Integrated Networking Solutions

Wireless access point

WEP-30L, WEP-30L-Z

User manual

Firmware version 2.5.2

IP address: 192.168.1.10

Username: admin

Password: password

www.eltex-co.com

Contents

1 Introduction

1.1 Annotation

Modern tendencies of telecommunication development necessitate operators to search for the most optimal technologies, allowing one to meet rapidly growing needs of subscribers, while maintaining at the same time consistency of business processes, development flexibility and reducing the costs of various services. 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 access networks equitable to speed of wired networks with high criteria to the quality of provided services.

The main purpose of WEP-30L and WEP-30L-Z is installation inside buildings as access points to various resources creating a seamless wireless network from several identical access points (“Roaming”), if the coverage area is large enough.

This manual specifies intended purpose, main technical parameters, design, safe operation rules, and installation and configuration recommendations for WEP-30L and WEP-30L-Z.

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

The wireless access points WEP-30L and WEP-30L-Z are designed to provide the user access to high-speed and secure network.

The main purpose of the devices is to create a Layer 2 wireless network at the junction with a wired network. WEP-30L and WEP-30L-Z connect to a wired network over 10/100/1000/2500M Ethernet interface and using radio interfaces create wireless high-speed access for devices that support Wi-Fi technology in the 2.4 GHz and 5 GHz bands.

The devices contain 2 radio interfaces for organizing two physical wireless networks.

WEP-30L-Z has a built-in IoT Hub compatible with Z-Wave devices from ELTEX, to interact with IoT ecosystem sensors and devices and to manage them through the Eltex Smart Cloud (Eltex SC) platform.

WEP-30L and WEP-30L-Z support modern quality of service requirements and allow one to transmit the most important traffic in higher priority queues than normal. Prioritization is provided by the following QoS technologies: CoS (special tags in the VLAN packet field) and ToS (tags in the IP packet field). Support for traffic shaping on each VAP allows one to fully manage access, quality of service and restrictions both for all subscribers and for everyone in particular.

The devices are designed for installation in offices (government institutions, conference rooms, laboratories, hotels, etc.). Ability to create virtual hotspots with different encryption types allows one to place WEP-30L and WEP-30L-Z in organizations where separation of access rights is required between ordinary users and dedicated user groups.

2.2 Device specification

Interfaces:

- 1 port of Ethernet 10/100/1000/2500BASE-T (RJ-45) with PoE support;
- Wi-Fi 2.4 GHz IEEE 802.11b/g/n/ax;
- Wi-Fi 5 GHz IEEE 802.11a/n/ac/ax;
- Z-Wave interface is a radio interface to manage the IoT ecosystem (for WEP-30L-Z only).

Functions:

WLAN capabilities:

- Support for IEEE 802.11a/b/g/n/ac/ax 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;
- Wireless bridging (WDS);
- Dynamic frequency selection (DFS);
- Support for hidden SSID;
- 14 virtual access points;
- Third-party access point detection;
- Spectrum analyzer;
- Support for APSD.

Network functions:

- Auto-negotiation of speed, duplex mode and switching between MDI and MDI-X modes;
- Support for VLAN (Access, Trunk, General);
- DHCP client;
- GRE;
- Transmission of subscriber traffic out of tunnel;
- ACL;
- NTP;
- Syslog;
- IPv6.

QoS functions:

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

Security:

- Centralized authorization via RADIUS server (802.1X WPA/WPA2/WPA3 Enterprise);
- WPA/WPA2/WPA3/OWE data encryption;
- Support for Captive Portal.

Figure 1 shows WEP-30L/WEP-30L-Z application diagram.

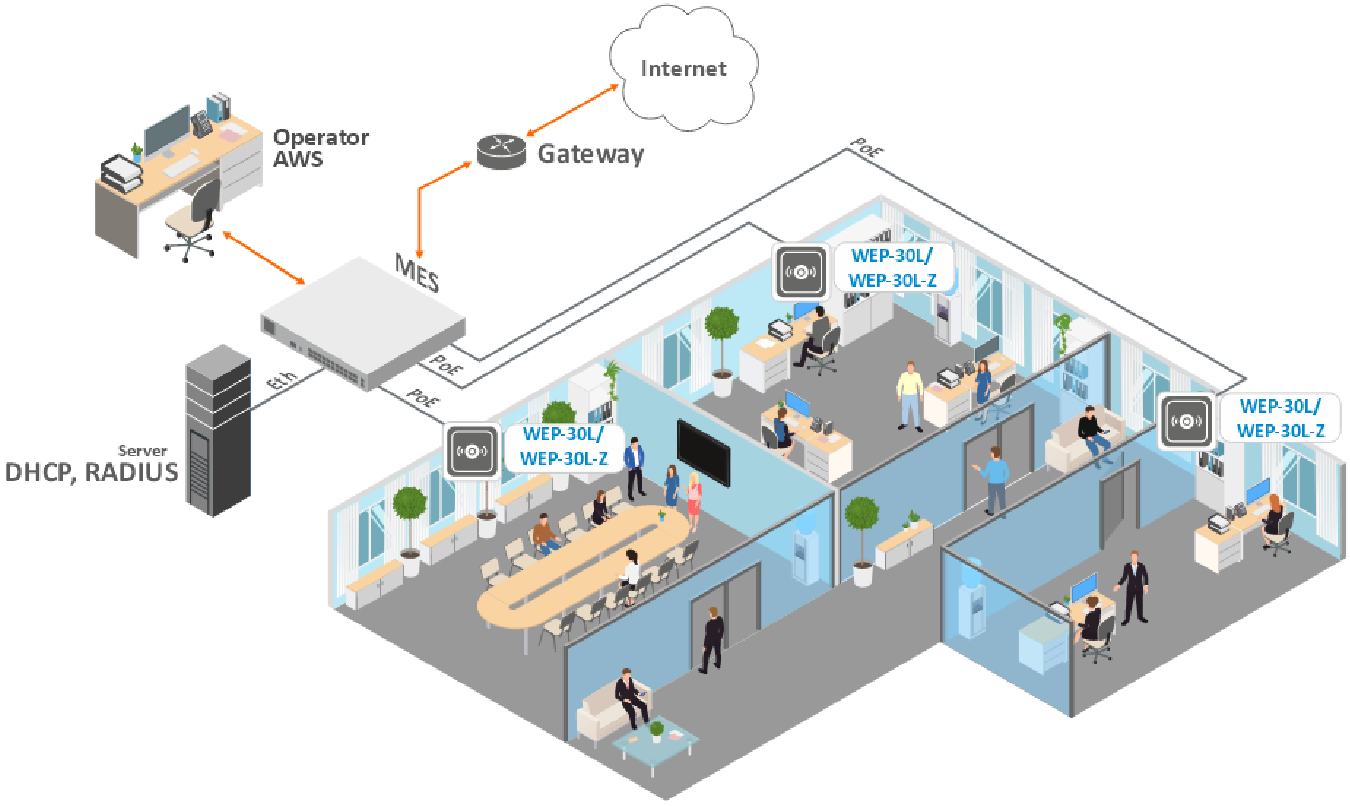


Figure 1 — WEP-30L/WEP-30L-Z application diagram

2.3 Technical parameters

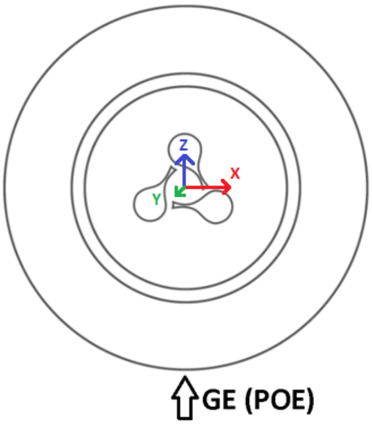
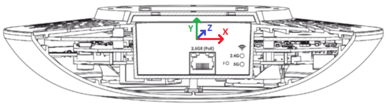
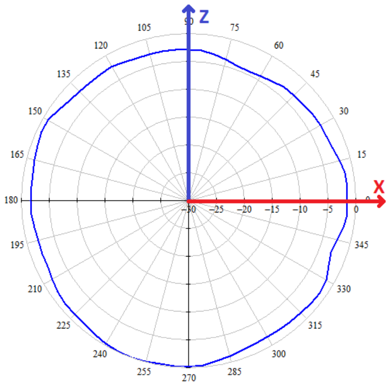
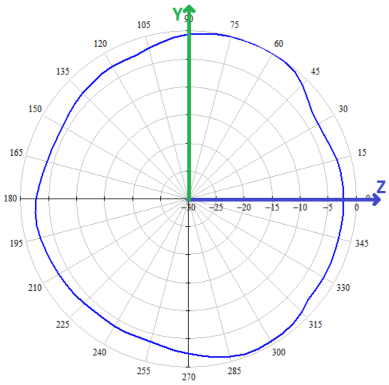
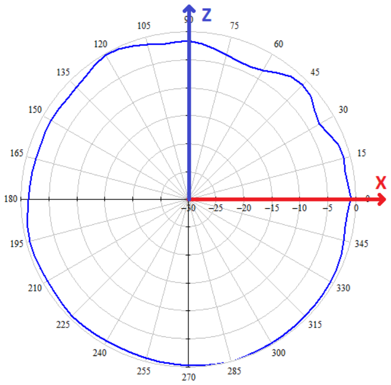
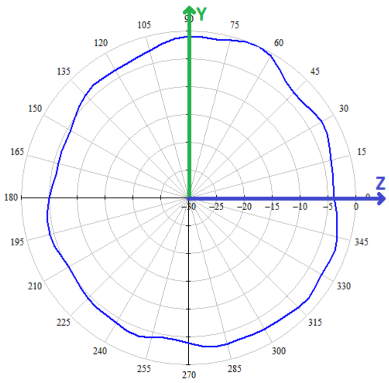
Table 1 — Main specifications

WAN interface parameters	
Number of ports	1
Electrical connector	RJ-45
Data rate	10/100/1000/2500 Mbps, auto-negotiation
Standards	BASE-T
Wireless interface parameters	
Standards	802.11a/b/g/n/ac/ax
Frequency range	2400–2483.5 MHz; 5150–5350 MHz, 5470–5850 MHz
Modulation	BPSK, QPSK, 16QAM, 64QAM, 256QAM, 1024QAM
Operating channels	802.11b/g/n/ax: 1–13 (2402–2482 MHz) 802.11a/n/ac/ax: • 36–64 (5170–5330 MHz) • 100–144 (5490–5730 MHz) • 149–165 (5735–5835 MHz)
Data rate	2.4 GHz, 802.11ax: 574 Mbps 5 GHz, 802.11ax: 1201 Mbps
Maximum number of concurrent sessions	2.4 GHz: 64 5 GHz: 64
Maximum output power of the transmitter	2.4 GHz: 20 dBm 5 GHz: 20 dBm
Built-in antenna gain	2.4 GHz: ~ 3 dBi 5 GHz: ~3 dBi
Receiver sensitivity	2.4 GHz: up to -95 dBm 5 GHz: up to -95 dBm
Security	centralized authorization via RADIUS server (802.1X WPA/WPA2/WPA3 Enterprise) WPA/WPA2/WPA3/OWE data encryption support for Captive Portal
Radio interface with OFDMA and MU-MIMO 2×2 support	
IoT hub (for WEP-30L-Z only)	
Z-Wave module signal frequency	869 MHz
Control	
Remote control	web interface, Telnet, SSH, CLI, SNMP, NETCONF
Access restriction	by password, authentication via RADIUS server
General parameters	
Flash	128 MB SPI-NAND Flash

RAM	256 MB DDR3 RAM
Power supply	PoE 48 V/56 V (IEEE 802.3af-2003)
Maximum power consumption	no more than 12.95 W
Operating temperature range	from +5 to +40 °C
Relative humidity at 25 °C	up to 80 %
Dimensions (diameter × height)	230 × 56 mm
Weight	0.5 kg
Service life	no less than 15 years

2.4 Radiation patterns

The figures below show the radiation patterns of the device.

Measurement position	
AZIMUTH (XZ)	ELEVATION (YZ)
	
2.4 GHz band	
	
5 GHz band	
	

2.5 Design

WEP-30L and WEP-30L-Z are enclosed in a plastic case.

2.5.1 Main panel of the device

The main panel layout of WEP-30L and WEP-30L-Z is shown in Figure 2.

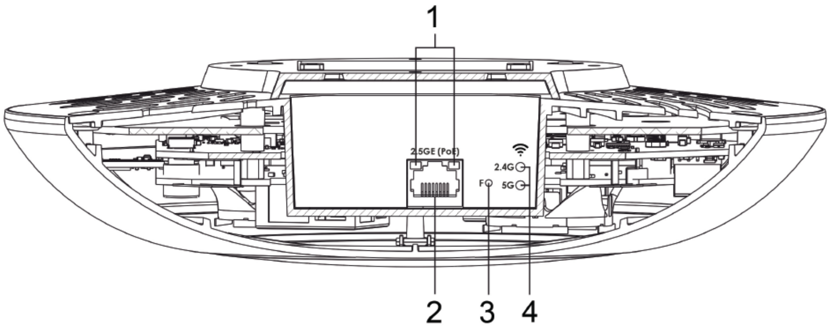


Figure 2 — WEP-30L and WEP-30L-Z main panel layout

The following indicator lights, connectors, and controls are placed on the main panel of WEP-30L and WEP-30L-Z (see table 2).

Table 2 — Description of indicators, ports and controls

Element		Description
1	LAN	2.5GE (PoE) port status LED
2	2.5GE (PoE)	2.5GE port for Ethernet cable connection and PoE+ power supply
3	F	Factory reset button
4	Wi-Fi	Wi-Fi module activity LEDs

2.5.2 Top panel of the device

The top panel layout of WEP-30L and WEP-30L-Z is shown in Figure 3.

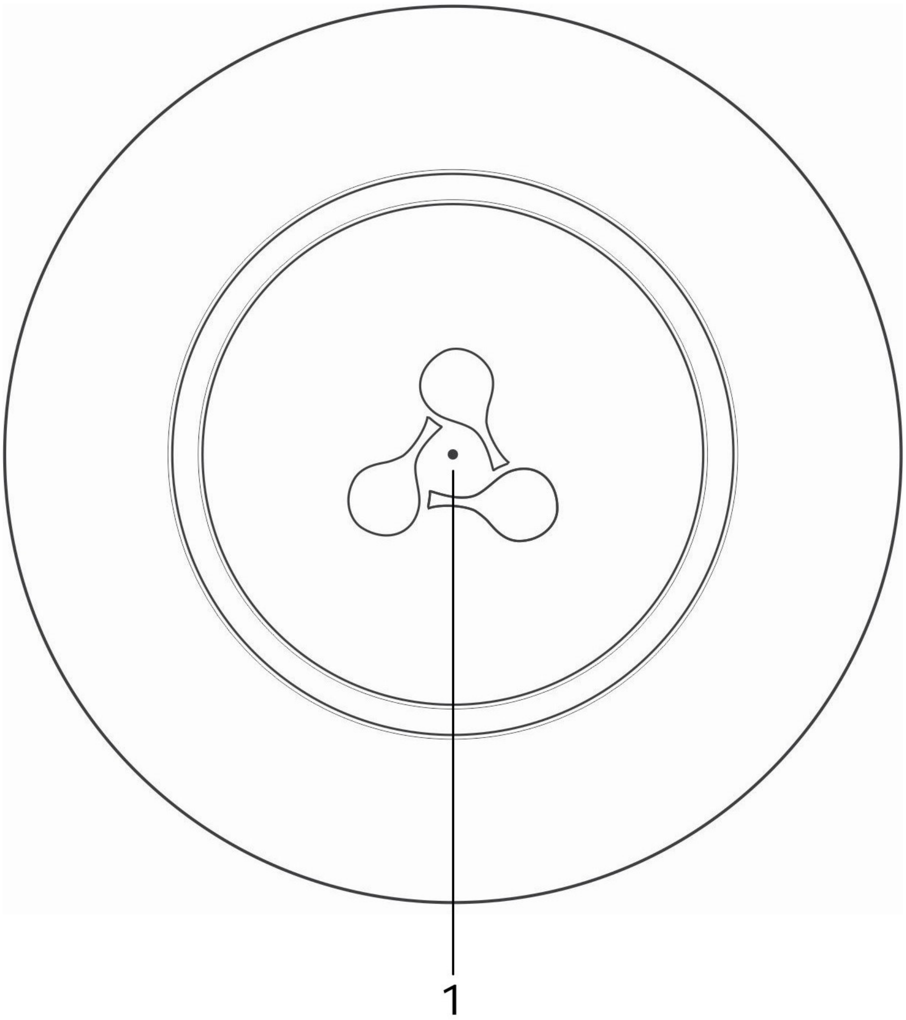


Figure 3 — WEP-30L and WEP-30L-Z top panel layout

Table 3 — Light indication of the top panel

Element		Description
1	Power	Device operation status indicator

2.6 Light indication

The current status of the device is displayed using **Wi-Fi, LAN, Power** LEDs. The possible indicator states are described in Table 4.

Table 4 — Light indication of device status

LED	LED status	Description
Wi-Fi	Solid green	Wi-Fi network is active
	Flashing green	Data transmission over wireless network
LAN	Solid green (10, 100 Mbps) Solid orange (1000, 2500 Mbps)	The connection with a connected network device is established
	Flashing green	Packet data transmission over LAN interface
Power	Solid green	The device power supply is enabled, normal operation
	Solid orange	The device is loaded but IP address is not received via DHCP
	Solid red	The device is loading

2.7 Restore the default configuration

The device can be reset to the factory configuration using the “F” button on the device. When the device is loaded, press and hold the “F“ button (approximately 10–15 seconds) until “Power” indicator is flashing. The device will be rebooted automatically. DHCP client will be launched by default. If the address is not obtained via DHCP, the device will have the factory IP address — *192.168.1.10*, and the following netmask — *255.255.255.0*.

