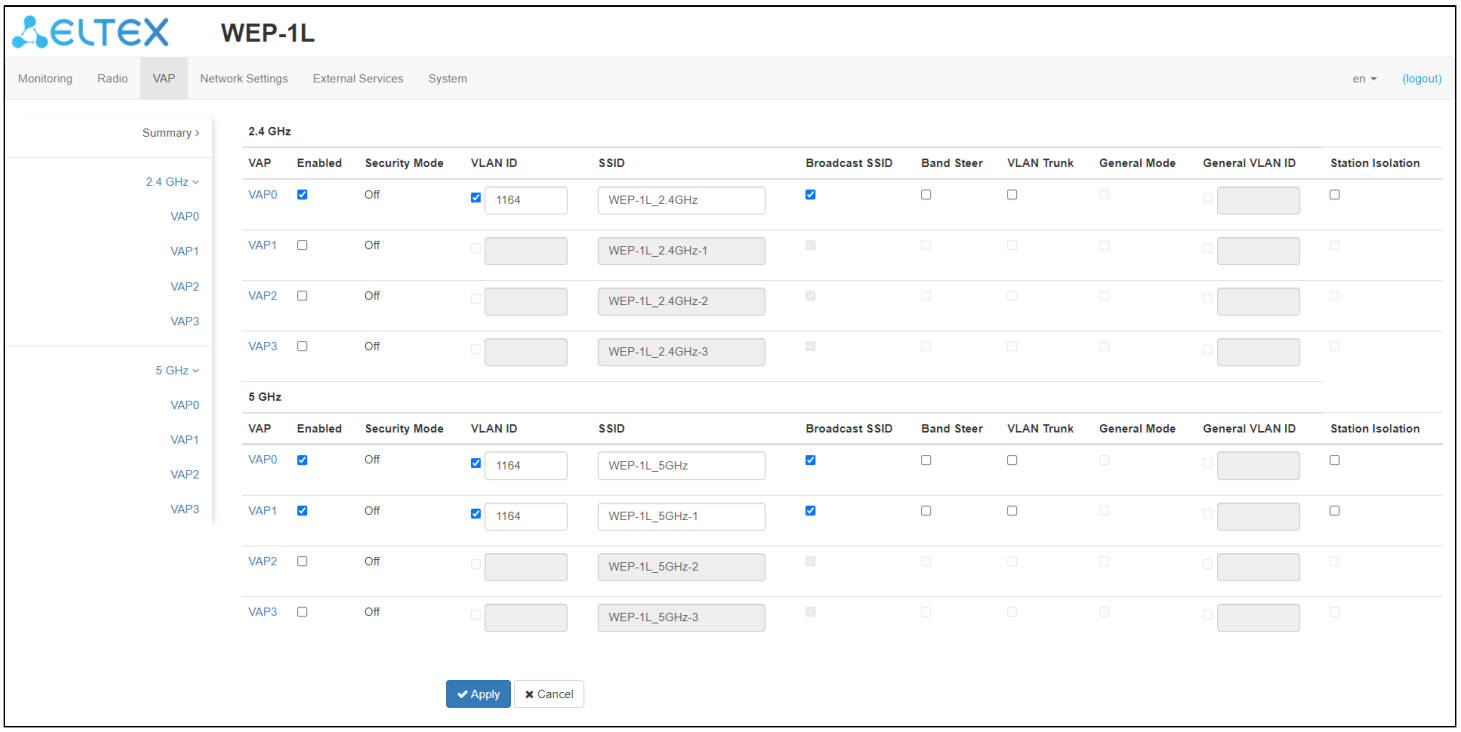
To apply a new configuration and save setting to non-volatile memory, click “Apply”. click “Cancel” to discard the changes.

4.6 The “VAP” menu

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

4.6.1 The “Summary” submenu

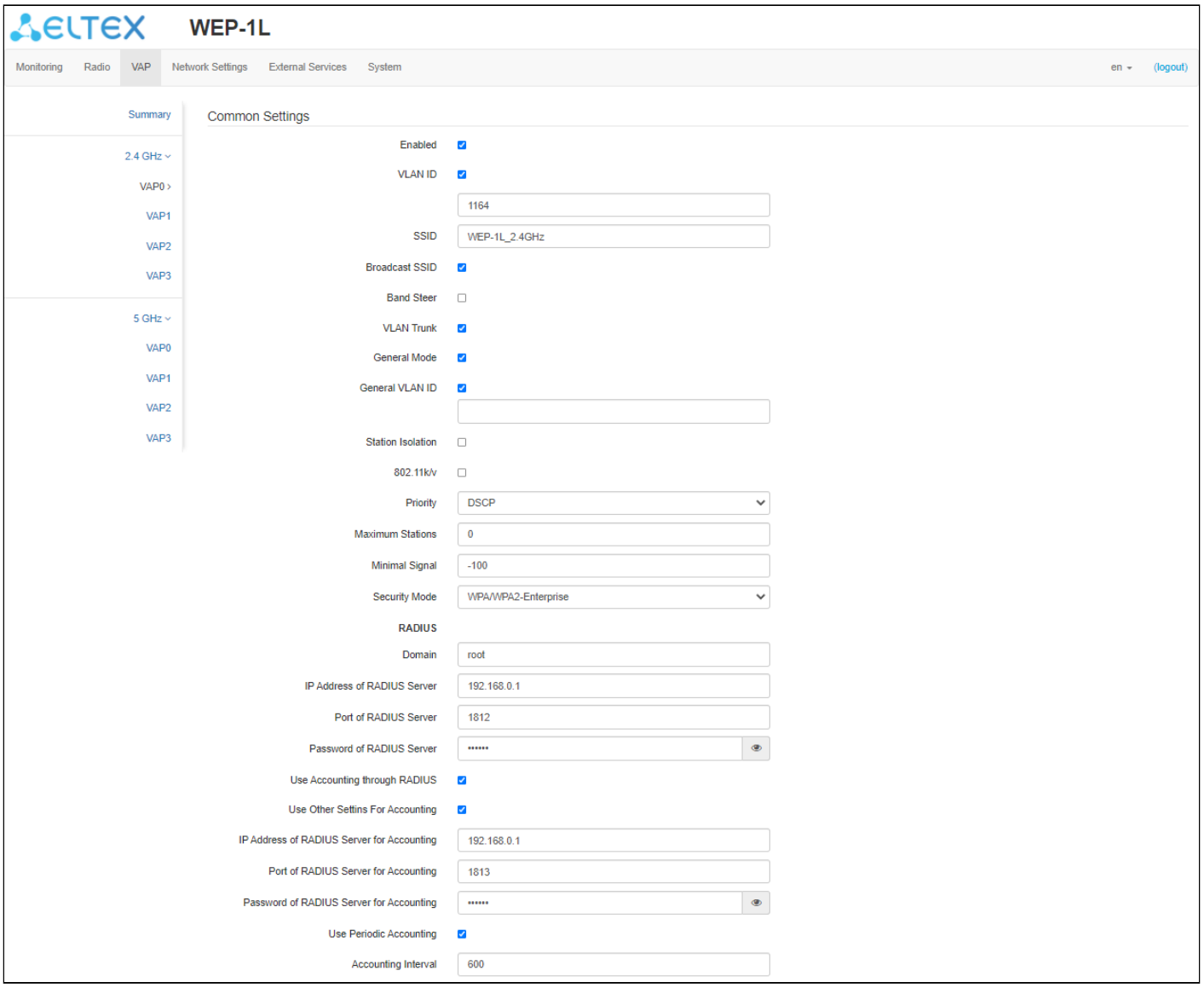
The “**Summary**” submenu displays the settings of all VAPs on Radio 2.4 GHz and Radio 5 GHz radio interfaces. You can see the settings of each virtual access point in sections VAP0..3.



- *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;
- *Band Steer mode* — when the flag is set, client priority connection to 5 GHz network is active. For capability operation, VAP with same SSID on each radio interface should be created and “Band Steer mode” should be activated on them;
- *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, click “Apply”. click “Cancel” to discard the changes.