2.8 Supply package

The supply package includes:

- WEP-30L/WEP-30L-Z radio access equipment;
- Mounting kit;
- User manual on a CD (optional);
- 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 near heat source and at places where temperature may reach values below +5 °C or higher +40 °C.
2. Do not use the device in rooms with high humidity. Do not expose the device to smoke, dust, water, mechanical vibration or shock.
3. Do not open the device case. There are no user serviceable parts inside.

> ❗ To prevent overheating of the device components and malfunction of the device, do not block the ventilation holes with foreign objects and do not place objects on the equipment surface.

3.2 Installation recommendations

1. The recommended installation position: horizontal, on the ceiling.

2. Before installing the device and turning it on, check the device for visible mechanical defects. If defects are observed, stop the device installation, fill in the corresponding act and contact the supplier.

3. If your device has been exposed to the cold for a long period of time, let it warm up at room temperature for two hours before starting work. If your device has been exposed to high humidity for a long period of time, let it stay under normal conditions for at least 12 hours before turning it on.

4. When placing your device, in order to provide the best Wi-Fi coverage consider the following rules:

- Install the device at the center of a wireless network;
- Minimize the number of barriers (walls, ceilings, furniture, and etc.) between WEP-30L/WEP-30L-Z and other wireless network devices;
- Do not install the device near (about 2 m) electrical and radio devices;
- It is not recommended to use radiophone and other equipment operating at the frequency of 2.4 GHz or 5 GHz, within the range of a Wi-Fi network;
- Obstacles like glass/metal constructions, brick/concrete walls, water cans and mirrors can significantly reduce Wi-Fi action radius. It is not recommended to place the device inside a false ceiling as metal frame causes multipath signal propagation and signal attenuation.

5. When installing several access points, cell action radius must overlap with action radius of a neighboring cell at the level from -65 to -70 dBm. It is allowed to reduce the signal level to -75 dBm at cell boundaries, if it is not intended to use VoIP, video streaming and other sensitive to losses traffic in wireless network.

3.3 Calculating the number of required access points

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

Table 5 — Attenuation values

Material	**Change of signal level, dB**	
	2.4 GHz	**5 GHz**
Organic glass	-0.3	-0.9
Brick	-4.5	-14.6
Glass	-0.5	-1.7
Plaster slab	-0.5	-0.8
Wood laminated plastic	-1.6	-1.9
Plywood	-1.9	-1.8
Plaster with wirecloth	-14.8	-13.2
Breezeblock	-7	-11
Metal lattice (mesh 13 × 6 mm, metal 2 mm)	-21	-13

3.4 Channel selection for neighboring access points

It is recommended to set non-overlapping channels to avoid inter-channel interference among neighboring access points.

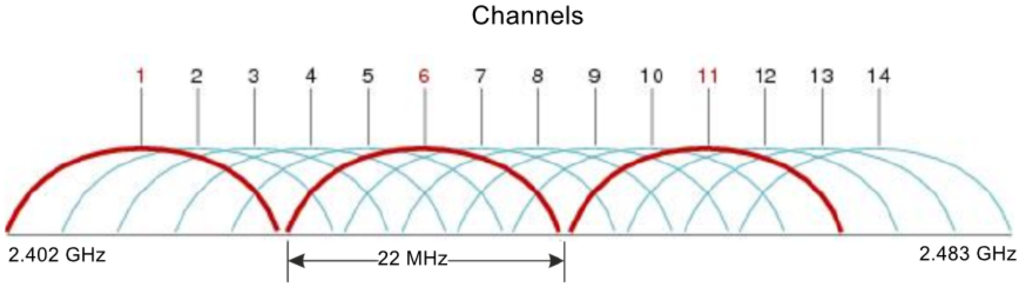


Figure 4 – General diagram of frequency channel overlap in the range of 2.4 GHz

Example of channel allocation scheme among neighboring access points in frequency range of 2.4 GHz when channel width is 20 MHz, see Figure 5.

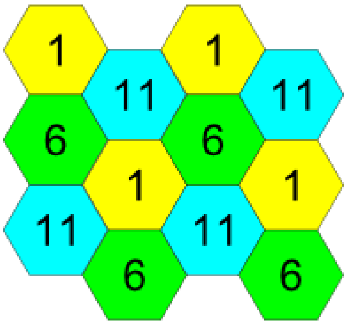


Figure 5 – Scheme of channel allocation among neighboring access points in the frequency range of 2.4 GHz when channel width is 20 MHz

Similarly, the procedure of channel allocation is recommended to save for access point allocation between floors, see Figure 6.

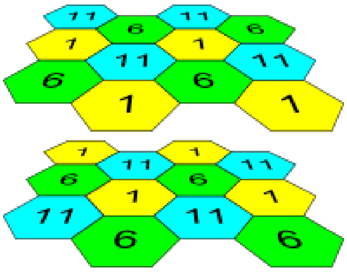


Figure 6 – Scheme of channel allocation between neighboring access points that are located between floors

With a channel width of 40 MHz there are no non-overlapping channels in the 2.4 GHz band. In such cases, you should select channels maximally separated from each other.

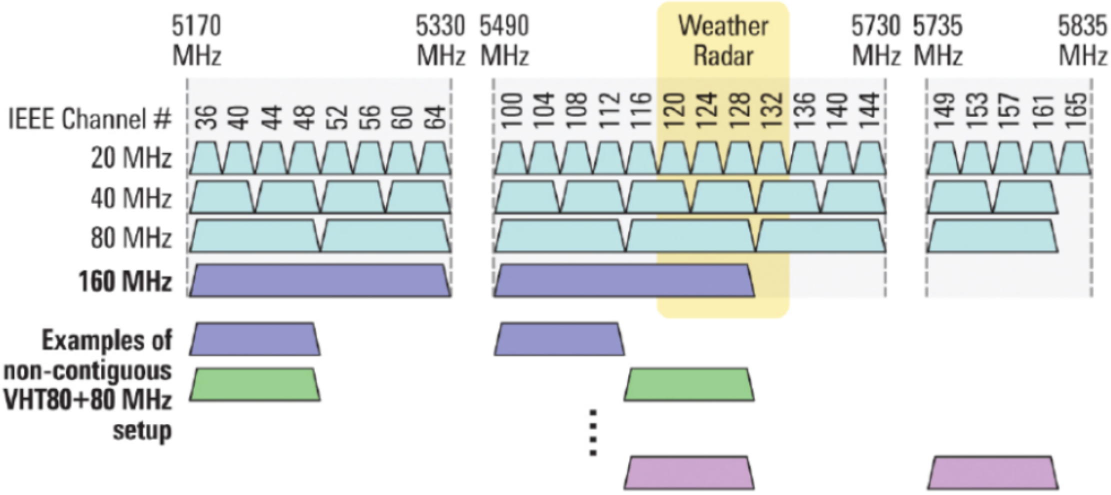


Figure 7 – Channels used in the 5 GHz band when channel width is 20, 40 or 80 MHz

4 Device installation

The device can be installed on the plain surface (wall or ceiling) in accordance with the safety instructions and recommendations listed above.

The device supply package includes required mounting kit to attach the device to plain surface.

4.1 Wall mounting procedure

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

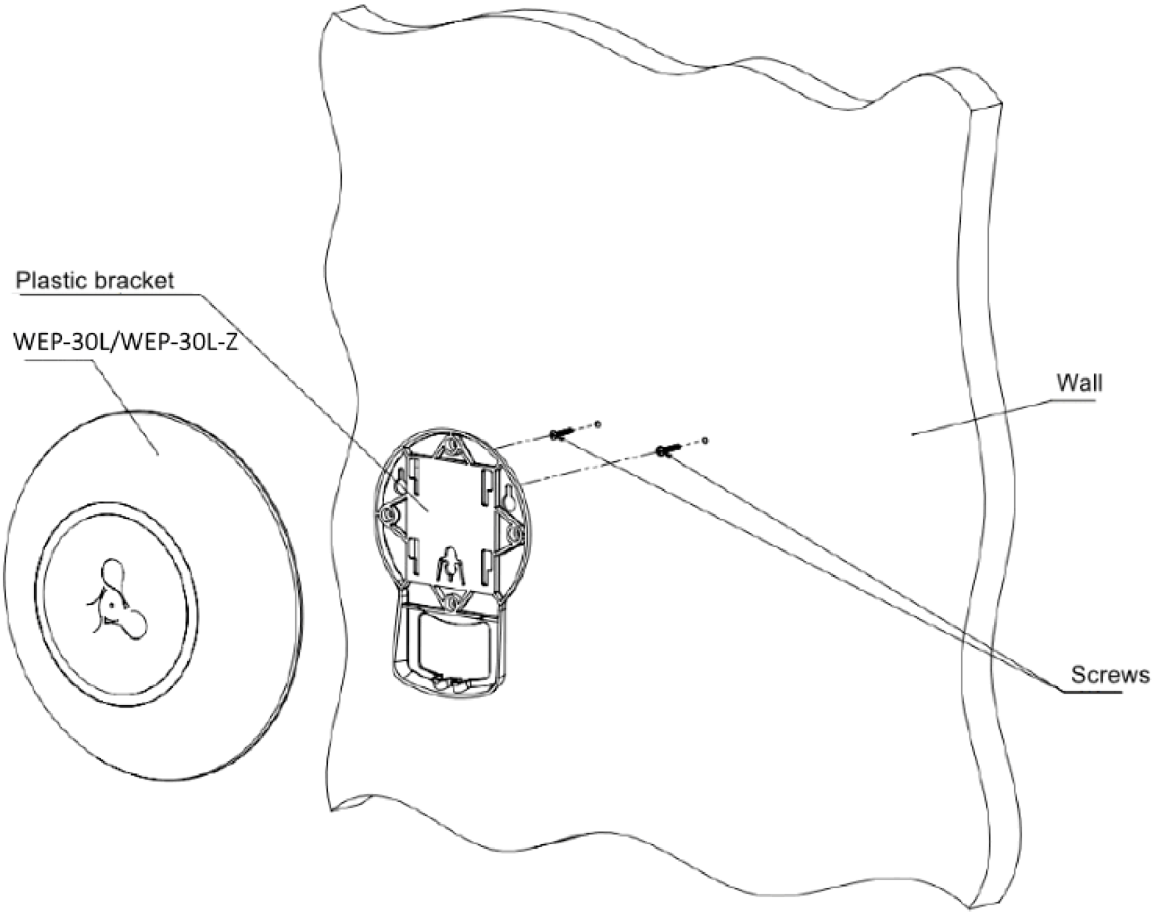


Figure 8 – Attaching the bracket to a wall

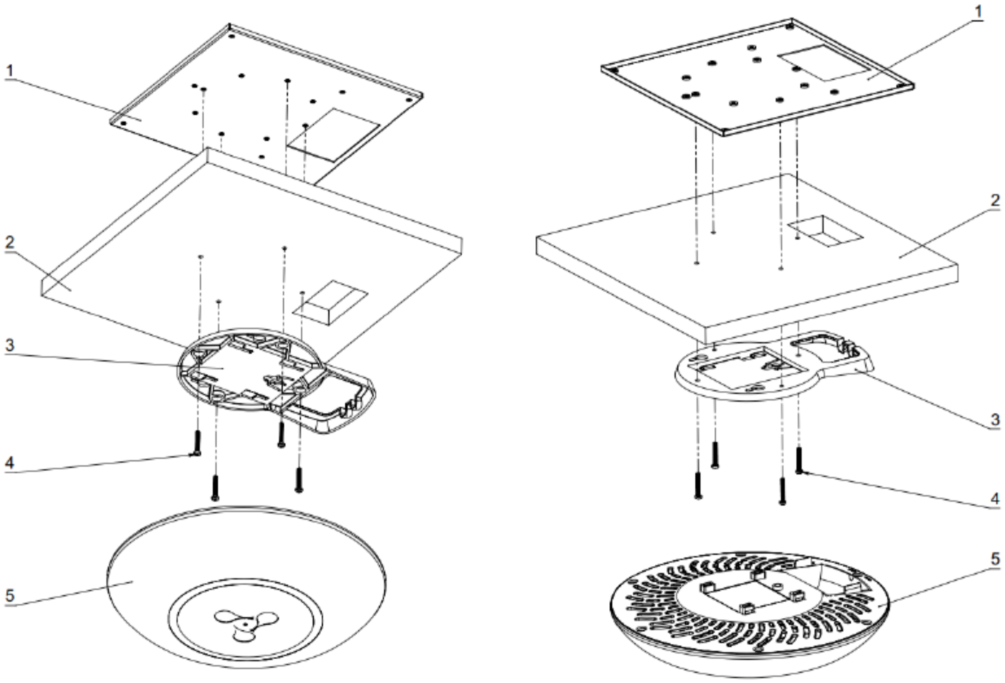
- An example of placing the plastic bracket is shown in Figure 8.
- When installing the bracket, pass wires through the corresponding channels of the bracket, see Figure 8.
- Align four screw holes on the bracket with the corresponding screw holes on the surface. Screw the bracket to the surface using a screwdriver.

2. Install the device:

- Connect cables to corresponding connectors of the device. Description of the connectors is given in the section Design.
- Align the device with the bracket and secure the position by pulling it down.

4.2 False ceiling mounting procedure

It is not recommended to place WEP-30L/WEP-30L-Z from the inside of the false ceiling, as the metal frame causes signal multipath propagation and its attenuation when passing through the lattice of the false ceiling frame.



1 — metal bracket; 2 — Armstrong panel; 3 — plastic bracket; 4 — screws; 5 — device.
Figure 9 — Mounting the device on a false ceiling

1. Attach the metal and plastic brackets to the ceiling (Figure 9).

- Fasten the plastic bracket (**3**) on false ceiling with the metal bracket (**1**) in the following order: metal bracket -> Armstrong panel -> plastic bracket.
- In the Armstrong panel, make a hole with the the size of the metal bracket. Run the wires through this hole.
- Align the holes on the metal bracket, Armstrong panel and plastic bracket. Next, align the screw holes on the plastic bracket with the same holes on the metal bracket. Use a screwdriver to fix brackets with screws.

2. Install the device.

- Connect cables to corresponding connectors of the device. Description of the connectors is given in the section Design.
- Align the device with the plastic bracket and secure the position by turning the device clockwise.

4.3 Removing the device from the bracket

To remove the device from the bracket:

1. Pull the device up (Figure 8).
2. Remove the device.

5 Device management via the web interface

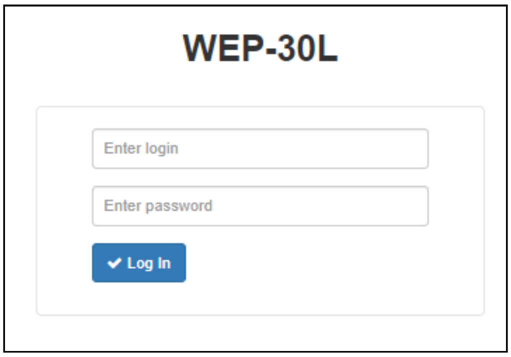
5.1 Getting started

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

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

> ✓ Factory IP address: 192.168.1.10, subnet mask: 255.255.255.0. By default, the device is capable to obtain an IP address via DHCP.

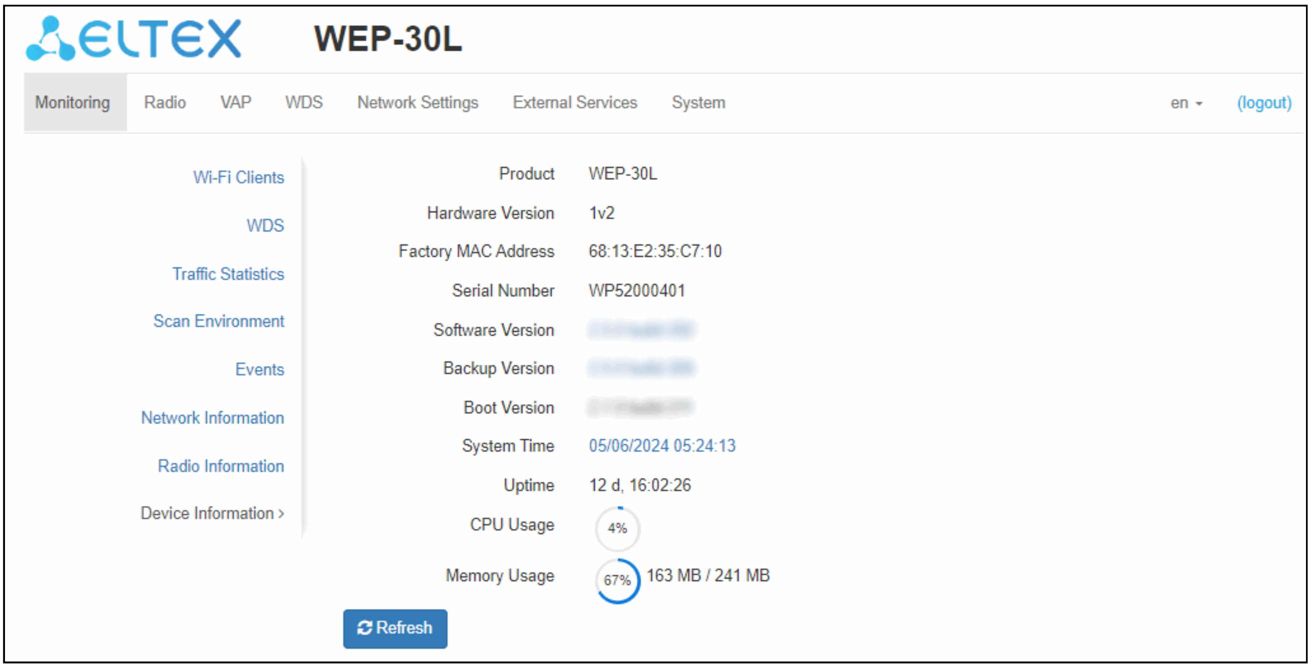
When the device is successfully detected, username and password request page will be shown in the browser window. As an example, this manual shows the web interface of WEP-30L. The only difference between the WEP-30L and WEP-30L-Z web interfaces is the presence of the Z-Wave tab, which is available for WEP-30L-Z only. A description of this tab will be given in the “Z-Wave” menu section.



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

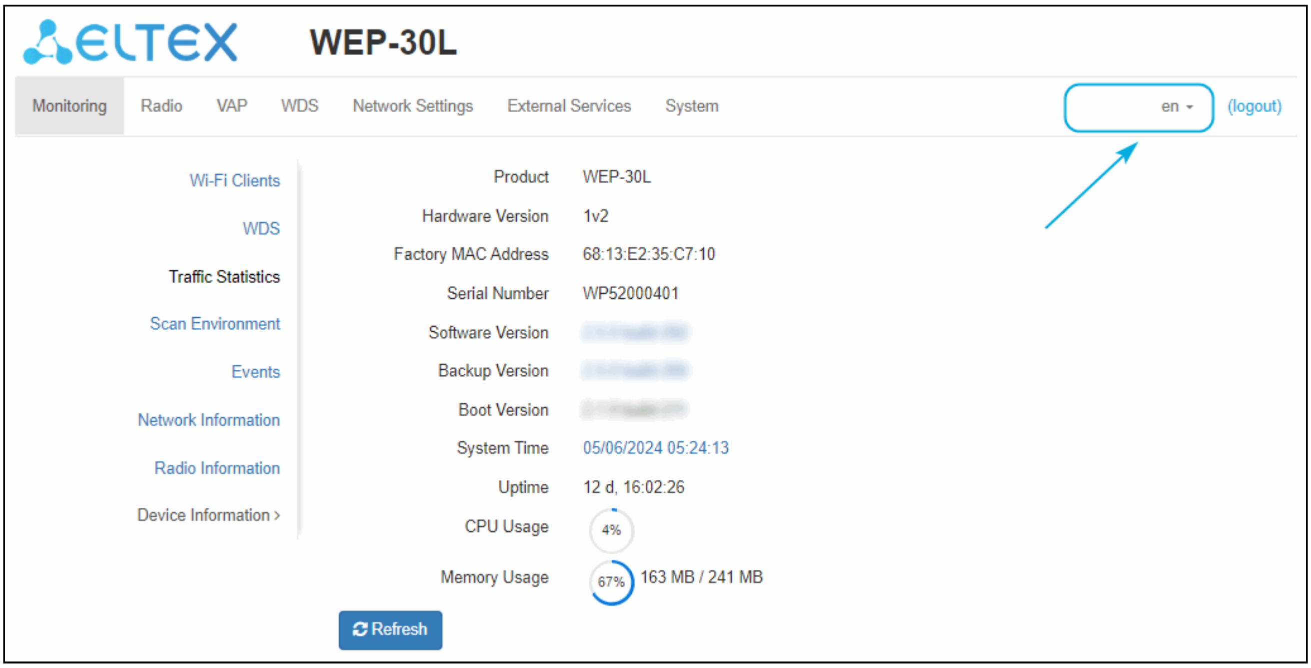
> ✓ Factory settings: login: *admin*, password: *password*.

4. Click the “Log in” button. A menu for monitoring the device status will open in a browser window.



Product	WEP-30L
Hardware Version	1v2
Factory MAC Address	68:13:E2:35:C7:10
Serial Number	WP52000401
Software Version	[redacted]
Backup Version	[redacted]
Boot Version	[redacted]
System Time	05/06/2024 05:24:13
Uptime	12 d, 16:02:26
CPU Usage	4%
Memory Usage	67% 163 MB / 241 MB

5. If necessary, select the information display language. Russian and English languages are available for web interface.



Product WEP-30L

Hardware Version 1v2

Factory MAC Address 68:13:E2:35:C7:10

Serial Number WP52000401

Software Version [redacted]

Backup Version [redacted]

Boot Version [redacted]

System Time 05/06/2024 05:24:13

Uptime 12 d, 16:02:26

CPU Usage 4%

Memory Usage 67% 163 MB / 241 MB

5.2 Applying configuration and discarding changes

1. Applying configuration

Clicking 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.

The WEP-30L/WEP-30L-Z web interface has a visual indication of the current status of the setting applying process (Table 6).

Table 6 — 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	The ✓ icon in the tab name indicates about successful saving and application of the settings.

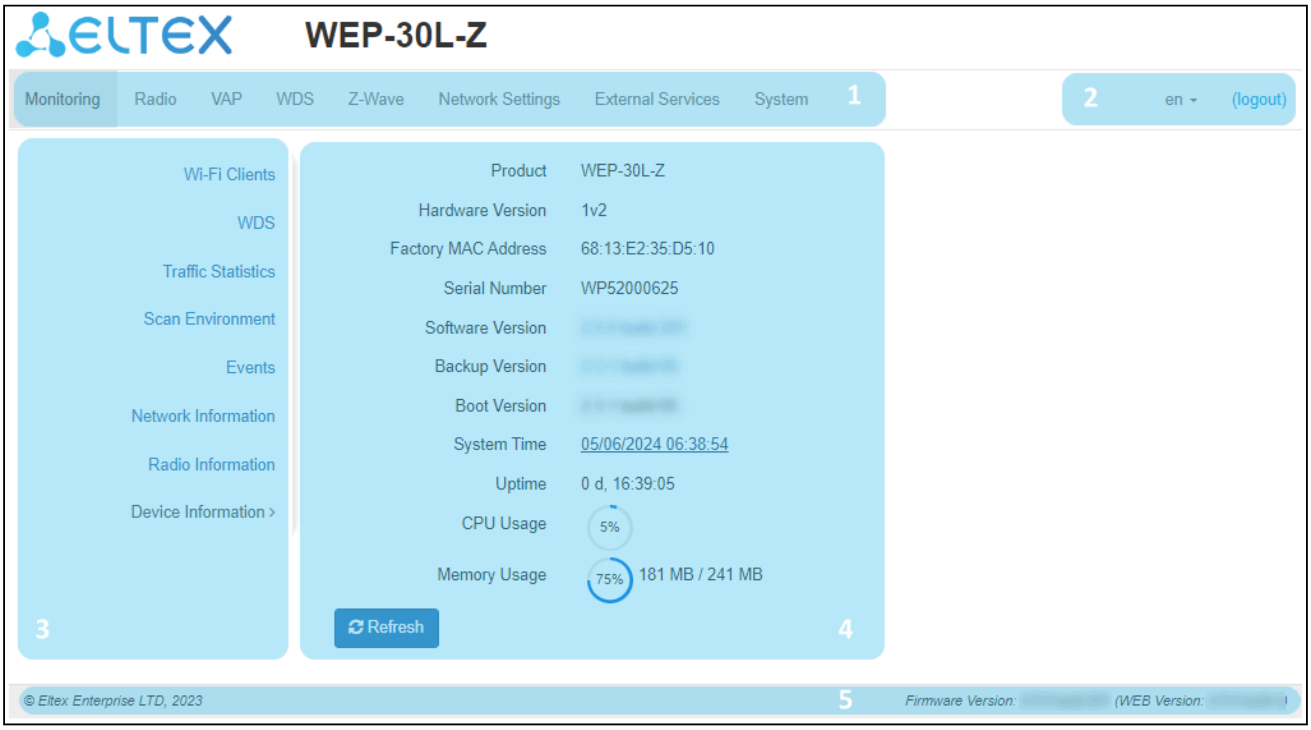
2. Discarding changes

The changes can be discarded only before clicking the "Apply" button. If you click the "Apply" button, all the changed parameters will be applied and saved to device memory. After clicking the "Apply" button, return to the previous settings will not be possible.

The button for discarding changes appears as follows: ✖ Cancel .

5.3 Web interface basic elements

Navigation elements of the web interface are shown in the figure below.



Product WEP-30L-Z
Hardware Version 1v2
Factory MAC Address 68:13:E2:35:D5:10
Serial Number WP52000625
Software Version [redacted]
Backup Version [redacted]
Boot Version [redacted]
System Time 05/06/2024 06:38:54
Uptime 0 d, 16:39:05
CPU Usage 5%
Memory Usage 75% 181 MB / 241 MB

© Eltex Enterprise LTD, 2023 Firmware Version: [redacted] (WEB Version: [redacted]

User interface window is divided into five general areas:

1. Menu tabs categorize the submenu tabs: **Monitoring, Radio, VAP, WDS, Z-Wave (for WEP-30L-Z only), Network Settings, External Services, System.**
2. Interface language selection and Logout button designed to end a session in the web interface under a given user.
3. Submenu tabs allow one to control settings field.
4. Device configuration field displays data and configuration.
5. Information field displays current firmware version.

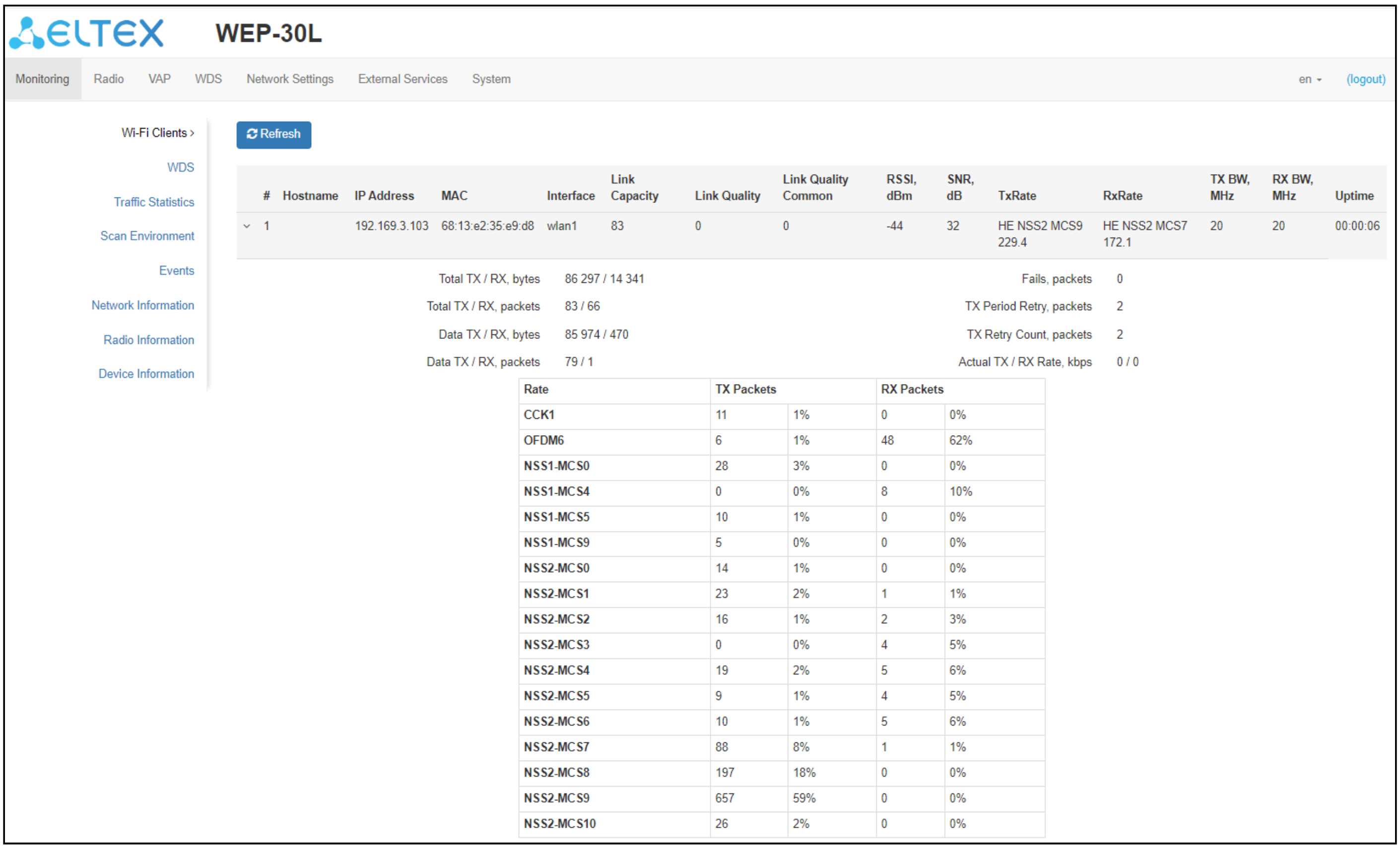
5.4 “Monitoring” menu

In the **“Monitoring”** menu, the current system state can be viewed.

5.4.1 “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, click “Refresh”.



#	Hostname	IP Address	MAC	Interface	Link Capacity	Link Quality	Link Quality Common	RSSI, dBm	SNR, dB	TxRate	RxRate	TX BW, MHz	RX BW, MHz	Uptime
1		192.169.3.103	68:13:e2:35:e9:d8	wlan1	83	0	0	-44	32	HE NSS2 MCS9 229.4	HE NSS2 MCS7 172.1	20	20	00:00:06

Total TX / RX, bytes	86 297 / 14 341	Fails, packets	0
Total TX / RX, packets	83 / 66	TX Period Retry, packets	2
Data TX / RX, bytes	85 974 / 470	TX Retry Count, packets	2
Data TX / RX, packets	79 / 1	Actual TX / RX Rate, kbps	0 / 0

Rate	TX Packets		RX Packets	
CCK1	11	1%	0	0%
OFDM6	6	1%	48	62%
NSS1-MCS0	28	3%	0	0%
NSS1-MCS4	0	0%	8	10%
NSS1-MCS5	10	1%	0	0%
NSS1-MCS9	5	0%	0	0%
NSS2-MCS0	14	1%	0	0%
NSS2-MCS1	23	2%	1	1%
NSS2-MCS2	16	1%	2	3%
NSS2-MCS3	0	0%	4	5%
NSS2-MCS4	19	2%	5	6%
NSS2-MCS5	9	1%	4	5%
NSS2-MCS6	10	1%	5	6%
NSS2-MCS7	88	8%	1	1%
NSS2-MCS8	197	18%	0	0%
NSS2-MCS9	657	59%	0	0%
NSS2-MCS10	26	2%	0	0%

- *№* — number of the connected device in the list;
- *Hostname* — network name of the device;
- *IP address* — IP address of the connected device;
- *MAC* — MAC address of the connected device;
- *Interface* — WEP-30L/WEP-30L-Z interaction interface with the connected device;
- *Link Capacity* — parameter that displays the efficiency of modulation on the transmission used by an access point. It is calculated based on the number of packets transmitted to the client on each modulation, 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 on the modulation nss1mcs0 for a client with MIMO 3×3 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;

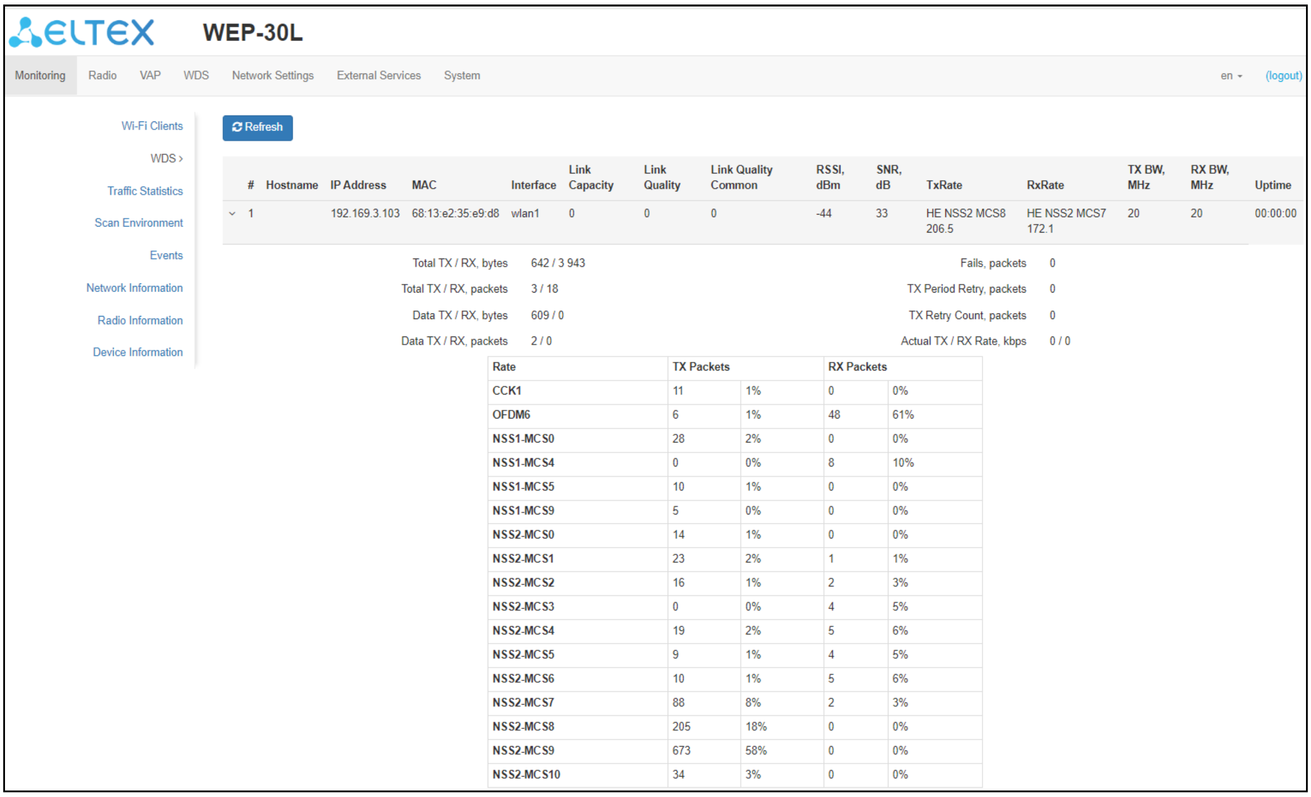
- *Link Quality Common* — parameter that displays the status of the link to the client, calculated based on the number of retransmit packets sent to the client. The maximum value is 100% (all transmitted packets were sent on the first attempt), the minimum value is 0% (no packets were successfully sent 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 time.