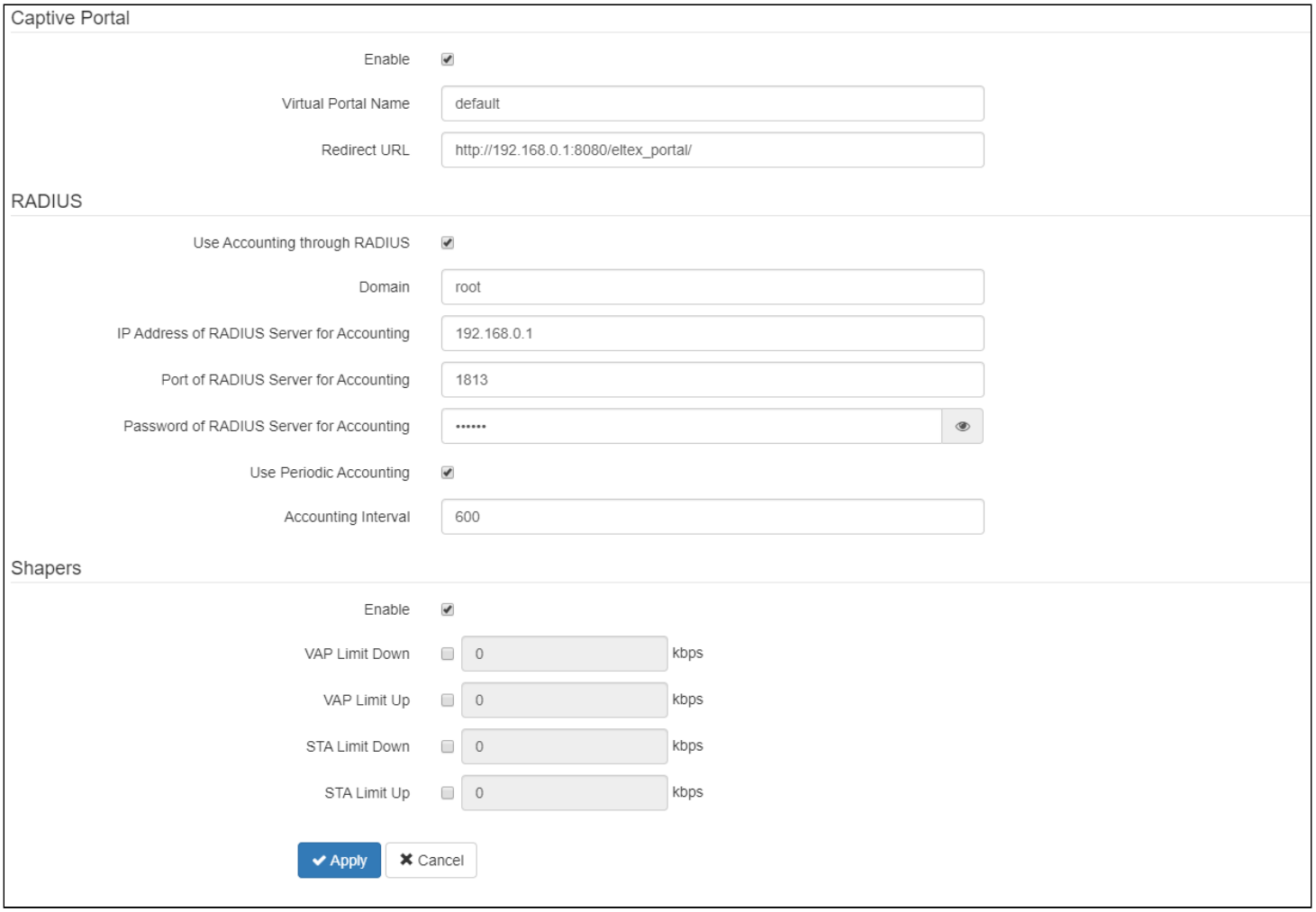
4.6.2 The “VAP” submenu



Common settings

- *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;
- *Band Steer mode* — when the flag is set, client priority connection to 5 GHz network is active. For capability operation, VAP with same SSID on each radio interface should be created and “Band Steer mode” should be activated on them;
- *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.
- *802.11k/v support* — enable support for 802.11k/v standarts on virtual access point;

- *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.

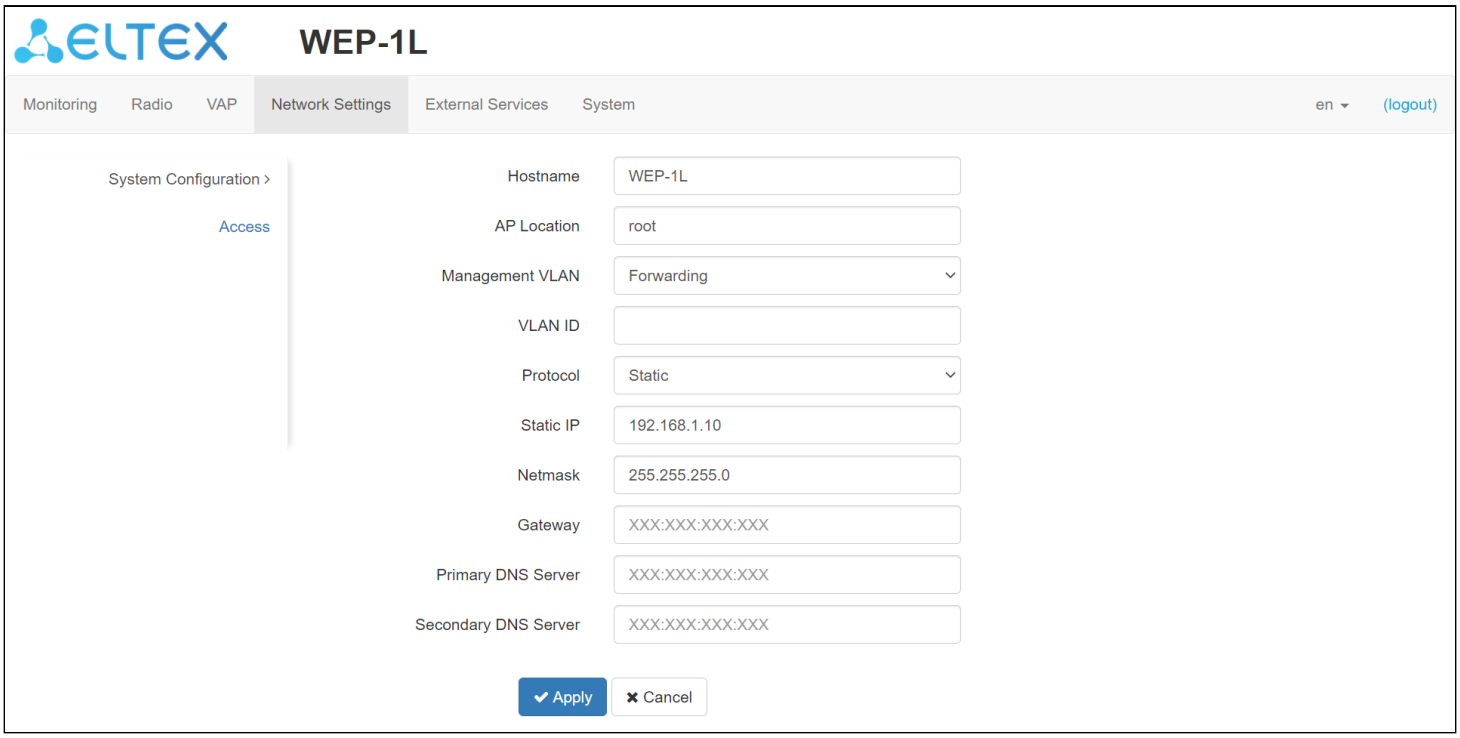
Shapers

- *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, click “Apply”. click “Cancel” to discard the changes.

4.7 The “Network Settings” menu

4.7.1 The “System Configuration” submenu



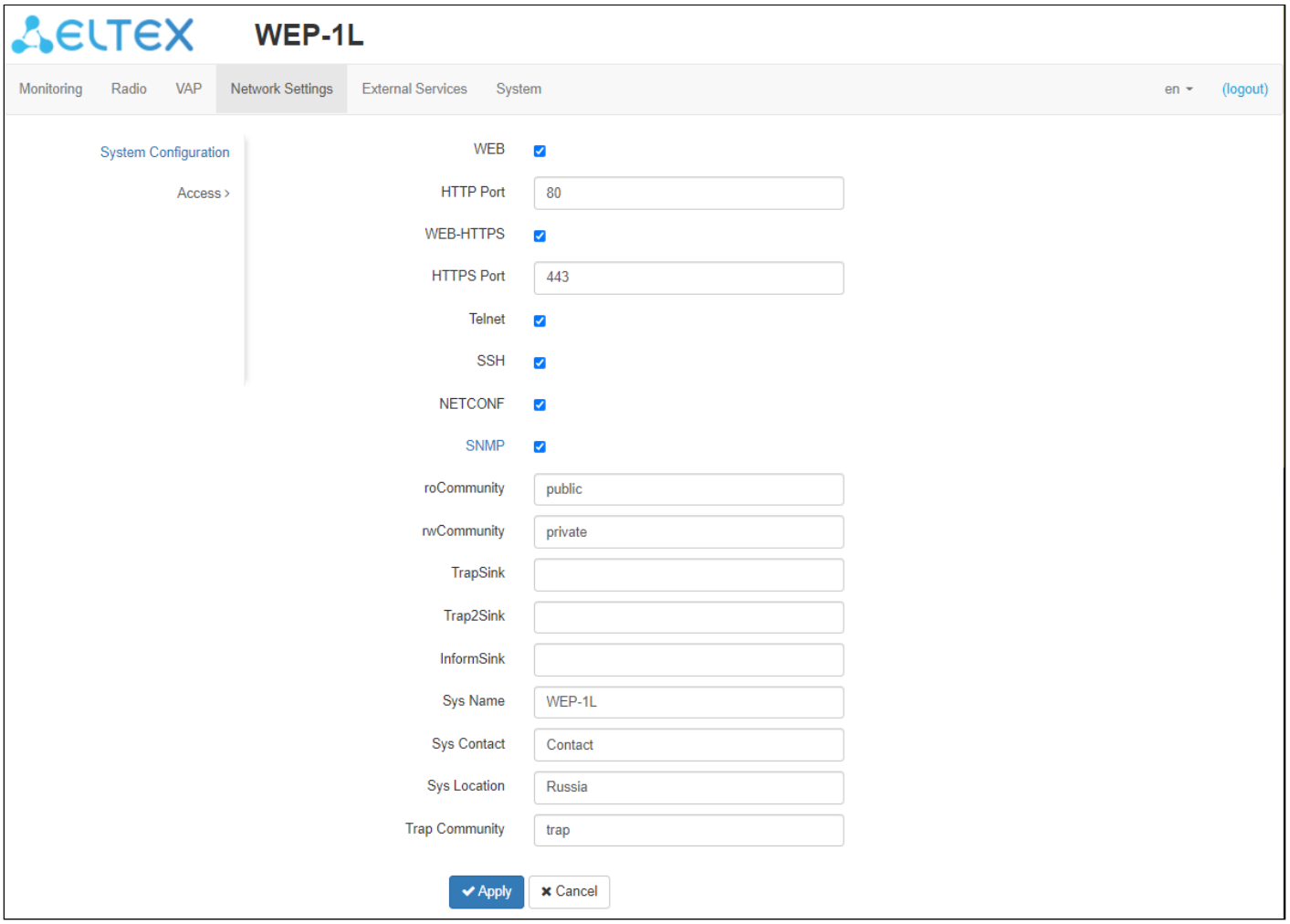
- *Hostname* — nertwork name of the device, specified by string from 1 to 63 characters; latin uppercase and lowercase letters, numbers, hyphen “-” (hyphen can not be the last character in the name);
- *AP Location* — domain of the EMS management system tree host where the access point is located;
- *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, click “Apply”. click “Cancel” to discard the changes.

4.7.2 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.

- To enable access to the device via Telnet, check the box next to “Telnet”;
- To enable access to the device via SSH, check the box next to “SSH”;
- To enable access to the device via NETCONF, check the box next to “NETCONF”;

WEP-1L 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:

- eltex.Ltd.1.127.1 — monitoring access point parameters and connected client devices;
- eltex.Ltd.1.127.3 — access point management (reboot).

where eltexLtd — 1.3.6.1.4.1.35265 is Eltex Enterprise ID.