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

5.4.2 “WDS” submenu

The **“WDS”** submenu displays information about the status of WEP-30L/WEP-30L-Z connected via WDS.



	#	Hostname	IP Address	MAC	Interface	Link Capacity	Link Quality	Link Quality Common	RSSI, dBm	SNR, dB	TxRate	RxRate	TX BW, MHz	RX BW, MHz	Uptime
˅	1		192.169.3.103	68:13:e2:35:e9:d8	wlan1	0	0	0	-44	33	HE NSS2 MCS8 206.5	HE NSS2 MCS7 172.1	20	20	00:00:00

Total TX / RX, bytes	642 / 3 943	Fails, packets	0
Total TX / RX, packets	3 / 18	TX Period Retry, packets	0
Data TX / RX, bytes	609 / 0	TX Retry Count, packets	0
Data TX / RX, packets	2 / 0	Actual TX / RX Rate, kbps	0 / 0

Rate	TX Packets		RX Packets	
CCK1	11	1%	0	0%
OFDM6	6	1%	48	61%
NSS1-MCS0	28	2%	0	0%
NSS1-MCS4	0	0%	8	10%
NSS1-MCS5	10	1%	0	0%
NSS1-MCS9	5	0%	0	0%
NSS2-MCS0	14	1%	0	0%
NSS2-MCS1	23	2%	1	1%
NSS2-MCS2	16	1%	2	3%
NSS2-MCS3	0	0%	4	5%
NSS2-MCS4	19	2%	5	6%
NSS2-MCS5	9	1%	4	5%
NSS2-MCS6	10	1%	5	6%
NSS2-MCS7	88	8%	2	3%
NSS2-MCS8	205	18%	0	0%
NSS2-MCS9	673	58%	0	0%
NSS2-MCS10	34	3%	0	0%

- *№* — number of the connected device in the list;
- *Hostname* — network name of the device;
- *IP address* — IP address of the connected device;
- *MAC* — MAC address of the connected device;
- *Interface* — WEP-30L/WEP-30L-Z interaction interface with the connected device;
- *Link Capacity* — parameter that displays the efficiency of modulation on the transmission used by an access point. It is calculated based on the number of packets transmitted to the client on each modulation, 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 on the modulation nss1mcs0 for a client with MIMO 3×3 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* — connection time.

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

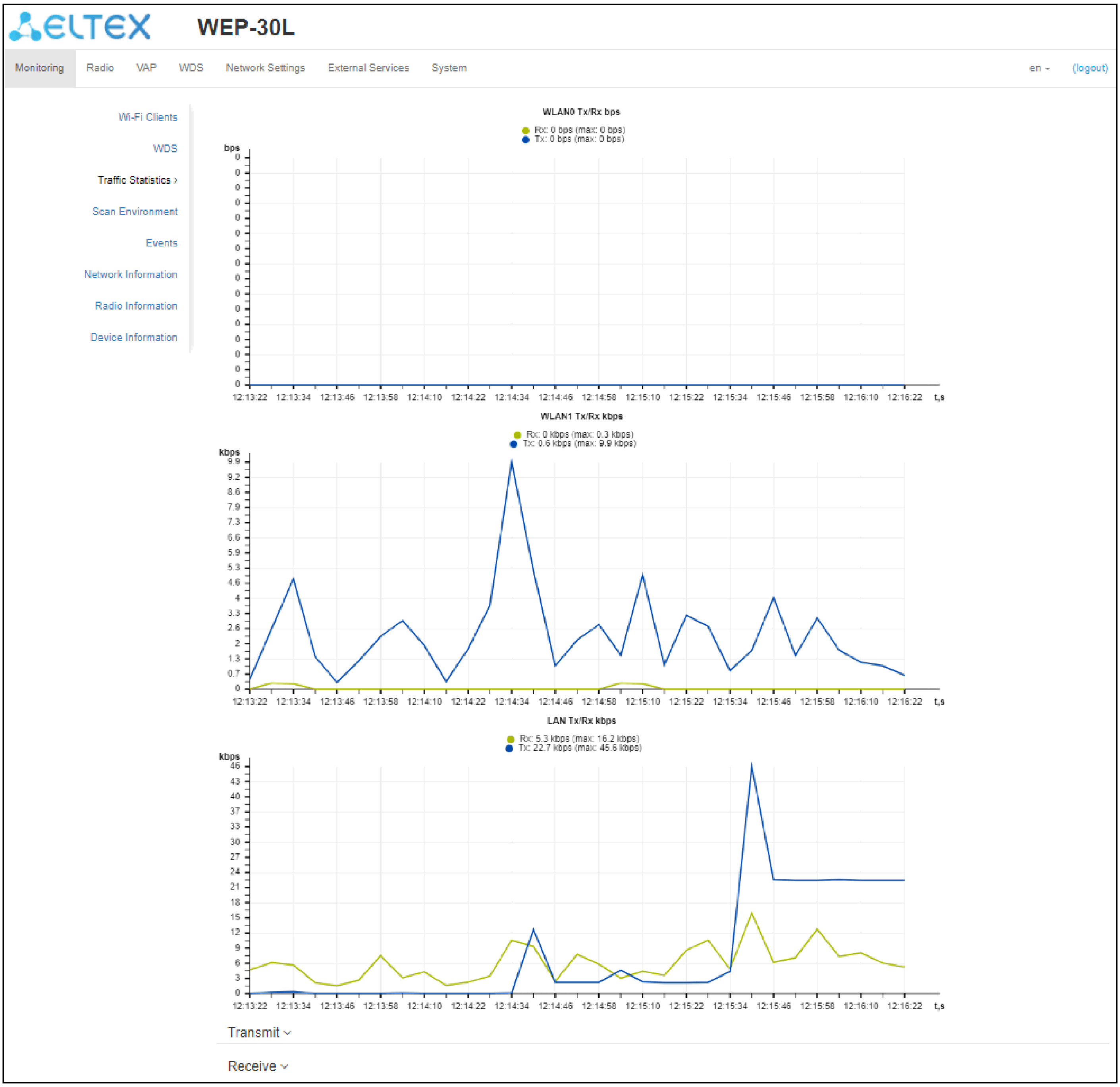
- *Total TX/RX, bytes* — number of bytes sent/received on the connected device;
- *Total TX/RX, packets* — number of packets sent/received on the connected device;
- *Data TX/RX, bytes* — number of data bytes sent/received on the connected device;
- *Data TX/RX, packets* — number of data packets sent/received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

5.4.3 “Traffic Statistics” submenu

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

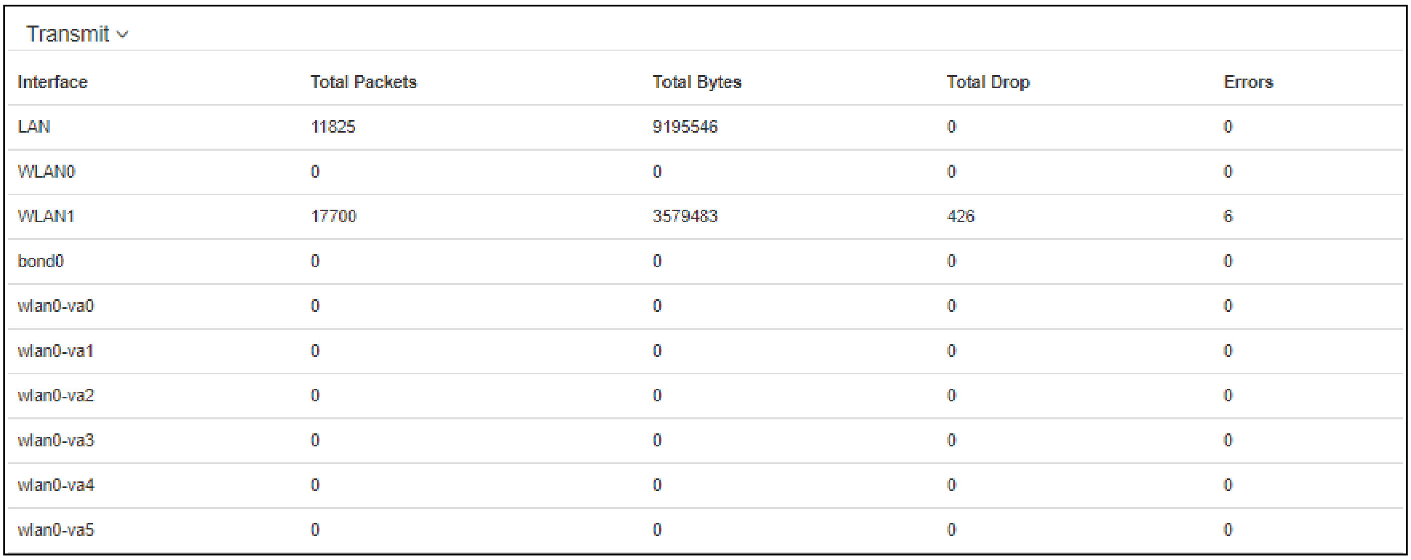
The LAN Tx/Rx diagram shows the speed of the transmitted/received traffic via Ethernet interface of the access point for the last 3 minutes. The graph is automatically updated every 6 seconds.

The WLAN0 and WLAN1 Tx/Rx graphs show the rate of transmitted/received traffic via Radio 2.4 GHz and Radio 5 GHz interfaces for the last 3 minutes. The graph is automatically updated every 6 seconds.



"Transmit" table description:

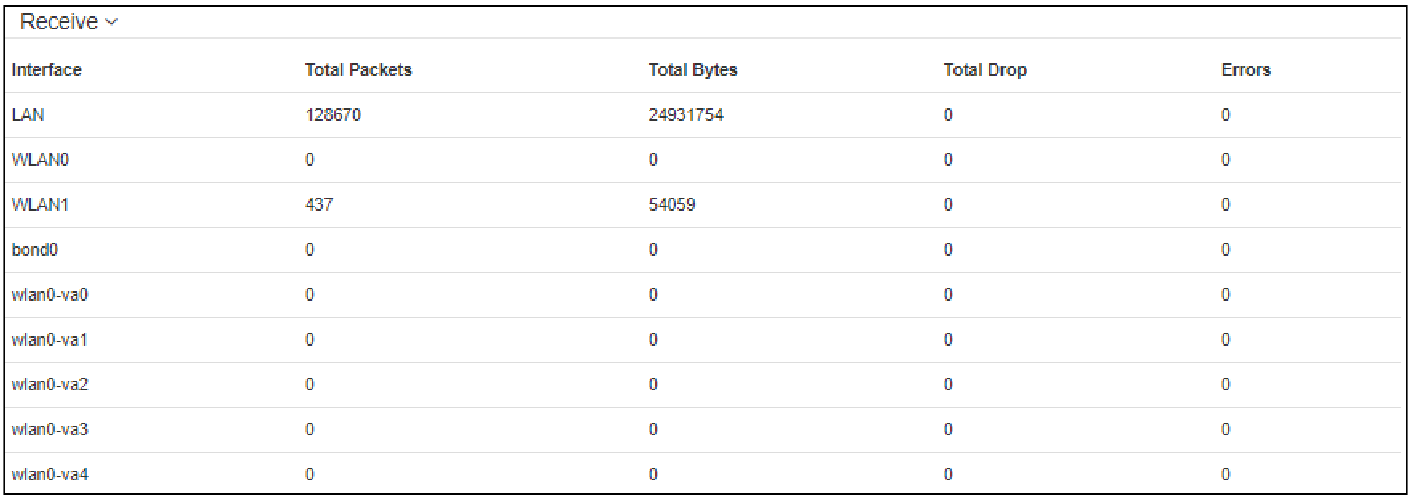
- *Interface* — name of the interface;
- *Total packets* — number of successfully sent packets;
- *Total bytes* — number of successfully sent bytes;
- *Total drop* — number of rejected packets;
- *Errors* — number of errors.



Interface	Total Packets	Total Bytes	Total Drop	Errors
LAN	11825	9195546	0	0
WLAN0	0	0	0	0
WLAN1	17700	3579483	426	6
bond0	0	0	0	0
wlan0-va0	0	0	0	0
wlan0-va1	0	0	0	0
wlan0-va2	0	0	0	0
wlan0-va3	0	0	0	0
wlan0-va4	0	0	0	0
wlan0-va5	0	0	0	0

"Receive" table description:

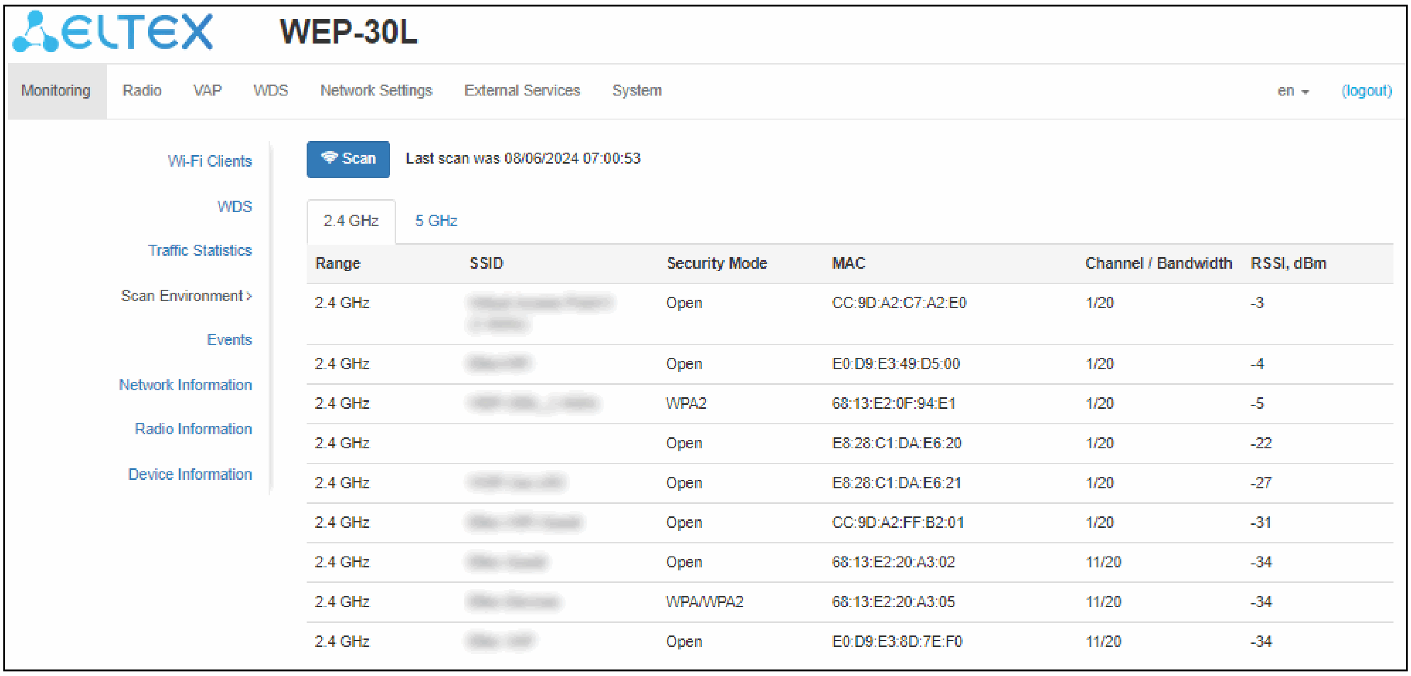
- *Interface* — name of the interface;
- *Total packets* — number of successfully received packets;
- *Total bytes* — number of successfully received bytes;
- *Total drop* — number of rejected packets;
- *Errors* — number of errors.



Interface	Total Packets	Total Bytes	Total Drop	Errors
LAN	128670	24931754	0	0
WLAN0	0	0	0	0
WLAN1	437	54059	0	0
bond0	0	0	0	0
wlan0-va0	0	0	0	0
wlan0-va1	0	0	0	0
wlan0-va2	0	0	0	0
wlan0-va3	0	0	0	0
wlan0-va4	0	0	0	0

5.4.4 “Scan Environment” submenu

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



Last scan was 08/06/2024 07:00:53

Range	SSID	Security Mode	MAC	Channel / Bandwidth	RSSI, dBm
2.4 GHz	[redacted]	Open	CC:9D:A2:C7:A2:E0	1/20	-3
2.4 GHz	[redacted]	Open	E0:D9:E3:49:D5:00	1/20	-4
2.4 GHz	[redacted]	WPA2	68:13:E2:0F:94:E1	1/20	-5
2.4 GHz		Open	E8:28:C1:DA:E6:20	1/20	-22
2.4 GHz	[redacted]	Open	E8:28:C1:DA:E6:21	1/20	-27
2.4 GHz	[redacted]	Open	CC:9D:A2:FF:B2:01	1/20	-31
2.4 GHz	[redacted]	Open	68:13:E2:20:A3:02	11/20	-34
2.4 GHz	[redacted]	WPA/WPA2	68:13:E2:20:A3:05	11/20	-34
2.4 GHz	[redacted]	Open	E0:D9:E3:8D:7E:F0	11/20	-34

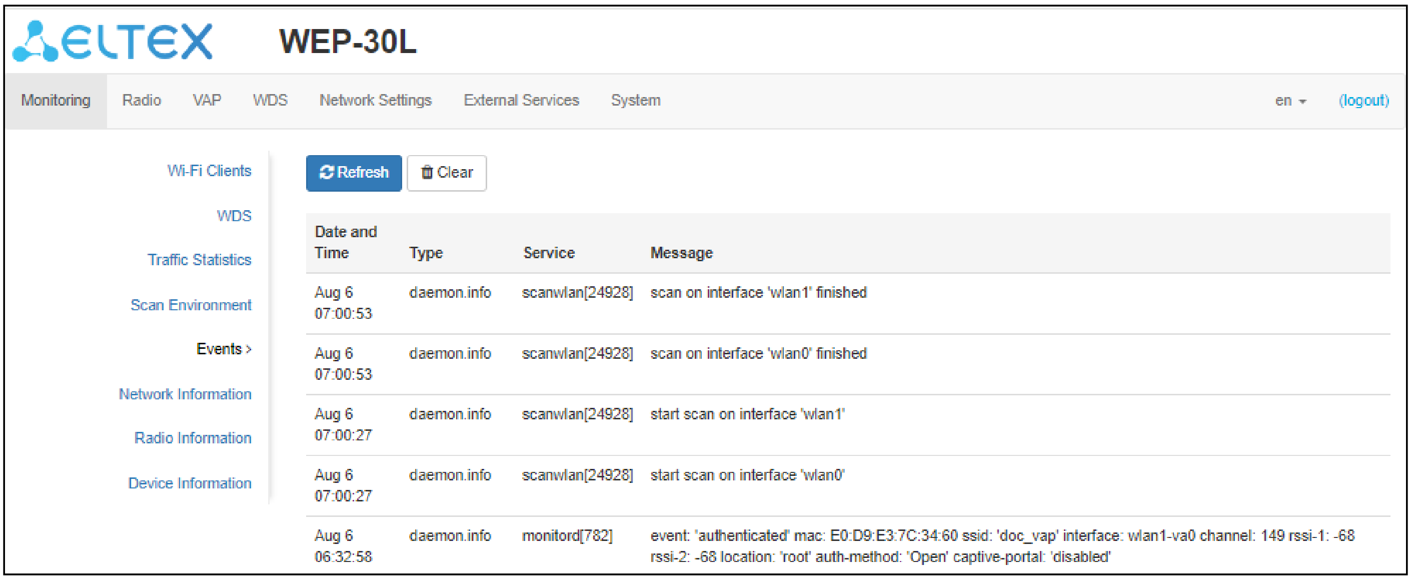
To start the scanning process, click the “Scan” button. After the scan is completed, a list of detected access points and information about them will appear:

- *Last scan was...* — date and time of the last scan;
- *Range* — specifies the range of 2.4 GHz or 5 GHz in 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.

✓ While scanning the environment, the device radio interface will be disabled, which will make it impossible to transfer data to Wi-Fi clients during scanning.

5.4.5 “Events” submenu

In the **“Events”** submenu, it is possible to view a list of real-time informational messages which contains the following information:



Date and Time	Type	Service	Message
Aug 6 07:00:53	daemon.info	scanwlan[24928]	scan on interface 'wlan1' finished
Aug 6 07:00:53	daemon.info	scanwlan[24928]	scan on interface 'wlan0' finished
Aug 6 07:00:27	daemon.info	scanwlan[24928]	start scan on interface 'wlan1'
Aug 6 07:00:27	daemon.info	scanwlan[24928]	start scan on interface 'wlan0'
Aug 6 06:32:58	daemon.info	monitord[782]	event: 'authenticated' mac: E0:D9:E3:7C:34:60 ssid: 'doc_vap' interface: wlan1-va0 channel: 149 rssi-1: -68 rssi-2: -68 location: 'root' auth-method: 'Open' captive-portal: 'disabled'

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

Table 7 — Description of event severity levels

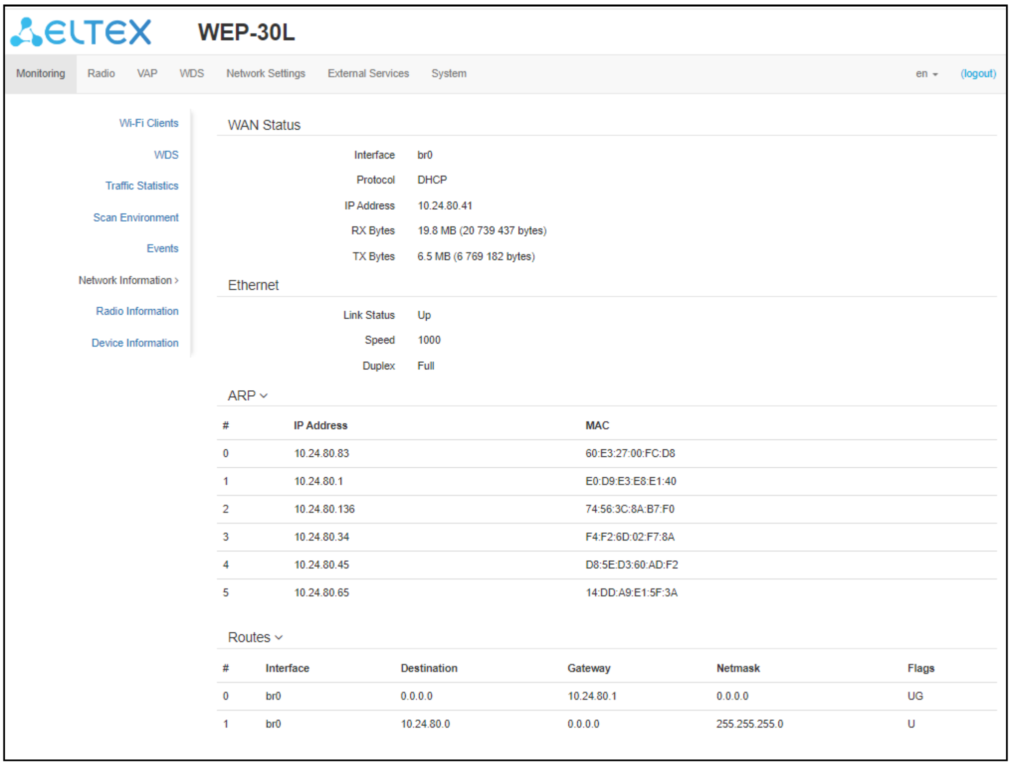
Level	Message severity level	Description
0	Emergency	A critical error has occurred in the system, the system may not work properly.
1	Alert	Immediate intervention is required.
2	Critical	A critical error has occurred in the system.
3	Error	An error has occurred in the system.
4	Warning	Warning, non-emergency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

To receive new messages in the event log, click "Refresh".

If necessary, all old messages can be deleted from the log by clicking on the “Clear” button.

5.4.6 “Network Information” submenu

In the **“Network Information”** submenu, general network settings of the device can be viewed.



WAN Status

Interface	br0
Protocol	DHCP
IP Address	10.24.80.41
RX Bytes	19.8 MB (20 739 437 bytes)
TX Bytes	6.5 MB (6 769 182 bytes)

Ethernet

Link Status	Up
Speed	1000
Duplex	Full

ARP

#	IP Address	MAC
0	10.24.80.83	60:E3:27:00:FC:D8
1	10.24.80.1	E0:D9:E3:E8:E1:40
2	10.24.80.136	74:56:3C:8A:B7:F0
3	10.24.80.34	F4:F2:6D:02:F7:8A
4	10.24.80.45	D8:5E:D3:60:AD:F2
5	10.24.80.65	14:DD:A9:E1:5F:3A

Routes

#	Interface	Destination	Gateway	Netmask	Flags
0	br0	0.0.0.0	10.24.80.1	0.0.0.0	UG
1	br0	10.24.80.0	0.0.0.0	255.255.255.0	U

<u>WAN Status</u>:

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

<u>Ethernet</u>:

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

<u>ARP:</u>
The ARP table contains mapping information between the IP and MAC addresses of neighboring network devices:

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

<u>Routes</u>:

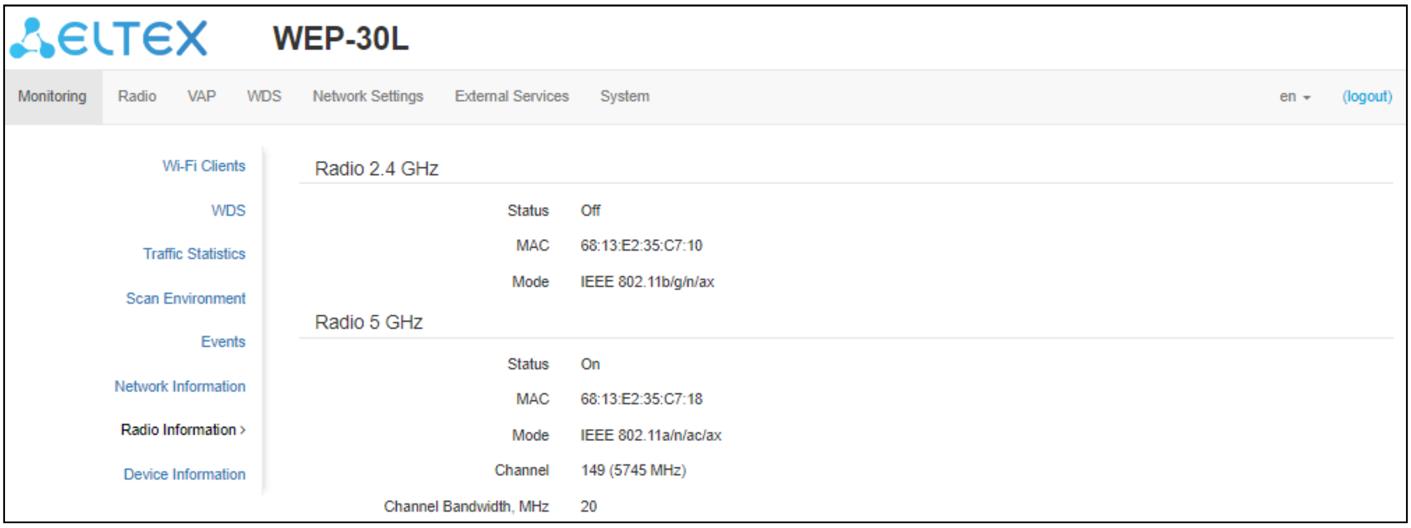
- *Interface* — name of the bridge interface;
- *Destination* — IP address of destination host or subnet that the route is established to;
- *Gateway* — IP address of the gateway through which access to the Destination is carried out;
- *Netmask* — subnet mask;
- *Flags* — certain route characteristics.

The following flag values exist:

- **U** — means that the route is created and passable;
- **H** — indicates 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 for the following packets intended for the same destination;
- **M** — means that the route was modified — likely by a dynamic routing protocol running on a local system with the “mod” parameter applied;
- **A** — points to a buffered route to which an entry in the ARP table corresponds;
- **C** — means that the route source is the core routing buffer;
- **L** — indicates that the destination of the route is one of the addresses of this computer. Such “local routes” exist in the routing buffer only;
- **B** — means that the route destination is a broadcasting address. Such “broadcast routes” exist in the routing buffer only;
- **I** — indicates that the route is connected to a ring (loopback) interface for a purpose other than to access the ring network. Such “internal routes” exist in the routing buffer only;
- **!** — means that datagrams sent to this address will be rejected by the system.

5.4.7 “Radio Information” submenu

In the **“Radio Information”** submenu, the current status of WEP-30L radio interfaces is displayed.



Radio 2.4 GHz

Status	Off
MAC	68:13:E2:35:C7:10
Mode	IEEE 802.11b/g/n/ax

Radio 5 GHz

Status	On
MAC	68:13:E2:35:C7:18
Mode	IEEE 802.11a/n/ac/ax
Channel	149 (5745 MHz)
Channel Bandwidth, MHz	20

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”:

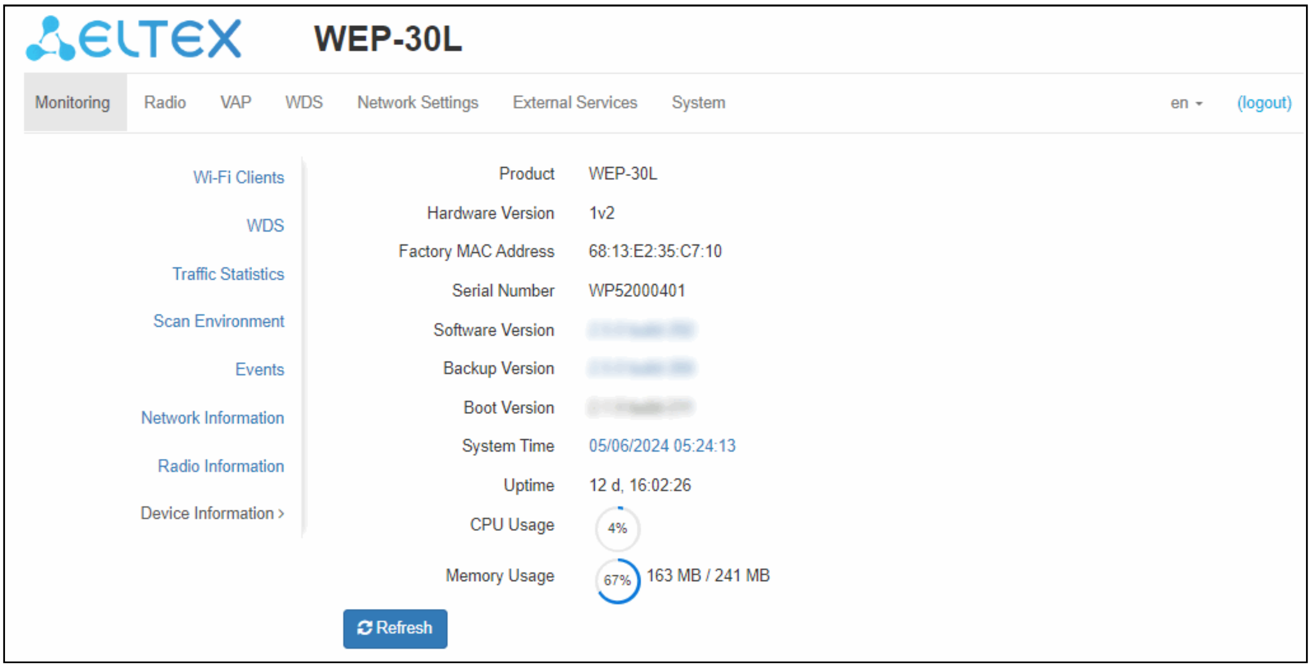
- *Status* — radio interface state;
- *MAC* — radio interface MAC address;
- *Mode* — radio interface operation mode according to IEEE 802.11 standards.

“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.

5.4.8 “Device Information” submenu

The **“Device Information”** submenu displays main WEP-30L parameters.



Product WEP-30L
Hardware Version 1v2
Factory MAC Address 68:13:E2:35:C7:10
Serial Number WP52000401
Software Version [redacted]
Backup Version [redacted]
Boot Version [redacted]
System Time 05/06/2024 05:24:13
Uptime 12 d, 16:02:26
CPU Usage 4%
Memory Usage 67% 163 MB / 241 MB

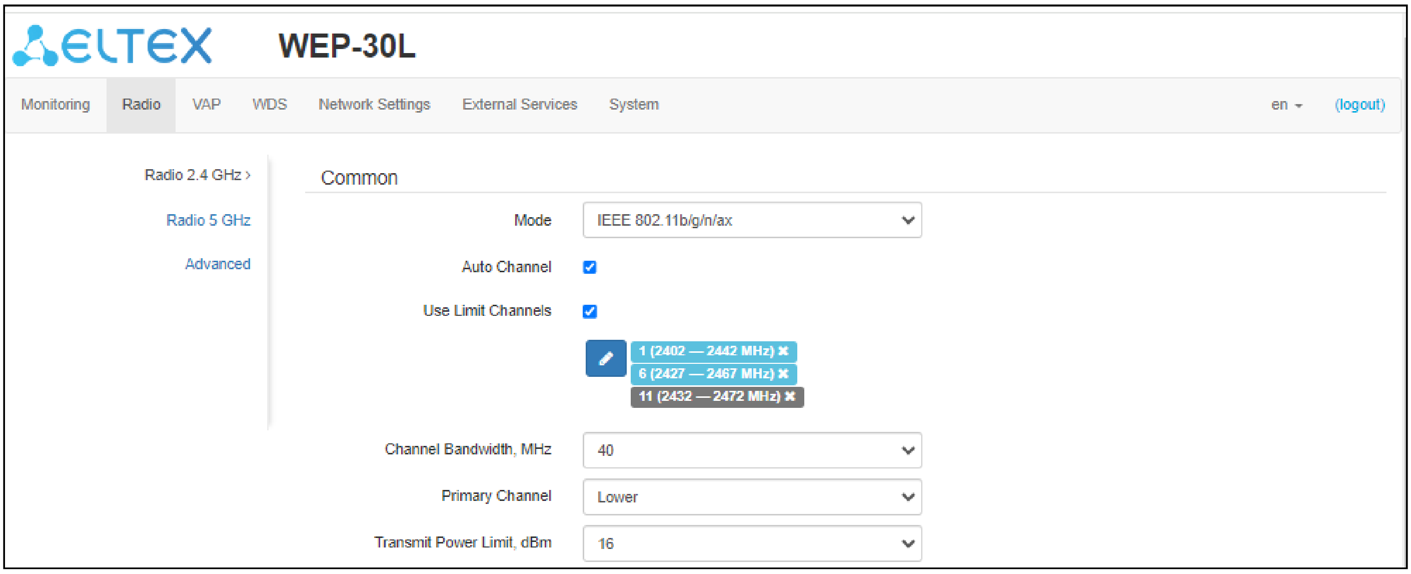
- *Product* — device model name;
- *Hardware Version* — device hardware version;
- *Factory MAC Address* — device WAN interface MAC address, factory set;
- *Serial Number* — device serial number, factory set;
- *Software Version* — device software version;
- *Backup Version* — previously installed firmware version;
- *Boot Version* — device firmware boot version;
- *System Time* — current time and date, set in the system;
- *Uptime* — operating time since the last time the device was turned on or rebooted;
- *CPU Usage* — average percentage of CPU load over the last 5 seconds;
- *Memory Usage* — percentage of device RAM usage.