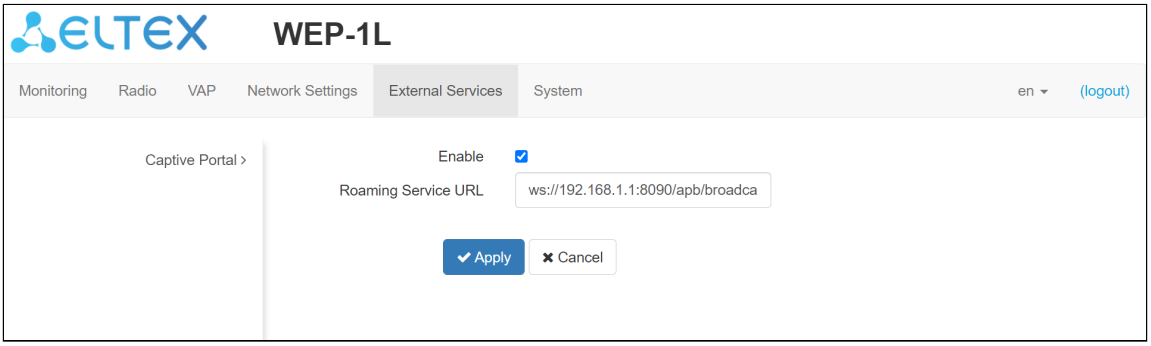
To apply a new configuration and save setting to non-volatile memory, click “Apply”. click “Cancel” to discard the changes.

4.8 The “External Services” menu

4.8.1 The “Captive Portal” submenu

The “Captive Portal” submenu is intended for enabling and configuring APB service on the access point.

APB service is used for providing captive portal roaming between access points connected to the service.



- *Enable* — when the flag is set, access point will connect to the APB service, address of which is specified in the “Roaming Service URL” field, so as to prodive clients' captive roaming;
- *Roaming Service URL* — Roaming Service URL for roaming support in captive portal mode. Specified in format: “ws://<host>:<port>/apb/broadcast”.

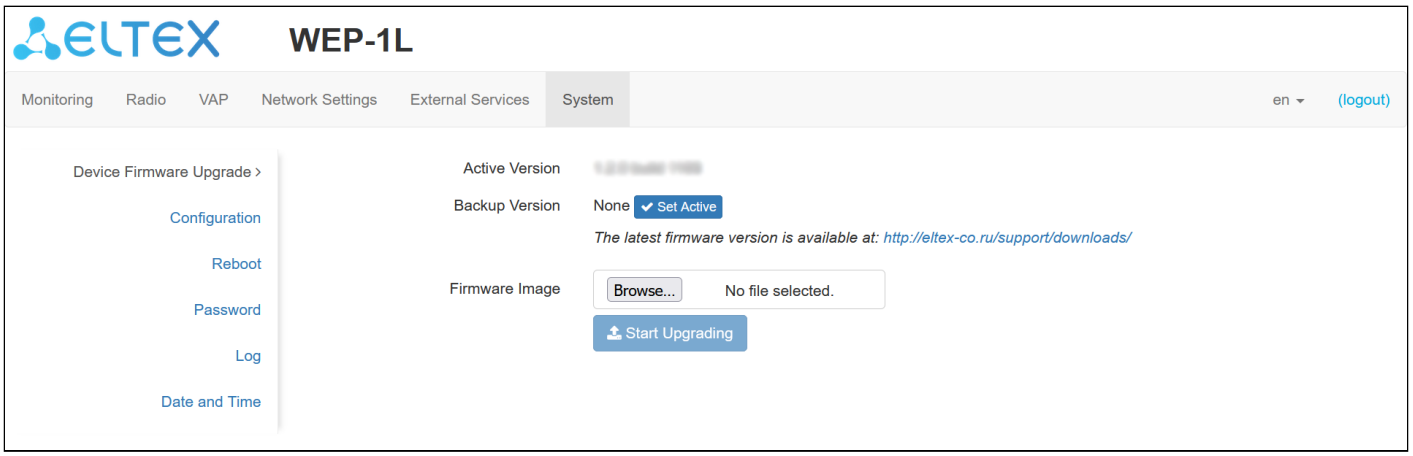
To apply a new configuration and save setting to non-volatile memory, click “Apply”. click “Cancel” to discard the changes.

4.9 The “System” menu

In the “**System**” menu you can configure system, time, device access via different protocols, change password and update device firmware.

4.9.1 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.

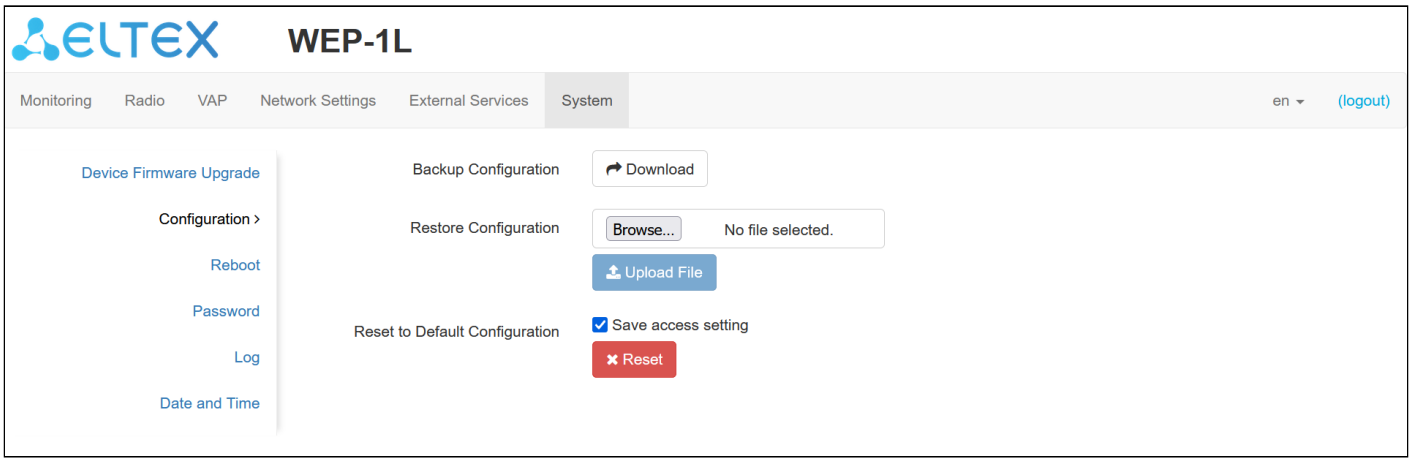
Firmware update

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 upgrade.

4.9.2 The "Configuration" submenu

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



Backup Configuration

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

Restore Configuration

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" click. Uploaded configuration will be applied automatically and does not require device reboot.

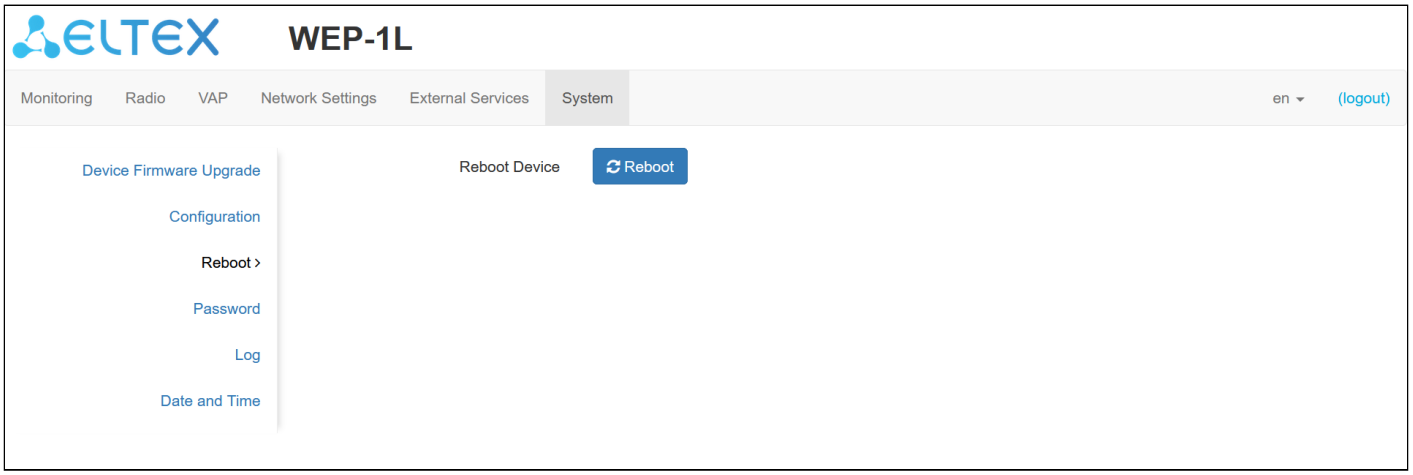
To change the passwords open the configuration file in text editor and change passwords. Then save the changes in configuration archive. The example of password changing is shown below:

Reset to Default Configuration

To reset all the settings to default values, click "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.

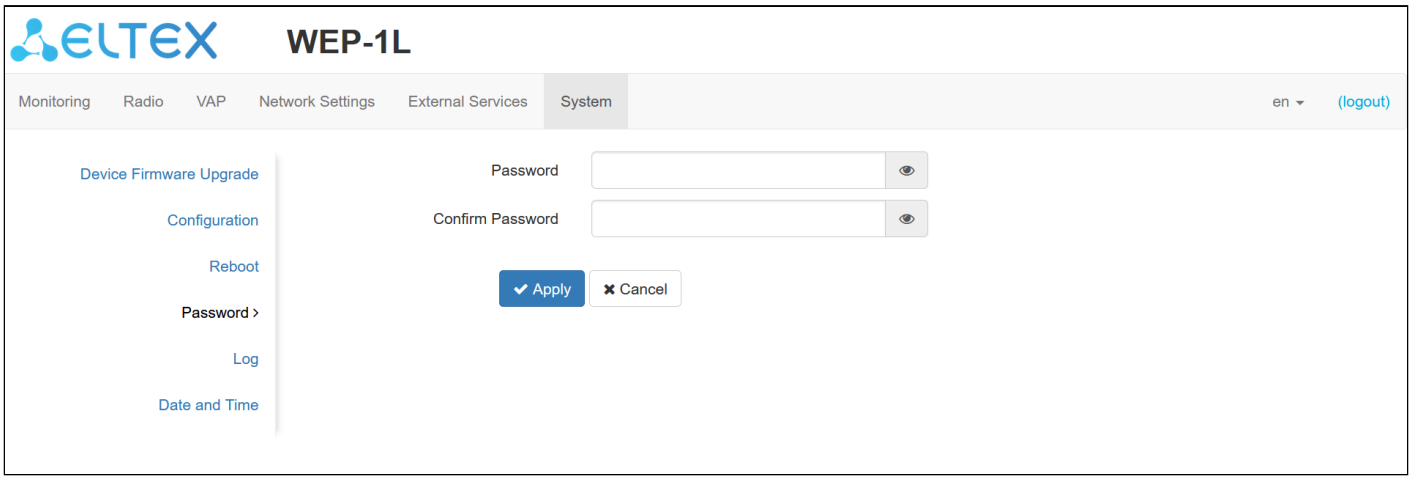
4.9.3 The “Reboot” submenu

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



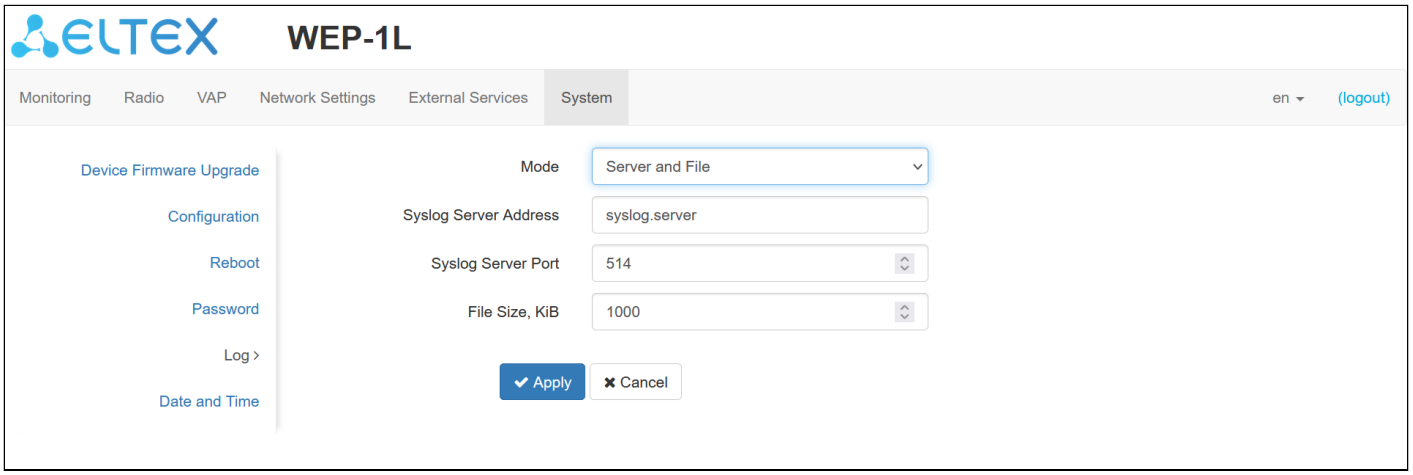
4.9.4 The “Password” submenu

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.



4.9.5 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.

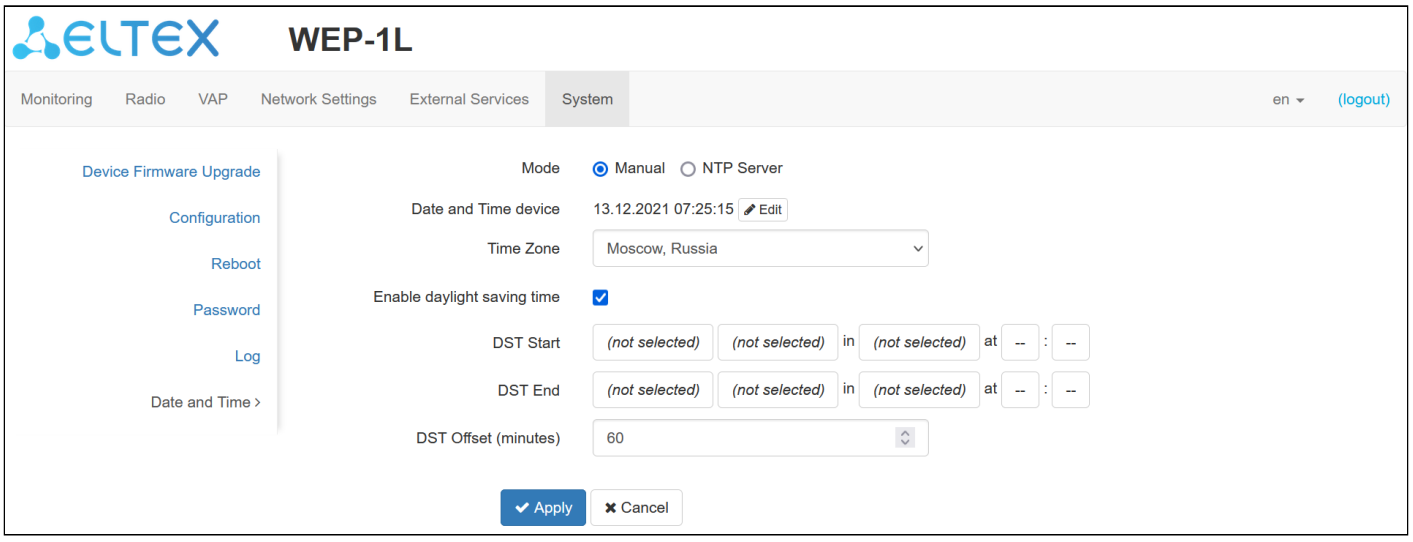


- *Mode* — Syslog agent operation mode:
  - *Local File* — log information is stored in a local file and is available in the device’s web interface on the “Monitoring/Events” tab;
  - *Server and File* — log information is sent to a remote Syslog server and stored in a local file.
- *Syslog Server Address* — 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).

To apply a new configuration and save settings into the non-volatile memory, click the *“Apply”* button. To discard changes click the *“Cancel”* button.

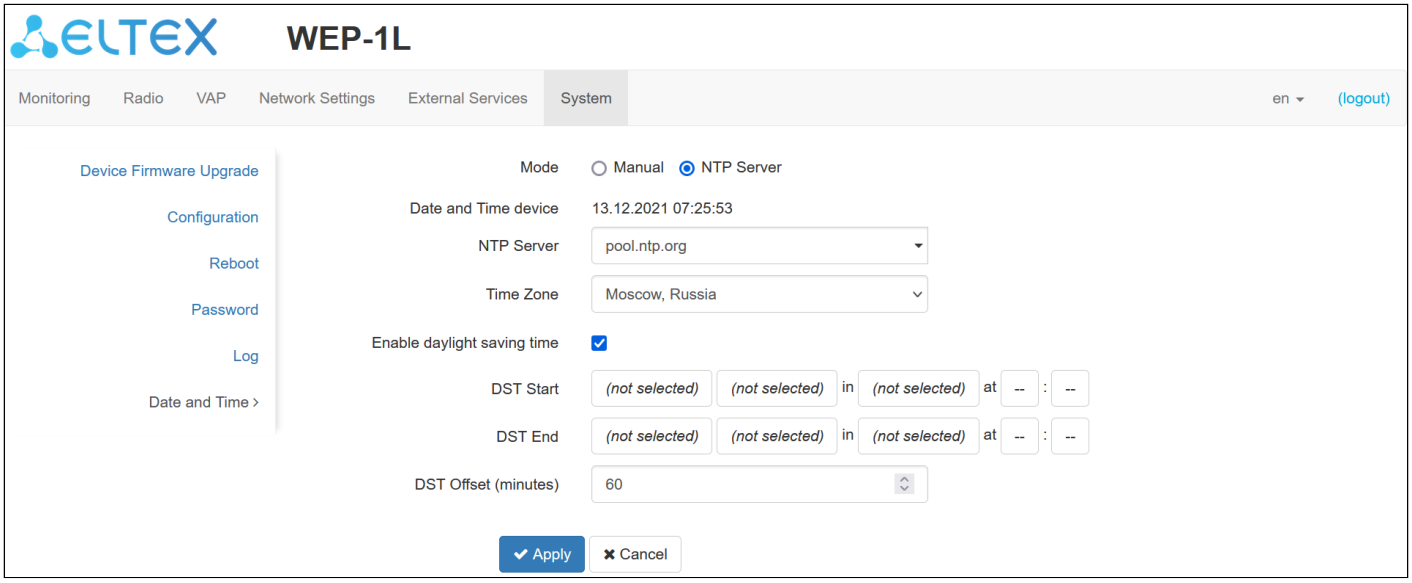
4.9.6 The “Date and Time” submenu

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;
- Enable daylight saving time — when the flag is set, daylight saving time will activate in specified time period:
  - DST Start — date and time when daylight saving time starts;
  - DST End — date and time when daylight saving time ends;
  - DST Offset — time period in minutes for which the time shift is performed.

To apply a new configuration and save settings into the non-volatile memory, click the *“Apply”* button. To discard changes click the *“Cancel”* button.

5 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.

5.1 Connection to the device

By default, WEP-1L 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-1L 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

5.2 Network parameters configuration

Configuration of access point static network parameters

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

Static routing

WEP-1L(config):/interface/br0/common# **exit**
WEP-1L(config):/interface/br0# **exit**
WEP-1L(config):/interface# **exit**
WEP-1L(config):/# **route**
WEP-1L(config):/route# **add default** (where default — route name)
WEP-1L(config):/route# **default**
WEP-1L(config):/route/default# destination X.X.X.X (where X.X.X.X — IP address of the network ordestination node, for default route — 0.0.0.0)
WEP-1L(config):/route/default# netmask X.X.X.X (where X.X.X.X — destination network mask, for default route — 0.0.0.0)
WEP-1L(config):/route/default# gateway X.X.X.X (where X.X.X.X — gateway IP address)
WEP-1L(config):/route/default# save (Save changes)

Configuration of reception of the network parameters via DHCP

WEP-1L(root):/# **configure**
WEP-1L(config):/# **interface**
WEP-1L(config):/interface# **br0**
WEP-1L(config):/interface/br0# **common**
WEP-1L(config):/interface/br0/common# **protocol dhcp**
WEP-1L(config):/interface/br0/common# **save** (Save changes)

5.2.1 Network parameters configuration via set-management-vlan-mode utility

Untagged access

Reception of the network parameters via DHCP:

WEP-1L(root):/# **set-management-vlan-mode off protocol dhcp**

Static settings:

WEP-1L(root):/# **set-management-vlan-mode off protocol static-ip ip-addr X.X.X.X netmask Y.Y.Y.Y gateway Z.Z.Z.Z** (where X.X.X.X — static IP address, Y.Y.Y.Y — subnet mask, Z.Z.Z.Z — gateway)