5.5 “Radio” menu

In the **“Radio”** menu, the wireless interface can be configured.

5.5.1 “Radio 2.4 GHz” submenu

In the **“Radio 2.4 GHz”** submenu, the main parameters of the radio interface of the device operating in the 2.4 GHz band can be configured.



Common

Mode: IEEE 802.11b/g/n/ax

Auto Channel: ☑

Use Limit Channels: ☑

1 (2402 — 2442 MHz) ✖
6 (2427 — 2467 MHz) ✖
11 (2432 — 2472 MHz) ✖

Channel Bandwidth, MHz: 40

Primary Channel: Lower

Transmit Power Limit, dBm: 16

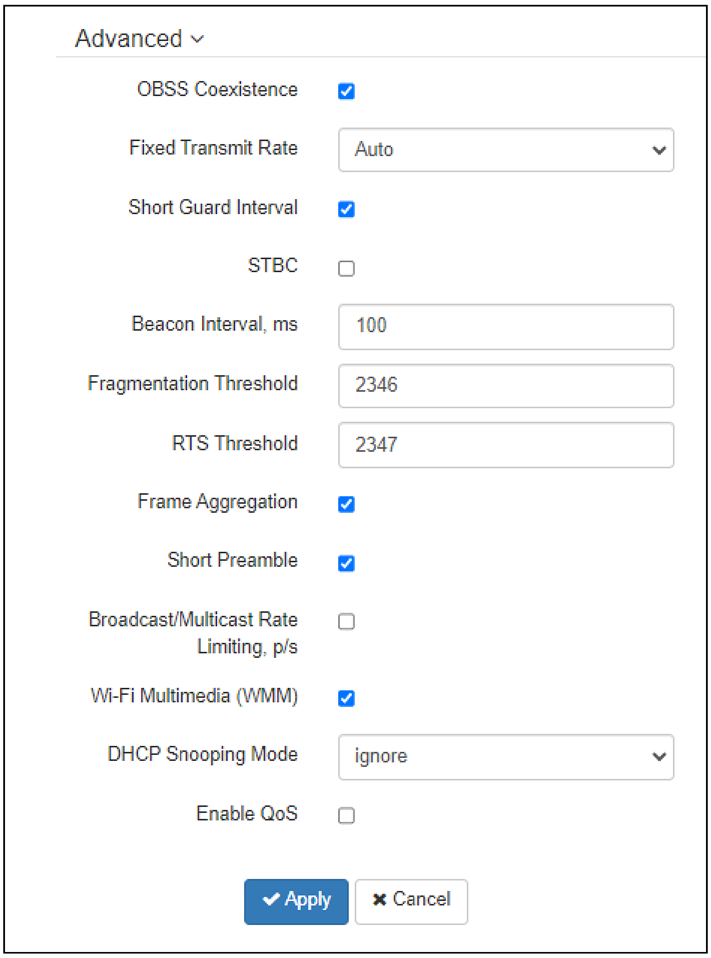
- *Mode* — interface operation mode according to the following standards:
  - IEEE 802.11ax;
  - IEEE 802.11n/ax;
  - IEEE 802.11b/g;
  - IEEE 802.11b/g/n;
  - IEEE 802.11b/g/n/ax.
- *Auto Channel* — when checked, the device will automatically select the least congested radio channel for the Wi-Fi interface. Unchecking 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 band channels: 1–13;
- *Channel Bandwidth, MHz* — channel bandwidth, on which the access point operates. The parameter may take values 20 and 40 MHz;
- *Primary Channel* — 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* — primary channel will be the upper 20 MHz channel in the 40 MHz band;
  - *Lower* — primary channel will be the lower 20 MHz channel in the 40 MHz band.
- *Transmit Power Limit, dBm* — adjustment of the signal strength of the Wi-Fi transmitter in dBm. Accepts value from 0 to 16 dBm.

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 grey.

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 were 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, it is possible to configure advanced radio interface parameters of the device.



Advanced

OBSS Coexistence ☑

Fixed Transmit Rate: Auto

Short Guard Interval ☑

STBC □

Beacon Interval, ms: 100

Fragmentation Threshold: 2346

RTS Threshold: 2347

Frame Aggregation ☑

Short Preamble ☑

Broadcast/Multicast Rate Limiting, p/s □

Wi-Fi Multimedia (WMM) ☑

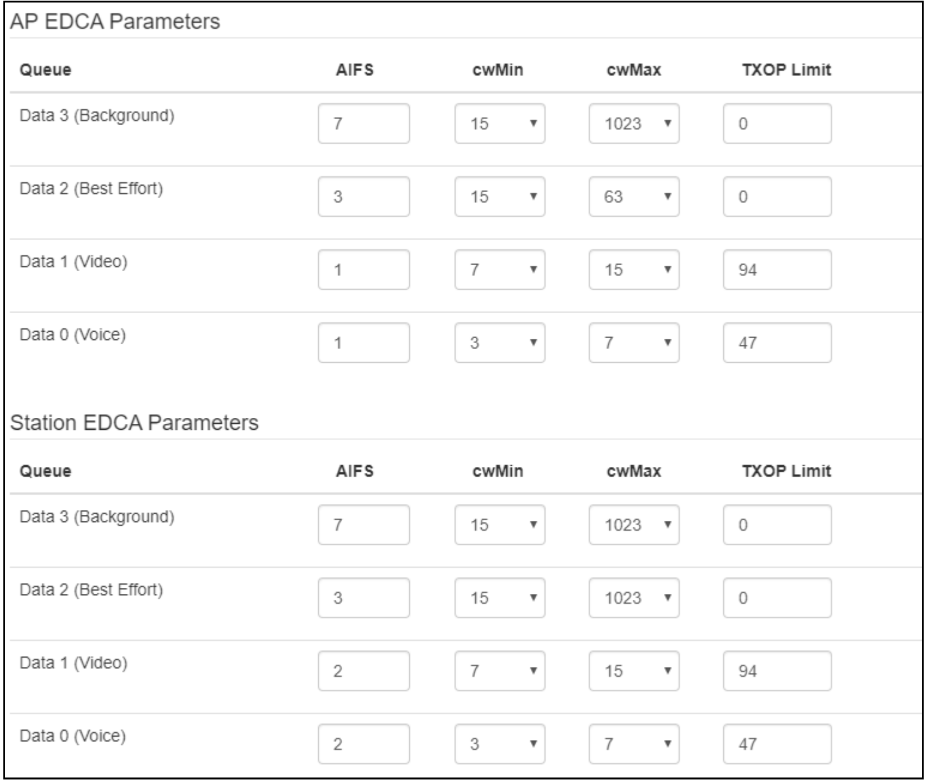
DHCP Snooping Mode: ignore

Enable QoS □

- *OBSS Coexistence* — automatic channel bandwidth reduction when the channel is loaded. When the flag is set, the mode is enabled;
- *Fixed Transmit Rate* — fixed wireless data rate, defined by the specifications of IEEE 802.11 standards;
- *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 Guard Interval;
- *STBC* — Space-Time Block Coding method dedicated to improve data transmission reliability. When checked, the device transmits one data flow through several antennas. When unchecked, the device does not transmit the same data flow through several antennas;
- *Beacon Interval, ms* — beacon frames transmission period. The frames are sent to detect access points on the air. 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* — specifies the number of bytes over which the Request to Send will be sent. Decreasing this value may improve the performance of the access point when there are a lot of connected clients. However this reduces general throughput of wireless network. The parameter takes values from 0 to 2347, by default: 2347;
- *Frame 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);
- *DHCP Snooping Mode*— selection of DHCP option 82 processing policy. Available values for selection:
  - *ignore* — option 82 processing is disabled. Default value;
  - *remove* — access point deletes the value of option 82;
  - *replace* — access point substitutes or replaces the value of option 82. When selecting this value to edit, the following parameters are opened:
    - *Option 82 CID format* — replacement of the CID parameter value, can take values:
      - *APMAC-SSID* — replacement of the CID parameter value to <MAC address of the access point>-<SSID name>. Default value;
      - *SSID* — replacement of the CID parameter value to SSID name, to which the client is connected;
      - *custom* — replacement of the CID parameter value to the value specified in the "Option 82 Unique CID";
        - *Option 82 Unique CID* — an arbitrary string of up to 52 characters that will be passed to the CID. If the parameter value is not set, the point will change the CID to the default value — APMAC-SSID.
    - *Option 82 RID format* — replacement of the RID parameter value, can take the following values:
      - *ClientMAC* — change the RID content to the MAC address of the client device. Default value;
      - *APMAC* — change the RID content to the MAC address of the access point;
      - *APdomain* — change the RID content to the domain in which the access point is located;
      - *custom* — change the RID content to the value specified in the "Option 82 Unique RID";
        - *Option 82 Unique RID* — an arbitrary string of up to 63 characters that will be passed to the RID. If the parameter value is not set, the point will change the RID to the default value — ClientMAC.
    - *MAC-address format* — selection of octet delimiters of the MAC address, which is transmitted in CID and RID:
      - *AA:BB:CC:DD:EE:FF* — the delimiter is a colon (:). Default value;
      - *AA-BB-CC-DD-EE-FF* — the delimiter is a dash (-).
- *Enable QoS* — when the flag is set, the setting of Quality of Service functions is available.

The following functions are available for quality assurance configuration:



AP EDCA Parameters

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

Station EDCA Parameters

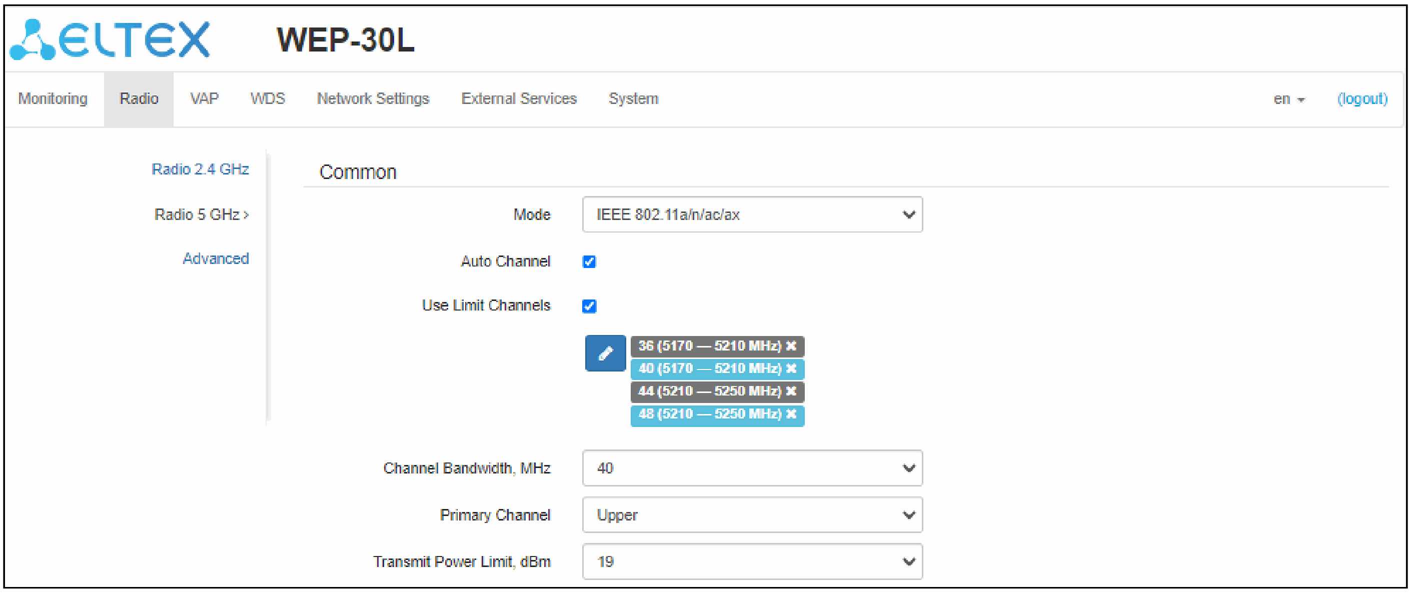
Queue	AIFS	cwMin	cwMax	TXOP Limit
Data 3 (Background)	7	15	1023	0
Data 2 (Best Effort)	3	15	1023	0
Data 1 (Video)	2	7	15	94
Data 0 (Voice)	2	3	7	47

- *AP EDCA parameters* — access point settings table (traffic is transmitted from the access point to the client):
  - *Queue* — predefined queues for various kinds of traffic:
    - *Data 3 (Background)* — low priority queue, high bandwidth (802.1p: cs1, cs2 priorities);
    - *Data 2 (Best Effort)* — middle priority queue, middle bandwidth and delay. Most of the traditional IP data is sent to this queue (802.1p: cs0, cs3 priorities);
    - *Data 1 (Video)* — high priority queue, minimal delay. In this queue, time-sensitive video data is automatically processed (802.1p: cs4, cs5 priorities);
    - *Data 0 (Voice)* — high priority queue, minimal delay. In this queue, time sensitive data is automatically processed, such as: VoIP, streaming video (802.1p: cs6, cs7 priorities).
  - *AIFS* — Arbitration Inter-Frame Spacing, defines the waiting time of data frames, measured in slots, takes values 1–255;
  - *cwMin* — 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* — 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 settings to non-volatile memory, click “Apply”. Click “Cancel” to discard the changes.

5.5.2 “Radio 5 GHz” submenu

In the **“Radio 5 GHz”** submenu, the main parameters of the radio interface of the device operating in the 5 GHz band can be configured.



Common

Mode: IEEE 802.11a/n/ac/ax

Auto Channel: ☑

Use Limit Channels: ☑

36 (5170 — 5210 MHz) ✖
40 (5170 — 5210 MHz) ✖
44 (5210 — 5250 MHz) ✖
48 (5210 — 5250 MHz) ✖

Channel Bandwidth, MHz: 40

Primary Channel: Upper

Transmit Power Limit, dBm: 19

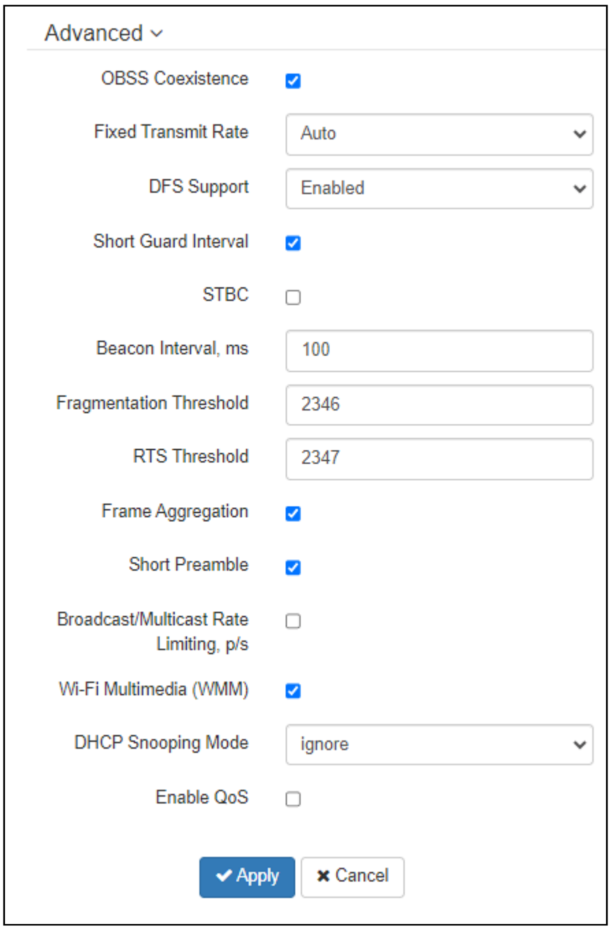
- *Mode* — select interface operation mode according to the following standards:
  - IEEE 802.11ax;
  - IEEE 802.11a/n/ac;
  - IEEE 802.11a/n/ac/ax.
- *Auto Channel* — when checked, the device will automatically select the least congested radio channel for the Wi-Fi interface. Removing the flag opens 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 band 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* — 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* — primary channel will be the upper 20 MHz channel in the 40 MHz band;
  - *Lower* — 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 0 and 19 dBm.

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, it is required to set “Channel Bandwidth” 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 grey.

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 were 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, it is possible to configure advanced radio interface parameters of the device.