Access via Management VLAN in Terminating mode

Reception of the network parameters via DHCP:

WEP-1L(root):/# **set-management-vlan-mode terminating vlan-id X protocol dhcp** (where X — VLAN ID used for access to the device. Possible values: 1-4094)

Static settings:

WEP-1L(root):/# **set-management-vlan-mode terminating vlan-id X protocol static-ip ip-addr X.X.X.X netmask Y.Y.Y.Y gateway Z.Z.Z.Z** (where X — VLAN ID used for access to the device. Possible values: 1-4094; X.X.X.X — static IP address, Y.Y.Y.Y — subnet mask, Z.Z.Z.Z — gateway)

Access via Management VLAN in Forwarding mode

Reception of the network parameters via DHCP:

WEP-1L(root):/# **set-management-vlan-mode forwarding vlan-id X protocol dhcp** (where X — VLAN ID used for access to the device. Possible values:: 1-4094)

Static settings:

WEP-1L(root):/# **set-management-vlan-mode forwarding vlan-id X protocol static-ip ip-addr X.X.X.X netmask Y.Y.Y.Y gateway Z.Z.Z.Z** (where X — VLAN ID used for access to the device. Possible values: 1-4094; X.X.X.X — static IP address, Y.Y.Y.Y — subnet mask, Z.Z.Z.Z — gateway)

Completion and changes save

WEP-1L(root):/# **save** (Save changes)

5.2.2 IPv6 network parameters configuration

Access to the device via IPv6 protocol is disabled by default.
Access to the device via IPv6 protocol is possible to configure only if VLAN management is not used on the access point.

Enabling access to the device via IPv6 protocol

WEP-1L(root):/# **configure**
WEP-1L(config):/# **interface**
WEP-1L(config):/interface# **br0**
WEP-1L(config):/interface/br0# **common**
WEP-1L(config):/interface/br0/common# **ipv6**
WEP-1L(config):/interface/br0/common/ipv6# **protocol dhcp** (Reception of the IPv6 network parameters via DHCP)
WEP-1L(config):/interface/br0/common/ipv6# **enabled true** (Enabling access to the device via IPv6 protocol. To disable, enter **false**)
WEP-1L(config):/interface/br0/common/ipv6# **save** (Save changes)

Configuring static IPv6 network settings for the access point

WEP-1L(root):/# **configure**
WEP-1L(config):/# **interface**
WEP-1L(config):/interface# **br0**
WEP-1L(config):/interface/br0# **common**
WEP-1L(config):/interface/br0/common# **ipv6**
WEP-1L(config):/interface/br0/common/ipv6# **address**
XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX (where XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX — static IPv6 address of the WEP-1L device)
WEP-1L(config):/interface/br0/common/ipv6# **address-prefix-length X** (where X — static IPv6 address prefix. Takes values from 0 to 128. By default — 64)
WEP-1L(config):/interface/br0/common/ipv6# **gateway XXXX:XXXX:XXXX:XXXX::/64** (IPv6 prefix is specified, for example 3211:0:0:1234::/64)
WEP-1L(config):/interface/br0/common/ipv6# **dns-server-1**
XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX/Y (where XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX/Y — IPv6 address of the dns server №1 with prefix)
WEP-1L(config):/interface/br0/common/ipv6# **dns-server-2**
XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX/Y (where XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX/Y — IPv6 address of the dns server №2 with prefix)
WEP-1L(config):/interface/br0/common/ipv6# **protocol static-ip** (Enabling use of static IPv6 networks parameters. For reception of IPv6 the network parameters via DHCP enter **dhcp**)
WEP-1L(config):/interface/br0/common/ipv6# **enabled true** (Enabling access to the device via IPv6 protocol. To disable enter **false**)
WEP-1L(config):/interface/br0/common/ipv6# **save** (Save changes)

5.3 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).

5.3.1 Configuration of VAP without encryption

Creation of VAP without encryption

```
WEP-1L(root):/# configure
WEP-1L(config):/# interface
WEP-1L(config):/interface# wlan1-va0
WEP-1L(config):/interface/wlan1-va0# vap
WEP-1L(config):/interface/wlan1-va0/vap# ssid 'SSID_WEP-1L_open' (Change SSID name)
WEP-1L(config):/interface/wlan1-va0/vap# security-mode off (Encryption mode off — Without password)
WEP-1L(config):/interface/wlan1-va0/common# exit
WEP-1L(config):/interface/wlan1-va0# common
WEP-1L(config):/interface/wlan1-va0/common# enabled true (Enable VAP)
WEP-1L(config):/interface/wlan1-va0/vap# save
```

5.3.2 Configuration of VAP with WPA-Personal security mode

Creation of VAP with WPA-Personal security mode

WEP-1L(root):/# **configure**
WEP-1L(config):/# **interface**
WEP-1L(config):/interface# **wlan1-va0**
WEP-1L(config):/interface/wlan1-va0# **vap**
WEP-1L(config):/interface/wlan1-va0/vap# **ssid 'SSID_WEP-1L_WPA2'** (Change SSID name)
WEP-1L(config):/interface/wlan1-va0/vap# **security-mode WPA_WPA2** (Encryption mode — WPA/WPA2)
WEP-1L(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-1L(config):/interface/wlan1-va0/common# **exit**
WEP-1L(config):/interface/wlan1-va0# **common**
WEP-1L(config):/interface/wlan1-va0/common# **enabled true** (Enable VAP)
WEP-1L(config):/interface/wlan1-va0/vap# **save**

5.3.3 Configuration of VAP with Enterprise authorization

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

WEP-1L(root):/# **configure**
WEP-1L(config):/# **interface**
WEP-1L(config):/interface# **wlan1-va0**
WEP-1L(config):/interface/wlan1-va0# **vap**
WEP-1L(config):/interface/wlan1-va0/vap# **ssid 'SSID_WEP-1L_enterprise'** (Change SSID name)
WEP-1L(config):/interface/wlan1-va0/vap# **security-mode WPA_WPA2_1X** (Encryption mode — WPA_WPA2-Enterprise)
WEP-1L(config):/interface/wlan1-va0/vap# **radius**
WEP-1L(config):/interface/wlan1-va0/vap/radius# **domain root** (where root — User domain)
WEP-1L(config):/interface/wlan1-va0/vap/radius# **auth-address X.X.X.X** (where X.X.X.X — RADIUS server IP address)
WEP-1L(config):/interface/wlan1-va0/vap/radius# **auth-port X** (where X — RADIUS server port, used for authentication and authorization. By default: 1812)
WEP-1L(config):/interface/wlan1-va0/vap/radius# **auth-password secret** (where secret — Password for RADIUS server, used for authentication and authorization)
WEP-1L(config):/interface/wlan1-va0/vap/radius# **acct-enable true** (Enable the sending of “Accounting” messages to the RADIUS server. By default: false)
WEP-1L(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-1L(config):/interface/wlan1-va0/vap/radius# **acct-password secret** (where secret — Password for RADIUS server, used for accounting)
WEP-1L(config):/interface/wlan1-va0/vap/radius# **acct-periodic true** (Enable the sending of “Accounting” messages to the RADIUS server. By default: false)
WEP-1L(config):/interface/wlan1-va0/vap/radius# **acct-interval 600** (Interval of sending of “Accounting” messages to the RADIUS server.)
WEP-1L(config):/interface/wlan1-va0/common# **exit**
WEP-1L(config):/interface/wlan1-va0# **common**
WEP-1L(config):/interface/wlan1-va0/common# **enabled true** (Enable VAP)
WEP-1L(config):/interface/wlan1-va0/vap# **save**

5.3.4 Configuration of VAP with Captive Portal

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

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

5.3.5 Advanced VAP settings

Enabling VLAN ID on VAP

WEP-1L(config):/interface/wlan1-va0/vap# **vlan-id X** (where X — VLAN-ID number on VAP)

Enabling Band Steer mode

WEP-1L(config):/interface/wlan1-va0/vap# **band-steer-mode true** (Enabling Band Steer mode. To disable, enter **false**)

Enabling VLAN trunk on VAP

WEP-1L(config):/interface/wlan1-va0/vap# **vlan-trunk true** (Enabling VLAN Trunk on VAP. To disable, enter **false**)

Enabling General VLAN on VAP

WEP-1L(config):/interface/wlan1-va0/vap# **general-vlan-mode true** (Enabling General VLAN on SSID. To disable, enter **false)**
WEP-1L(config):/interface/wlan1-va0/vap# **general-vlan-id X** (where X — General VLAN number)

Selection of the prioritization method

WEP-1L(config):/interface/wlan1-va0/vap# **priority-by-dscp false** (Priority analysis from CoS field (Class of Service) tagged packets. Value by default: **true**. In this case, DSCP header field of the IP packet is analyzed)

Enabling use of TLS at authorization

WEP-1L(config):/interface/wlan1-va0/vap/radius# **tls-enable true** (Enabling use of TLS at authorization. To disable, enter **false**)

Enabling hidden SSID

WEP-1L(config):/interface/wlan1-va0/vap# **hidden true** (Enabling hidden SSID. To disable, enter **false**)

Enabling client isolation on VAP

WEP-1L(config):/interface/wlan1-va0/vap# **station-isolation true** (Enable traffic isolation between clients within a single VAP. To disable, enter **false**)

Limiting the number of clients on VAP

WEP-1L(config):/interface/wlan1-va0/vap# **sta-limit X** (where X — maximum allowed number of clients connected to the virtual network)

Enabling Minimal Signal

WEP-1L(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).