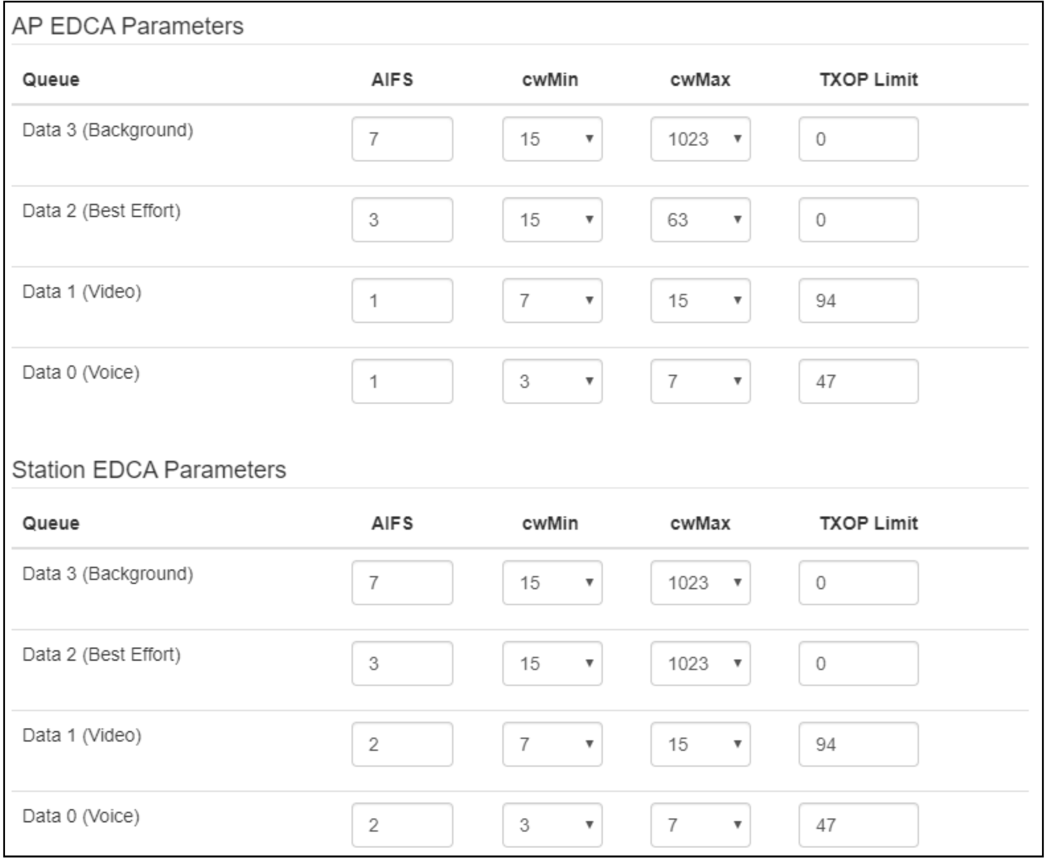
Advanced

OBSS Coexistence	☑
Fixed Transmit Rate	Auto
DFS Support	Enabled
Short Guard Interval	☑
STBC	☐
Beacon Interval, ms	100
Fragmentation Threshold	2346
RTS Threshold	2347
Frame Aggregation	☑
Short Preamble	☑
Broadcast/Multicast Rate Limiting, p/s	☐
Wi-Fi Multimedia (WMM)	☑
DHCP Snooping Mode	ignore
Enable QoS	☐

- *OBSS Coexistence* — automatic channel bandwidth reduction when the channel is loaded. When the flag is set, the mode is enabled;
- *Fixed Transmit Rate* — fixed wireless data rate, defined by the specifications of IEEE 802.11 standards;
- *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* — mechanism is disabled. DFS channels are not available for selection;
  - *Enabled* — mechanism is enabled;
  - *Forced* — 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 Guard Interval;
- *STBC* — Space-Time Block Coding method dedicated to improve data transmission reliability. When checked, the device transmits one data flow through several antennas. When unchecked, the device does not transmit the same 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* — specifies the number of bytes over which the Request to Send will be sent. Decreasing this value may improve the performance of the access point when there are a lot of connected clients. However this reduces general throughput of wireless network. The parameter takes values from 0 to 2347, by default: 2347;
- *Frame aggregation* — enables 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);
- *DHCP Snooping Mode*— selection of DHCP option 82 processing policy. Available values for selection:
    - *ignore* — option 82 processing is disabled. Default value;
    - *remove* — access point deletes the value of option 82;
    - *replace* — access point substitutes or replaces the value of option 82. When selecting this value to edit, the following parameters are opened:
        - *Option 82 CID format* — replacement of the CID parameter value, can take values:
            - *APMAC-SSID* — replacement of the CID parameter value to <MAC address of the access point>-<SSID name>. Default value;
            - *SSID* — replacement of the CID parameter value to SSID name, to which the client is connected;
            - *custom* — replacement of the CID parameter value to the value specified in the "Option 82 Unique CID";
                - *Option 82 Unique CID* — an arbitrary string of up to 52 characters that will be passed to the CID. If the parameter value is not set, the point will change the CID to the default value — APMAC-SSID.
        - *Option 82 RID format* — replacement of the RID parameter value, can take the following values:
            - *ClientMAC* — change the RID content to the MAC address of the client device. Default value;
            - *APMAC* — change the RID content to the MAC address of the access point;
            - *APdomain* — change the RID content to the domain in which the access point is located;
            - *custom* — change the RID content to the value specified in the "Option 82 Unique RID";
                - *Option 82 Unique RID* — arbitrary string of up to 63 characters that will be passed to the RID. If the parameter value is not set, the point will change the RID to the default value — ClientMAC.
        - *MAC-address format* — selection of octet delimiters of the MAC address, which is transmitted in CID and RID:
            - *AA:BB:CC:DD:EE:FF* — delimiter is a colon (:). Default value;
            - *AA-BB-CC-DD-EE-FF* — delimiter is a dash (-).
- *Enable QoS* — when the flag is set, the setting of Quality of Service functions is available.

The following functions are available for quality assurance configuration:



AP EDCA Parameters

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

Station EDCA Parameters

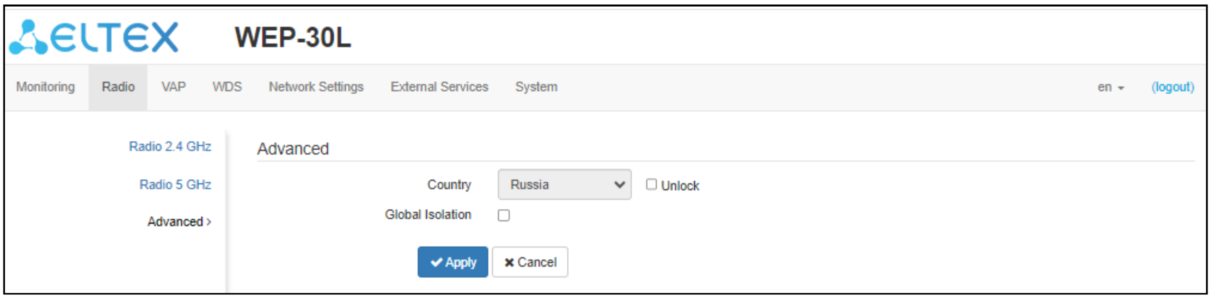
Queue	AIFS	cwMin	cwMax	TXOP Limit
Data 3 (Background)	7	15	1023	0
Data 2 (Best Effort)	3	15	1023	0
Data 1 (Video)	2	7	15	94
Data 0 (Voice)	2	3	7	47

- *AP EDCA parameters* — access point settings table (traffic is transmitted from the access point to the client):
  - *Queue* — predefined queues for various kinds of traffic:
    - *Data 3 (Background)* — low priority queue, high bandwidth (802.1p: cs1, cs2 priorities);
    - *Data 2 (Best Effort)* — middle priority queue, middle bandwidth and delay. Most of the traditional IP data is sent to this queue (802.1p: cs0, cs3 priorities);
    - *Data 1 (Video)* — high priority queue, minimal delay. In this queue, time-sensitive video data is automatically processed (802.1p: cs4, cs5 priorities);
    - *Data 0 (Voice)* — high priority queue, minimal delay. In this queue, time sensitive data is automatically processed, such as: VoIP, streaming video (802.1p: cs6, cs7 priorities).
  - *AIFS* — Arbitration Inter-Frame Spacing, defines the waiting time of data frames, measured in slots, takes values 1–255;
  - *cwMin* — 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* — 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 settings to non-volatile memory, click “Apply”. Click “Cancel” to discard the changes.

5.5.3 “Advanced” submenu

In the **“Advanced”** submenu, it is possible to configure advanced radio interface parameters of the device.



Advanced

Country: Russia □ Unlock

Global Isolation □

- *Country* — country of access point operation. Select the “Unlock” checkbox to change a country. Depending on the selected value the channel bandwidth and transmit power limit restrictions will be applied. The list of available frequency channels depends on the selected country, which affects the automatic channel selection in the Channel = Auto mode. If the subscriber equipment is licensed for use in a different region, probably, a connection with the access point will not be established.

> Local country regulations settings, including operation within legal frequency channels and output power, is the installer's responsibility.

> Selecting the wrong region may result in compatibility issues with different client devices.

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

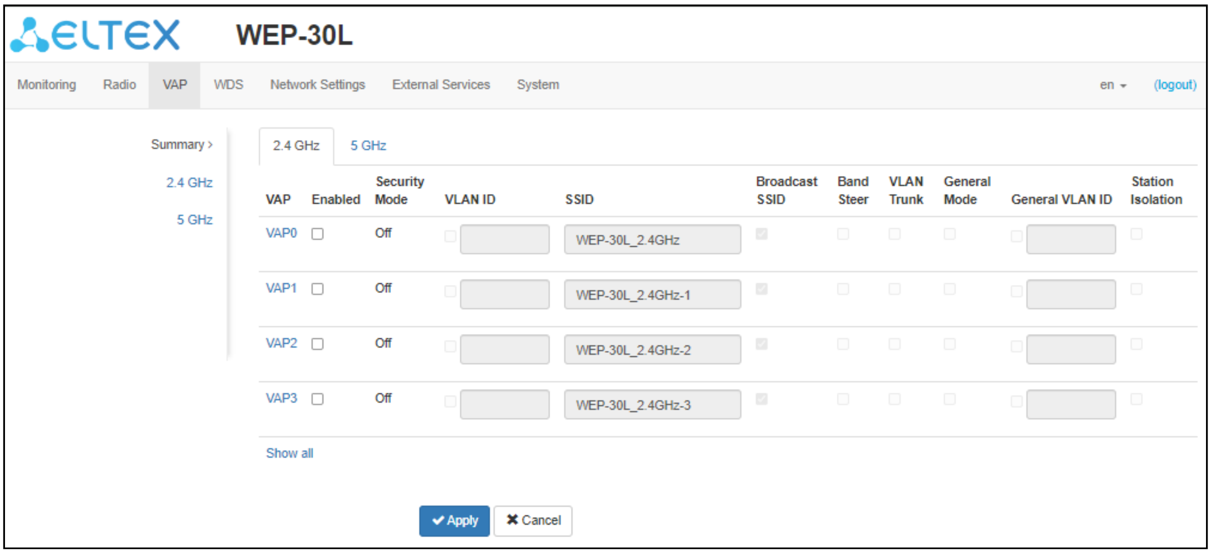
To apply a new configuration and save settings to non-volatile memory, click “Apply”. Click “Cancel” to discard the changes.

5.6 “VAP” menu

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

5.6.1 “Summary” submenu

The **“Summary”** submenu displays the settings of all VAPs on Radio 2.4 GHz and Radio 5 GHz radio interfaces. The settings of each virtual access point can be viewed in sections of VAP0–VAP6.

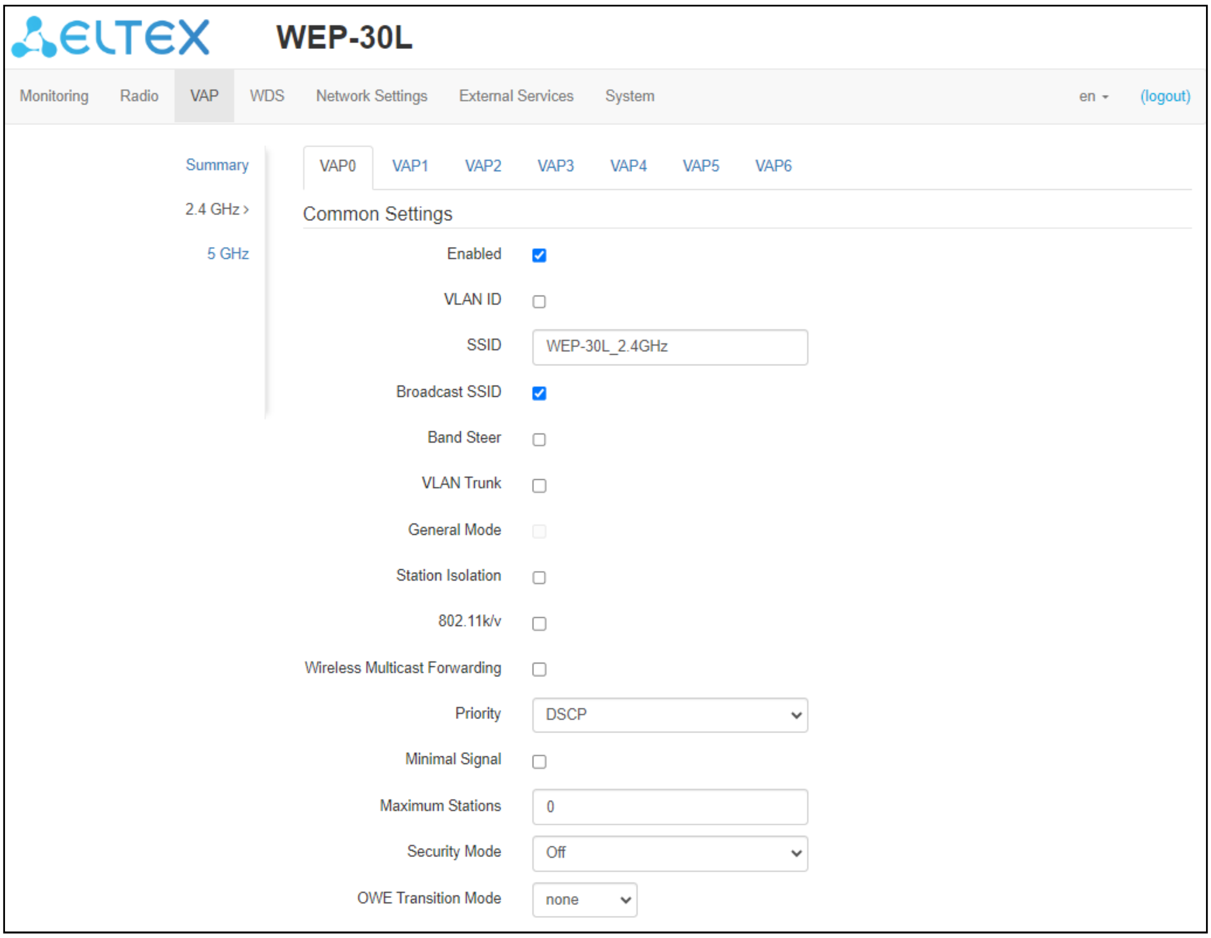


VAP	Enabled	Security Mode	VLAN ID	SSID	Broadcast SSID	Band Steer	VLAN Trunk	General Mode	General VLAN ID	Station Isolation
VAP0	☐	Off	☐	WEP-30L_2.4GHz	☑	☐	☐	☐	☐	☐
VAP1	☐	Off	☐	WEP-30L_2.4GHz-1	☑	☐	☐	☐	☐	☐
VAP2	☐	Off	☐	WEP-30L_2.4GHz-2	☑	☐	☐	☐	☐	☐
VAP3	☐	Off	☐	WEP-30L_2.4GHz-3	☑	☐	☐	☐	☐	☐

- *VAP0–VAP6* — sequence number of the virtual access point;
- *Enabled* — when checked, the virtual access point is enabled, otherwise it is disabled;
- *Security Mode* — 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, the priority connection of the client to 5 GHz network is active. In order for this feature to work, it is required to create a VAP with the same SSID on each radio interface and activate the “Band Steer mode” 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* — 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 settings to non-volatile memory, click “Apply”. Click “Cancel” to discard the changes.

5.6.2 “VAP” submenu



Common Settings

Enabled ☑

VLAN ID □

SSID WEP-30L_2.4GHz

Broadcast SSID ☑

Band Steer □

VLAN Trunk □

General Mode □

Station Isolation □

802.11k/v □

Wireless Multicast Forwarding □

Priority DSCP

Minimal Signal □

Maximum Stations 0

Security Mode Off

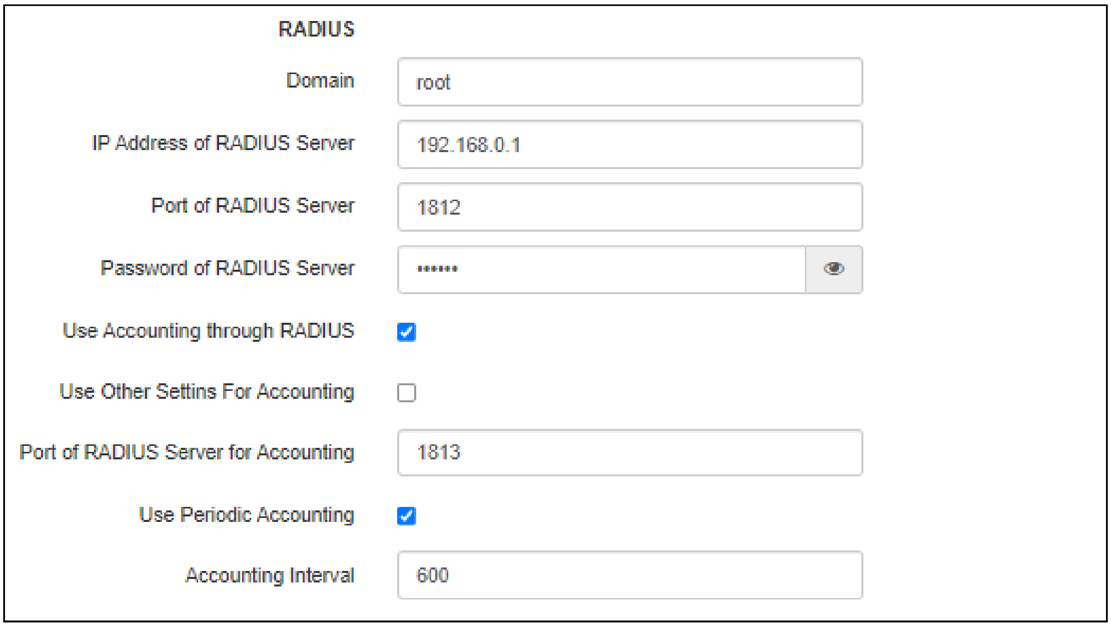
OWE Transition Mode none

<u>Common settings</u>

- *Enabled* — when checked, the virtual access point is enabled, otherwise it is disabled;
- *VLAN ID* — VLAN number from which the tag will be removed when transmitting Wi-Fi traffic to clients connected to this VAP. When traffic flows in the opposite direction, untagged traffic from clients will be tagged with VLAN ID (when VLAN Trunk mode is disabled);
- *SSID* — virtual wireless network name;
- *Broadcast SSID* — when checked, SSID broadcasting is on, otherwise it is disabled;
- *Band Steer mode* — when the flag is set, the priority connection of the client to 5 GHz network is active. In order for this feature to work, it is required to create a VAP with the same SSID on each radio interface and activate the “Band Steer mode” 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* — enable support for 802.11k/v standards on virtual access point;
- *Wireless Multicast Forwarding* — when the flag is set, traffic towards clients will be converted to Unicast before each client, if it is disabled, it will pass without modifications;
- *Priority* — select prioritization mode. 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.