Configuring speed limit

Configuring shaper for outbound customers' traffic (each separately) connected to this VAP:

WEP-1L(config):/interface/wlan1-va0/vap# **shaper-per-sta-rx**
WEP-1L(config):/interface/wlan1-va0/vap/shaper-per-sta-rx# **value X** (where X — maximum speed in kbps)
WEP-1L(config):/interface/wlan1-va0/vap/shaper-per-sta-rx# **mode kbps** (Enabling shaper. To disable, enter **off**)
WEP-1L(config):/interface/wlan1-va0/vap/shaper-per-sta-rx# **exit**
WEP-1L(config):/interface/wlan1-va0/vap# **save** (Save changes)

Configuring shaper for customers' traffic (each separately) connected to this VAP:

WEP-1L(config):/interface/wlan1-va0/vap# **shaper-per-sta-tx**
WEP-1L(config):/interface/wlan1-va0/vap/shaper-per-sta-tx# **value X** (where X — maximum speed in kbps)
WEP-1L(config):/interface/wlan1-va0/vap/shaper-per-sta-tx# **mode kbps** (Enabling shaper. To disable, enter **off**)
WEP-1L(config):/interface/wlan1-va0/vap/shaper-per-sta-tx# **exit**
WEP-1L(config):/interface/wlan1-va0/vap# **save** (Save changes)

Configuring shaper for outbound customers' traffic (in total) connected to this VAP:

WEP-1L(config):/interface/wlan1-va0/vap# **shaper-per-vap-rx**
WEP-1L(config):/interface/wlan1-va0/vap/shaper-per-vap-rx# **value X** (where X — maximum speed in kbps)
WEP-1L(config):/interface/wlan1-va0/vap/shaper-per-vap-rx# **mode kbps** (Enabling shaper. To disable, enter **off**)
WEP-1L(config):/interface/wlan1-va0/vap/shaper-per-vap-rx# **exit**
WEP-1L(config):/interface/wlan1-va0/vap# **save** (Save changes)

Configuring shaper for inbound customers' traffic (in total) connected to this VAP:

WEP-1L(config):/interface/wlan1-va0/vap# **shaper-per-vap-tx**
WEP-1L(config):/interface/wlan1-va0/vap/shaper-per-vap-tx# **value X** (where X — maximum speed in kbps)
WEP-1L(config):/interface/wlan1-va0/vap/shaper-per-vap-tx# **mode kbps** (Enabling shaper. To disable, enter **off**)
WEP-1L(config):/interface/wlan1-va0/vap/shaper-per-vap-tx# **exit**
WEP-1L(config):/interface/wlan1-va0/vap# **save** (Save changes)

802.11r configuration
This type of roaming is available only for customers' devices supporting 802.11r.

802.11r roaming is possible only between VAP with WPA2-Personal and WPA2-Enterprise security modes.

VAP configuration with WPA2-Personal security mode manual and others can be seen in section Configuration of VAP with WPA-Personal security mode.

Each VAP on the access points should be configured individually, eg. AP1(wlan1) ↔ AP2(wlan1), AP1(wlan0) ↔ AP2(wlan0), AP1(wlan1) ↔ AP3(wlan1), etc.

Below is the example of 802.11r configuring on two access points: AP1 and AP2.

Configuring 802.11r on AP1

WEP-1L(config):/interface/wlan1-va0/vap/ft-config# **enabled false**
WEP-1L(config):/interface/wlan1-va0/vap/ft-config# **r1-key-holder-id E8:28:C1:FC:D6:80** (MAC address of VAP. Can be viewed in **ifconfig** output)
WEP-1L(config):/interface/wlan1-va0/vap/ft-config# **r0-key-holder-id 12345** (Unique key for this VAP)
WEP-1L(config):/interface/wlan1-va0/vap/ft-config# **mobility-domain 100** (Domain must match on oncoming VAPs)
WEP-1L(config):/interface/wlan1-va0/vap/ft-config# **mac**
WEP-1L(config):/interface/wlan1-va0/vap/ft-config/mac# **add E4:5A:D4:E2:C4:B0** (MAC address of VAP interface of oncoming access point — AP2)
WEP-1L(config):/interface/wlan1-va0/vap/ft-config/mac# **E4:5A:D4:E2:C4:B0**
WEP-1L(config):/interface/wlan1-va0/vap/ft-config/mac/E4:5A:D4:E2:C4:B0# **r0-kh-id 23456** (Unique key of oncoming VAP access point AP2 — r0-key-holder-id)
WEP-1L(config):/interface/wlan1-va0/vap/ft-config/mac/E4:5A:D4:E2:C4:B0# **r1-kh-id E4:5A:D4:E2:C4:B0** (MAC address of oncoming VAP on AP2)
WEP-1L(config):/interface/wlan1-va0/vap/ft-config/mac/E4:5A:D4:E2:C4:B0# **r0-kh-key 0102030405060708** (Random key. Must not match r1-kh-key AP1, but necessarily must match r1-kh-key of oncoming AP2)
WEP-1L(config):/interface/wlan1-va0/vap/ft-config/mac/E4:5A:D4:E2:C4:B0# **r1-kh-key 0001020304050607** (Random key. Must not match r0-kh-key AP1, but necessarily must match r0-kh-key of oncoming AP2)
WEP-1L(config):/interface/wlan1-va0/vap/ft-config/mac/E4:5A:D4:E2:C4:B0# **exit**
WEP-1L(config):/interface/wlan1-va0/vap/ft-config/mac# **exit**
WEP-1L(config):/interface/wlan1-va0/vap/ft-config# **enabled true** (Enabling access point operation via 802.11r protocol)
WEP-1L(config):/interface/wlan1-va0/vap/ft-config# **save** (Save changes)

Configuring 802.11r on AP2

WEP-1L(config):/interface/wlan1-va0/vap/ft-config# **enabled false**
WEP-1L(config):/interface/wlan1-va0/vap/ft-config# **r1-key-holder-id E4:5A:D4:E2:C4:B0** (MAC address of VAP. Can be viewed in **ifconfig** output)
WEP-1L(config):/interface/wlan1-va0/vap/ft-config# **r0-key-holder-id 23456** (Unique key for this VAP)
WEP-1L(config):/interface/wlan1-va0/vap/ft-config# **mobility-domain 100** (Domain must match on oncoming VAPs)
WEP-1L(config):/interface/wlan1-va0/vap/ft-config# **mac**
WEP-1L(config):/interface/wlan1-va0/vap/ft-config/mac# **add E8:28:C1:FC:D6:80** (MAC address of VAP interface of oncoming access point — AP1)
WEP-1L(config):/interface/wlan1-va0/vap/ft-config/mac# **E8:28:C1:FC:D6:80**
WEP-1L(config):/interface/wlan1-va0/vap/ft-config/mac/E8:28:C1:FC:D6:80# **r0-kh-id 12345** (Unique key of oncoming VAP access point AP1 — r0-key-holder-id)
WEP-1L(config):/interface/wlan1-va0/vap/ft-config/mac/E8:28:C1:FC:D6:80# **r1-kh-id E8:28:C1:FC:D6:80** (MAC address of oncoming VAP on AP1)
WEP-1L(config):/interface/wlan1-va0/vap/ft-config/mac/E8:28:C1:FC:D6:80# **r0-kh-key 0001020304050607** (Random key. Must not match r1-kh-key AP2, but necessarily must match r1-kh-key of oncoming AP1)
WEP-1L(config):/interface/wlan1-va0/vap/ft-config/mac/E8:28:C1:FC:D6:80# **r1-kh-key 0102030405060708** (Random key. Must not match r0-kh-key AP2, but necessarily must match r0-kh-key of oncoming AP1)
WEP-1L(config):/interface/wlan1-va0/vap/ft-config/mac/E8:28:C1:FC:D6:80# **exit**
WEP-1L(config):/interface/wlan1-va0/vap/ft-config/mac# **exit**
WEP-1L(config):/interface/wlan1-va0/vap/ft-config# **enabled true** (Enabling access point operation via 802.11r protocol)
WEP-1L(config):/interface/wlan1-va0/vap/ft-config# **save** (Save changes)

802.11k configuration

802.11k protocol roaming can be organized between any network (open/secure). If the access point is configured to work under the 802.11k protocol, then when a customer connects, the access point sends them the list of “friendly” access points to which a customer can switch in a roaming process. The list contains information about access points' MAC addresses and channels they work with.

Use of 802.11k allows to reduce the time that the spends looking for another network when roaming, since the customer does not need to scan channels on which there are no target access points available for switching.

This type of roaming is available only for customers' devices supporting 802.11k.

Below is the example of 802.11k configuring access point — making a list of “friendly” access points.

802.11k configuring

WEP-1L(config):/interface/wlan1-va0/vap/w80211kv-config# **enabled false**
WEP-1L(config):/interface/wlan1-va0/vap/w80211kv-config# **mac**
WEP-1L(config):/interface/wlan1-va0/vap/w80211kv-config/mac# **add E8:28:C1:FC:D6:90** (where E8:28:C1:FC:D6:90 — MAC address of “friendly” access point)
WEP-1L(config):/interface/wlan1-va0/vap/w80211kv-config/mac# **E8:28:C1:FC:D6:90**
WEP-1L(config):/interface/wlan1-va0/vap/w80211kv-config/mac/E8:28:C1:FC:D6:90# **channel 132** (where 132 — channel on which access point with E8:28:C1:FC:D6:90 MAC address operates)
WEP-1L(config):/interface/wlan1-va0/vap/w80211kv-config/mac/E8:28:C1:FC:D6:90# **exit**
WEP-1L(config):/interface/wlan1-va0/vap/w80211kv-config/mac# **add E8:28:C1:FC:D6:70** (where E8:28:C1:FC:D6:70 — MAC address of “friendly” access point)
WEP-1Lx(config):/interface/wlan1-va0/vap/w80211kv-config/mac# **E8:28:C1:FC:D6:70**
WEP-1L(config):/interface/wlan1-va0/vap/w80211kv-config/mac/E8:28:C1:FC:D6:70# **channel 36** (where 36 — channel on which access point with E8:28:C1:FC:D6:70 MAC address operates)
WEP-1L(config):/interface/wlan1-va0/vap/w80211kv-config/mac/E8:28:C1:FC:D6:70# **exit**
WEP-1L(config):/interface/wlan1-va0/vap/w80211kv-config/mac# **exit**
WEP-1L(config):/interface/wlan1-va0/vap/w80211kv-config# **enabled true** (Enabling access point operation via 802.11k protocol)
WEP-1L(config):/interface/wlan1-va0/vap/w80211kv-config# **save** (Save changes)

5.4 Radio settings

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-1L(root):/# **configure**
WEP-1L(config):/# **interface**
WEP-1L(config):/interface# **wlan0**
WEP-1L(config):/interface/wlan0# **wlan**
WEP-1L(config):/interface/wlan0/wlan# **radio-2g** (for wlan1 section is called radio-5g)
WEP-1L(config):/interface/wlan0/wlan/radio-2g# **channel X** (where X — number of the static channel on which the point will operate)
WEP-1L(config):/interface/wlan0/wlan/radio-2g# **auto-channel false** (Disable Auto Channel. To enable, enter **true**)
WEP-1L(config):/interface/wlan0/wlan/radio-2g# **use-limit-channels false** (Disable Use Limit Channels. To enable, enter **true**)
WEP-1L(config):/interface/wlan0/wlan/radio-2g# **bandwidth X** (where X — channel width. Parameter can take the following value: for Radio 1: 20, 40; Radio 2: 20, 40, 80)
WEP-1L(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-1L(config):/interface/wlan0/wlan/radio-2g# **save** (Save changes)

Lists of available channels

Channels available for selection for radio 2.4 GHz :

- for 20 MHz channel width: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13.
- for 40 MHz channel width:
  - if “control-sideband” = lower: 1, 2, 3, 4, 5, 6, 7, 8, 9.
  - fi “control-sideband” = upper: 5, 6, 7, 8, 9, 10, 11, 12, 13.

Channels available for selection for radio 5 GHz:

- for 20 MHz channel width: 36, 40, 44, 48, 52, 56, 60, 64, 132, 136, 140, 144, 149, 153, 157, 161, 165.
- for 40 MHz channel width:
  - if “control-sideband” = lower: 36, 44, 52, 60, 132, 140, 149, 157.
  - if “control-sideband” = upper: 40, 48, 56, 64, 136, 144, 153, 161.
- for 80 MHz channel width: 36, 40, 44, 48, 52, 56, 60, 64, 132, 136, 140, 144, 149, 153, 157, 161.

5.4.1 Advanced Radio settings

Configuring the limited list of channels

WEP-1L(config):/interface/wlan0/wlan/radio-2g# use-limit-channels true (Enabling use of limited list of channels in channel autoselection operation. To disable, enter **false**)
WEP-1L(config):/interface/wlan0/wlan/radio-2g# limit-channels '1 6 11' (where 1, 6, 11 are channels of range in which the configurable radio interface can operate)

Changing the primary channel

WEP-1L(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)

Enabling the use of Short Guard Interval

WEP-1L(config):/interface/wlan0/wlan/radio-2g# **sgi true** (Switching on the use of a Short Guard Interval for data transmission of 400 ns instead of 800 ns. To disable, enter **false**)

Enabling STBC

WEP-1L(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-1L(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-1L(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-1L(config):/interface/wlan0/wlan/radio-2g# **wmm true** (Enabling the support for WMM (Wi-Fi Multimedia). To disable, enter **false**)

Configuring DFS mechanism

Configuring is done only on Radio 5 GHz (wlan1)

WEP-1L(config):/interface/wlan1/wlan/radio-5g# **dfs X** (where X — DFS mechanism operating mode. May take values: **forced** — the mechanism is disabled, DFS channels available for selection; **auto** — the mechanism is enabled; **disabled** — the mechanism is disabled, DFS channels unavailable for selection)

Enabling automatic channel width switch mode

WEP-1L(config):/interface/wlan0/wlan/radio-2g# **obss-coex true** (Enabling automatic channel width switch mode from 40 MHz to 20 MHz with a busy radio environment. To disable, enter **false**)

Enabling Broadcast/Multicast shaper

WEP-1L(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-1L(config):/interface/wlan0/wlan/radio-2g# **qos**
WEP-1L(config):/interface/wlan0/wlan/radio-2g/qos# **enable true** (Enabling the use of Quality of Service functions. To disable, enter **false**)
WEP-1L(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-1L(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-1L(config):/interface/wlan0/wlan/radio-2g/qos/edca-ap/bk# **aifs X** (where X — the time frame(s) of data measured in slots. May take values of 1-255)
WEP-1L(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-1L(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-1L(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-1L(config):/interface/wlan0/wlan/radio-2g/qos/edca-ap/bk# **exit**
WEP-1L(config):/interface/wlan0/wlan/radio-2g/qos/edca-ap# **exit**
WEP-1L(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**.

5.5 System settings

5.5.1 Device firmware upgrade

Device firmware update via tftp

WEP-1L(root):/# **firmware upload tftp < tftp server ip address> <Firmware image name>** (Example: firmware upload tftp 192.168.1.15 WEP-1L-1.2.2_build_X.tar.gz)
WEP-1L(root):/# **firmware upgrade**

Device firmware update via http

WEP-1L(root):/# **firmware upload http <URL to download firmware image>** (Example: firmware upload http http://192.168.1.100:8080/files/WEP-1L-1.2.2_build_X.tar.gz)
WEP-1L(root):/# **firmware upgrade**

Switching to access point firmware backup

WEP-1L(root):/# **firmware switch**

5.5.2 Device configuration management

Resetting the device configuration to a default state without saving the access parameters

WEP-1L(root):/# **manage-config reset-to-default**

Resetting the device configuration to a default state with saving the access parameters

WEP-1L(root):/# **manage-config reset-to-default-without-management**

Download the device configuration file to tftp server

WEP-1L(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-1L(root):/# **manage-config upload tftp <tftp server ip address> <Configuration file name>**
(Example: manage-config upload tftp 192.168.1.15 config.json)
WEP-1L(root):/# **manage-config apply** (Apply configuration on the access point)

5.5.3 Device reboot

The command for rebooting the device.

WEP-1L(root):/# **reboot**

5.5.4 Setting the date and time

Commands to configure NTP server time synchronization

WEP-1L(root):/# **configure**
WEP-1L(config):/# **date-time**
WEP-1L(config):/date-time# **mode ntp** (Enable NTP operation mode)
WEP-1L(config):/date-time# **ntp**
WEP-1L(config):/date-time/ntp# **server <NTP server IP address>** (NTP server configuration)
WEP-1L(config):/date-time/ntp# **exit**
WEP-1L(config):/date-time# **common**
WEP-1L(config):/date-time/common# **timezone 'Asia/Novosibirsk (Novosibirsk)'** (Timezone configuration)
WEP-1L(config):/date-time/common# **save** (Save changes)

5.5.5 Advanced system settings

Enabling global isolation

WEP-1L(root):/# **configure**
WEP-1L(config):/# **system**
WEP-1L(config):/system# **global-station-isolation true** (Enabling global traffic isolation between customers of different VAP и different radio interfaces. To disable, enter **false**)
WEP-1Lconfig):/system# **save** (Save changes)

Changing device name

WEP-1L(root):/# **configure**
WEP-1L(config):/# **system**
WEP-1L(config):/system# **hostname WEP-1L_room2** (where WEP-1L_room2 — new name of the device. A parameter can contain from 1 to 63 symbols: capital и lowercase latin letters, nu,bers, hyphen character “-” (hyphen can not be the last character in name). By default: WEP-1L)
WEP-1L(config):/system# **save** (Save changes)

Changing geographical domain

WEP-1L(root):/# **configure**
WEP-1L(config):/# **system**
WEP-1L(config):/system# **ap-location ap.test.root** (where ap.test.root — EMS management system device tree node domain, where access point is located. By default: root)
WEP-1L(config):/system# **save** (Save changes)

Changing password

WEP-1L(root):/# **configure**
WEP-1L(config):/# **authentication**
WEP-1L(config):/authentication# **admin-password newpassword** (where newpassword — new password to login to the access point. By default: password)
WEP-1L(config):/authentication# **save** (Save changes)

5.6 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-1L(root):/# **configure**
WEP-1L(config):/# **captive-portal**
WEP-1L(config):/captive-portal# **apbd**
WEP-1L(config):/captive-portal/apbd# **roam_service_url <APB service address>** (Example: roam_service_url ws://192.168.1.100:8090/apb/broadcast)
WEP-1L(config):/captive-portal/apbd# **enabled true** (Enabling APB service. To disable it, enter **false**)
WEP-1L(config):captive-portal/apbd# **save** (Save changes)

5.7 Monitoring

5.7.1 Wi-Fi Clients

To display monitoring of connected Wi-Fi clients, use the command:

monitoring associated-clients <mac address of client 1> ... <mac address of client N> **filter** <parameter 1> ... <parameter N>,

where <mac address of client 1> ... <mac address of client N> — mac addresses of customer devices, connected to the access point. In order to display information for all customers, instead of <mac address of client> enter **all**;

filter — a special word followed by the monitoring parameters required for withdrawal by client/clients;

<parameter 1> ... <parameter N> — monitoring parameter/parameters, necessary for client/clients display.

To display a list of clients connected to the access point, press Tab after **monitoring associated-clients.**

WEP-1L(root):/# **monitoring associated-clients** <Tab>

```
32:5b:60:62:e0:a4
bc:2e:f6:cc:85:46
all
```

To get a list of monitoring parameters, press Tab after **filter.**

WEP-1L(root):/# **monitoring associated-clients all filter** <Tab>

```
index
interface
ssid
hw-addr
state
ip-addr
hostname
rx-retry-count
tx-fails
tx-period-retry
tx-retry-count
.....
```

WEP-1L(root):/# **monitoring associated-clients** (or **monitoring associated-clients all**)

```
 index                    | 0
 interface                | wlan1-va0
 state                    | ASSOC SLEEP AUTH_SUCCESS
 hw-addr                  | 32:5b:60:62:e0:a4
 ssid                     | 2ac-open
 ip-addr                  | 10.24.80.58
 authorized               | true
 captive-portal-vap       | false
 enterprise-vap           | false
 rx-retry-count           | 161
 tx-fails                 | 0
 tx-period-retry          | 3
 tx-retry-count           | 626
 rssi-1                   | -20
 rssi-2                   | -20
 snr-1                    | 14
 snr-2                    | 14
 tx-rate                  | MCS15 NO SGI 270
 rx-rate                  | MCS15 NO SGI 130
 rx-bw                    | 20M
 rx-bw-all                | 20M
 tx-bw                    | 40M
 uptime                   | 00:01:32
 multicast-groups-count   | 1
 wireless-mode            | n
 perftest-capable         | false
 snr-rssi-capable         | false
 link-capacity            | 100
 link-quality             | 99
 link-quality-common      | 96
 actual-tx-rate           | 449
 actual-rx-rate           | 30
 shaped-rx-rate           | 32
 actual-tx-pps            | 49
 actual-rx-pps            | 29
 shaped-rx-pps            | 29
 name                     | 0

 Rate                  Transmitted            Received
-------------------------------------------------------------------
 Total Packets:       | 8165                 | 6387                |
 TX success:          | 100                  |                     |
 Total Bytes:         | 8446088              | 1125301             |
 Data Packets:        | 8158                 | 6008                |
 Data Bytes:          | 8233649              | 959850              |
 Mgmt Packets:        | 7                    | 379                 |
 Mgmt Bytes:          | 331                  | 291                 |
-------------------------------------------------------------------

 Rate                  Transmitted            Received
-------------------------------------------------------------------
 ofdm6                | 9              |   0%|            378 |   5%|
 mcs7                 | 2              |   0%|              0 |   0%|
 mcs11                | 0              |   0%|              3 |   0%|
```

```
 mcs12                | 28             |   0%|              66 |   1%|
 mcs14                | 1183           |  14%|               0 |   0%|
 mcs15                | 6943           |  85%|            5939 |  93%|
-------------------------------------------------------------------------


Multicast groups:
 MAC                IP
--------------------------------------
 01:00:5E:00:00:FB |     xxx.0.0.251 |
--------------------------------------


 index                    | 1
 interface                | wlan1-va2
 state                    | ASSOC AUTH_SUCCESS
 hw-addr                  | bc:2e:f6:cc:85:46
 ssid                     | 2ac-enter
 ip-addr                  | 10.24.80.90
 hostname                 | HUAWEI_P40_Pro-81afe9c34a
 username                 | tester
 domain                   | enterprise.service.root
 authorized               | true
 captive-portal-vap       | false
 enterprise-vap           | true
 rx-retry-count           | 7
 tx-fails                 | 0
 tx-period-retry          | 1
 tx-retry-count           | 1
 rssi-1                   | -37
 rssi-2                   | -54
 snr-1                    | 11
 snr-2                    | 10
 tx-rate                  | MCS15 NO SGI 130
 rx-rate                  | MCS15 NO SGI 130
 rx-bw                    | 20M
 rx-bw-all                | 20M
 tx-bw                    | 20M
 uptime                   | 00:00:13
 multicast-groups-count   | 0
 wireless-mode            | ac
 perftest-capable         | false
 snr-rssi-capable         | false
 link-capacity            | 76
 link-quality             | 99
 link-quality-common      | 99
 actual-tx-rate           | 49
 actual-rx-rate           | 24
 shaped-rx-rate           | 23
 actual-tx-pps            | 17
 actual-rx-pps            | 20
 shaped-rx-pps            | 19
 name                     | 1

 Rate                  Transmitted            Received
-------------------------------------------------------------------------
 Total Packets:       | 178                  | 263                  |
 TX success:          | 100                  |                      |
```

```
 Total Bytes:          | 68476                | 38913                |
 Data Packets:         | 174                  | 207                  |
 Data Bytes:           | 63720                | 32019                |
 Mgmt Packets:         | 4                    | 56                   |
 Mgmt Bytes:           | 232                  | 240                  |
-------------------------------------------------------------------

 Rate                   Transmitted            Received
-------------------------------------------------------------------
 ofdm6                 | 21             |  11%|             33 |  12%|
 ofdm24                | 0              |   0%|             43 |  16%|
 mcs7                  | 15             |   8%|              0 |   0%|
 mcs12                 | 41             |  23%|              0 |   0%|
 mcs13                 | 43             |  24%|              0 |   0%|
 mcs14                 | 0              |   0%|              3 |   1%|
 mcs15                 | 58             |  32%|            183 |  69%|
-------------------------------------------------------------------


Multicast groups: none
```

Filtering monitoring parameters

WEP-1L(root):/# **monitoring associated-clients 32:5b:60:62:e0:a4 filter hw-addr ip-addr tx-rate rx-rate uptime** (display of a limited number of monitoring parameters for a certain client. It is possible to specify several mac addresses)

```
 hw-addr                | 32:5b:60:62:e0:a4
 ip-addr                | 10.24.80.58
 tx-rate                | MCS15 NO SGI 270
 rx-rate                | MCS14 NO SGI 117
 uptime                 | 00:07:57
```

WEP-1L(root):/# **monitoring associated-clients all filter hw-addr rssi-1 rssi-2 wireless-mode interface** (display of a limited number of monitoring parameters for all clients)

```
 hw-addr                | 32:5b:60:62:e0:a4
 rssi-1                 | -24
 rssi-2                 | -24
 wireless-mode          | n
 interface              | wlan1-va0

 hw-addr                | bc:2e:f6:cc:85:46
 rssi-1                 | -38
 rssi-2                 | -53
 wireless-mode          | ac
 interface              | wlan1-va2
```

5.7.2 Device info

WEP-1L(root):/# **monitoring information**

```
system-time: 09:15:16 28.10.2021
uptime: 15:45:10
software-version: 1.2.2 build X
secondary-software-version: 1.1.0 build 444
boot-version: 1.1.0 build 444
memory-usage: 67
memory-free: 34
memory-used: 71
memory-total: 105
cpu: 0.28
is-default-config: true
board-type: WEP-1L
hw-platform: WEP-1L
factory-wan-mac: E8:28:C1:xx:xx:xx
factory-lan-mac: E8:28:C1:xx:xx:xx
factory-serial-number: WP39000059
hw-revision: 1v1
session-password-initialized: false
ott-mode: false
last-reboot-reason: firmware update
test-changes-mode: false
```

5.7.3 Network information

WEP-1L(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-1L(root):/# **monitoring ethernet**

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

WEP-1L(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-1L(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
```

5.7.4 Wireless interfaces

WEP-1L(root):/# **monitoring radio-2**

```
hwaddr: E8:28:C1:xx:xx:xx
status: on
noise-1: -100
noise-2: -100
utilization: 10
channel: 5
thermal: 32
bandwidth: 40
frequency: 2432
```

WEP-1L(root):/# **monitoring radio-5**

```
hwaddr: E8:28:C1:xx:xx:xx
status: on
noise-1: -100
noise-2: -100
utilization: 0
channel: 132
thermal: 32
bandwidth: 80
frequency: 5660
```

5.7.5 Event logging

WEP-1L(root):/# **monitoring events**

```
Jan  23 00:00:07 WEP-1L daemon.info syslogd[925]: started: BusyBox v1.21.1

Jan  23 00:00:09 WEP-1L daemon.info configd[955]: The AP startup configuration was loaded
successfully.

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

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

Jan 23 07:17:14 WEP-1L daemon.info monitord[1055]: event: 'associated' mac: E4:0E:EE:BD:AE:
6B ssid: 'WEP-1L_2.4GHz' int0
```

5.7.6 Environment scan

Note that during environment scan the device radio interface will be disabled, which will result in the impossibility of data transmission to Wi-Fi clients during scanning.

WEP-1L(root):/# **monitoring scan-wifi**

```
SSID                              |Mode |Security|MAC               |Channel|RSSI, dBm|
Bandwidth, MHz
----------------------------------|-----|--------|------------------|-------|---------|-----
---------
ESRAP1_of30_smart                 |AP   |off     |A8:F9:4B:B0:2C:C7 |6      |-65      |20
litv_hots_2                       |AP   |off     |E0:D9:E3:8A:38:52 |1      |-65      |20
test_001                          |AP   |off     |E0:D9:E3:4B:FB:30 |11     |-67      |20
2G-COVID_TOWER                    |AP   |off     |E0:D9:E3:98:12:72 |11     |-71      |20
Tam2.4G                           |AP   |wpa     |E0:D9:E3:98:1F:7A |1      |-73      |20
litv_hots_1                       |AP   |off     |E0:D9:E3:8A:38:51 |1      |-77      |20
WEP-1L_ZN_Personal                |AP   |wpa     |E0:D9:E3:49:79:06 |44     |-16      |20
WEP-1L_ZN_Open                    |AP   |off     |E0:D9:E3:49:79:07 |44     |-17      |20
Eltex-Guest                       |AP   |off     |CC:9D:A2:C7:D9:21 |36     |-38      |20
Eltex-Local                       |AP   |wpa     |CC:9D:A2:C7:D9:22 |36     |-38      |20
BRAS-Guest                        |AP   |off     |CC:9D:A2:C7:D9:20 |36     |-38      |20
2L_301_nsk                        |AP   |off     |E8:28:C1:DA:C8:16 |56     |-41      |20
chudo_waffly                      |AP   |wpa     |E0:D9:E3:70:94:00 |60     |-44      |20
Eltex VAP                         |AP   |off     |A8:F9:4B:B0:40:70 |48     |-46      |20
VK_enterprise                     |AP   |wpa     |E8:28:C1:DA:C8:99 |56     |-47      |20
VK_portal                         |AP   |off     |E8:28:C1:DA:C8:98 |56     |-49      |20
WOP-2ac                           |AP   |off     |E8:28:C1:00:FC:A1 |36     |-50      |80
Open_VK_switch                    |AP   |off     |E8:28:C1:DA:C8:96 |56     |-50      |20
testSSID10                        |AP   |off     |A8:F9:4B:B0:05:54 |40     |-51      |20
```

5.7.7 Spectrum Analyzer

Note that during the spectrum analyzer operation all clients are disconnected from the access point. Clients will only reconnect when the spectrum analyzer is finished. The analysis time for all radio channels of the two bands is approximately 5 minutes.

The spectrum analyzer operaates only on those channels that are specified in the limit-channels parameter in the radio interface settings. For example, if the channels' 1 6 11 'are specified in the limit-channels on wlan0, and the channels '36 40 44 48' are specified on wlan1, then the spectrum analysis will be performed only for channels 1, 6, 11, 36, 40, 44, 48.
In order to analyze all channels of the range on which the radio interface operates, change the value of the use-limit-channels parameter in the settings of each radio interface to false. After receiving the results of the spectrum analyzer, set the use-limit-channels value back to the original value true.
For more information on configuring the radio interface through the CLI, see the Radio section.

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

WEP-1L(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.

6 The list of changes

Document version	Issue date	Revisions
Version 1.2	24.01.2022	Syncronization with firmware version 1.2.2 Added sections: • 4.8 The “External Services” menu • 5.2.1 Network parameters configuration via set-management-vlan-mode utility • 5.2.2 IPv6 network parameters configuration • 5.7.6 Environment scan Corrected: • 2.2 Device specification • 4.4.1 The “Wi-Fi Clients” submenu • 4.6.1 The “Summary” submenu • 4.6.2 The “VAP” submenu • 5.3.5 Advanced VAP settings • 5.7.2 Device info
Version 1.1	30.06.2020	Syncronization with firmware version 1.1.0
Version 1.0	11.02.2020	First issue
Firmware version 1.2.2		

TECHNICAL SUPPORT

For technical assistance in issues related to handling Eltex Ltd. equipment, please, address to Service Center of the company:

http://www.eltex-co.com/support

You are welcome to visit Eltex official website to get the relevant technical documentation and software, to use our knowledge base or consult a Service Center Specialist in our technical forum.

http://www.eltex-co.com/

http://www.eltex-co.com/support/downloads/