- *Minimal signal* — when the checkbox is selected, the function of disabling the client Wi-Fi equipment when the signal level is low (Minimal Signal Level) is enabled. It is necessary to configure the following parameters:
  - *Minimal Signal Level, dBm* — signal level in dBm below which the client equipment is disconnected from the virtual network;
  - *Roaming Signal Level, dBm* — roaming sensitivity level in dBm, below which the client equipment switches to another access point. The parameter should be higher than the *Minimal Signal Level*: if the *Minimal Signal Level* is -75 dBm, then the *Roaming Signal Level* should be equal to, for example, -70 dBm;
  - *Minimal Signal Timeout, s* — period of time after which a decision is made to disconnect the client equipment from the virtual network.
- *Maximum Stations* — maximum allowable number of clients connected to the virtual network;
- *MFP* — management frame protection (available for WPA2, WPA3, WPA2/WPA3, WPA2-Enterprise, WPA2/WPA3-Enterprise и WPA3-Enterprise, selected security mode, selecting other security modes puts the MFP in the disabled state, when the WPA3, WPA3-Enterprise security mode is selected, the MFP is set to the enabled state):
  - *Off* — management frame protection is disabled;
  - *Optional* — protection works if the client supports MFP. Clients without MFP support can connect to this VAP;
  - *On* — management frame protection is enabled, clients that do not support MFP cannot connect.

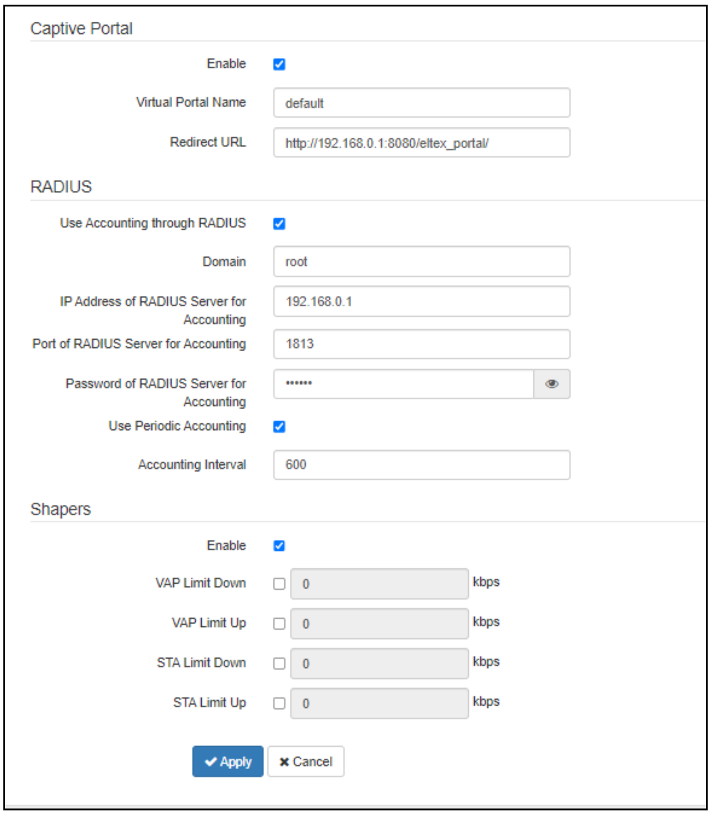
- *Security Mode* — wireless access security mode:
  - *Off* — do not use encryption for data transfer. The access point is available for any subscriber to connect. For open networks, “OWE Transition Mode[1]” can be additionally configured. In this field, specify the interface with the OWE encryption type with which communication will be established;
  - *OWE (Opportunistic Wireless Encryption)* — encryption method that provides the security of data transmitted over an unsecured network. In this case, users do not need to do some additional actions and enter a password to connect to the network. When choosing this mode, a non-editable OWE Transition Mode field is displayed, which indicates an interface with an open encryption type with which connectivity is configured in this moment;
  - *WPA, WPA2, WPA/WPA2, WPA2/WPA3, WPA3* — 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, WPA2/WPA3-Enterprise and WPA3-Enterprise* — wireless channel encryption mode, in which the client is authorized on the centralized RADIUS server. To configure this security mode, specify the parameters of the RADIUS server. Also specify a key for the RADIUS server. When selecting one of the these methods, the following setting will be available:



RADIUS	
Domain	root
IP Address of RADIUS Server	192.168.0.1
Port of RADIUS Server	1812
Password of RADIUS Server	••••••
Use Accounting through RADIUS	☑
Use Other Settins For Accounting	□
Port of RADIUS Server for Accounting	1813
Use Periodic Accounting	☑
Accounting Interval	600

- *Domain* — user domain;
- *IP Address of RADIUS Server* — RADIUS server address;
- *Port of RADIUS Server* — port of the RADIUS server that used for authentication 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. The interval for sending messages can be set in the “Accounting Interval” field.

[1] *"OWE transition mode"* provides backward compatibility with Wi-Fi clients that do not support OWE authentication. When attempting to connect to an open network where *"OWE transition mode"* is configured, a client that supports OWE will connect to the encrypted network configured on the specified interface, and a client that does not support OWE will connect to the current open network without encryption.



Captive Portal

Enable ☑

Virtual Portal Name: default

Redirect URL: http://192.168.0.1:8080/eltex_portal/

RADIUS

Use Accounting through RADIUS ☑

Domain: root

IP Address of RADIUS Server for Accounting: 192.168.0.1

Port of RADIUS Server for Accounting: 1813

Password of RADIUS Server for Accounting: ••••••

Use Periodic Accounting ☑

Accounting Interval: 600

Shapers

Enable ☑

VAP Limit Down □ 0 kbps

VAP Limit Up □ 0 kbps

STA Limit Down □ 0 kbps

STA Limit Up □ 0 kbps

Captive Portal

When selecting one of the following security modes: Off, WPA, WPA2, WPA/WPA2, WPA3, WPA2/WPA3, 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* — address of the external virtual portal to which the user will be redirected when connecting to the network.

RADIUS

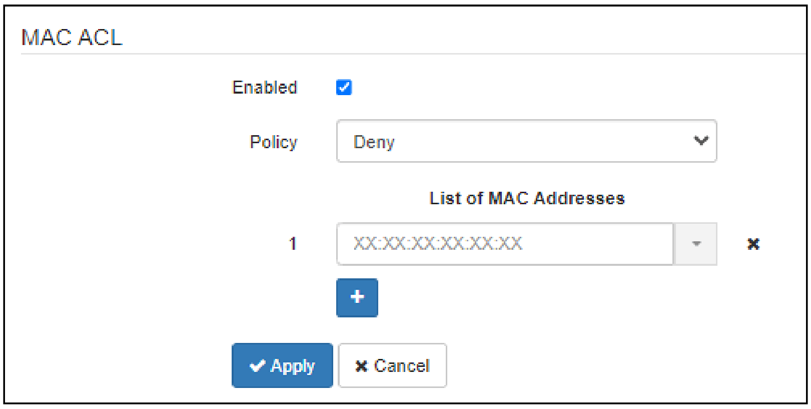
- *Use Accounting through RADIUS* — when checked, "Accounting" messages will be sent to the RADIUS server;
- *Domain* — user domain;
- *IP Address of RADIUS Server for Accounting* — address of the RADIUS server, used for accounting;
- *Port of RADIUS Server for Accounting* — port that will be used to 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. The interval for sending messages can be set in the "Accounting Interval" field.

Shapers

- *Enable* — activate the setting 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.

MAC ACL

This subsection allows configuring the lists of MAC addresses of clients who, depending on the selected access policy, are allowed or prohibited from connecting to this VAP.



MAC ACL

Enabled ☑

Policy Deny

List of MAC Addresses

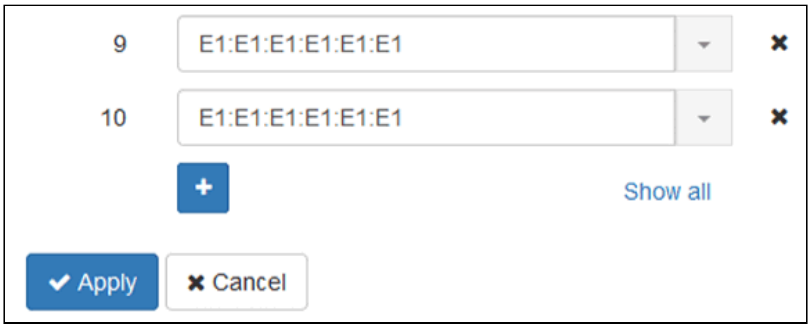
1 XX:XX:XX:XX:XX:XX

- *Enabled* — when the checkbox is selected, the chosen policy is active;
- *Policy* — access policy. Available options:
  - *Deny* — specified MAC addresses will be denied to connect to this VAP. The access will be allowed for everyone else;
  - *Allow* — specified MAC addresses will be allowed to connect to this VAP. The access will be denied for everyone else.
- *List of MAC Addresses* — list of MAC addresses of clients who are allowed or denied access to this VAP. Can contain up to 128 addresses.

To add an address to the list, click the button + and enter the MAC address in the appeared field. To remove an address from the list, click the button ✖ in the corresponding line.

If there is a need to add to the list the MAC address of the client that is currently connected to the base station, click the button ▾ at the end of the line and select the desired address from the list, it will automatically be added to the field.

By default, the list displays up to 10 addresses. To see the full list if it contains more than 10 addresses, click the “Show all” button.



9 E1:E1:E1:E1:E1:E1

10 E1:E1:E1:E1:E1:E1

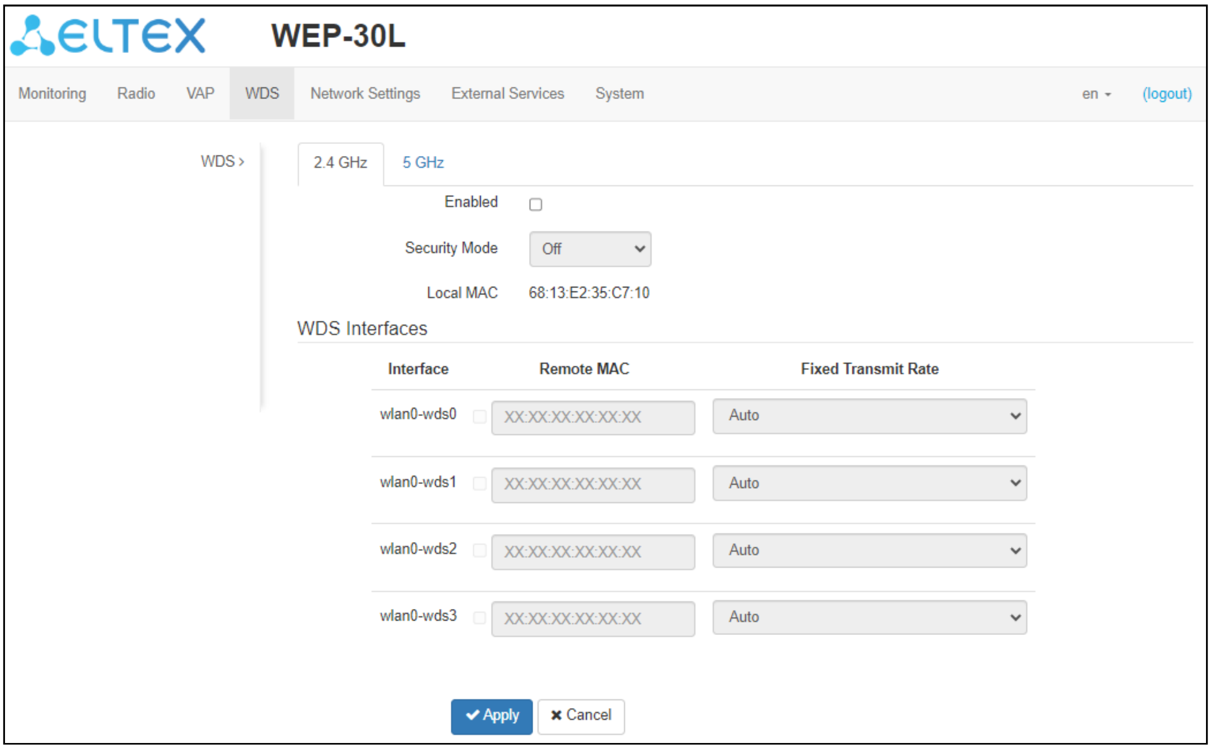
To apply a new configuration and save settings to non-volatile memory, click “Apply”. Click “Cancel” to discard the changes.

5.7 “WDS” menu

In the **“WDS”** menu, wireless bridges are configured between WEP-30L.

> When configuring a WDS connection, it is necessary that the devices connected via WDS have the same channel and channel width selected in the radio interface settings.

5.7.1 **“WDS” submenu**



Enabled ☐

Security Mode: Off

Local MAC: 68:13:E2:35:C7:10

WDS Interfaces

Interface	Remote MAC	Fixed Transmit Rate
wlan0-wds0 ☐	XX:XX:XX:XX:XX:XX	Auto
wlan0-wds1 ☐	XX:XX:XX:XX:XX:XX	Auto
wlan0-wds2 ☐	XX:XX:XX:XX:XX:XX	Auto
wlan0-wds3 ☐	XX:XX:XX:XX:XX:XX	Auto

In the “2.4 GHz” and “5 GHz” tabs, select the radio interface of the device on which you need to build a wireless bridge.

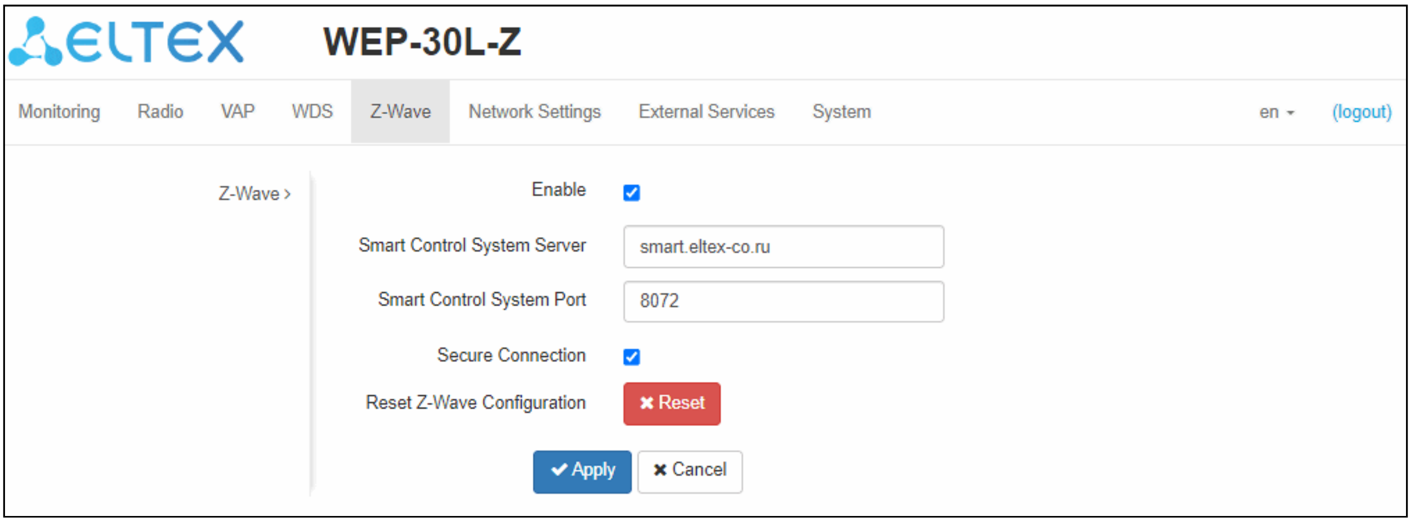
- *Enabled* — when the flag is set, the wireless bridge mode is enabled; otherwise, it is disabled;
- *Security Mode* — wireless network access security mode:
  - *Off* — do not use encryption for data transfer;
  - *WPA2* — encryption method for which the following setting is available:
    - *WPA Key* — key/password required to connect to the remote access point. The key length is from 8 to 63 characters.
- *Local MAC* — enable wireless bridge link;
- *Interface* — select and enable the WDS interface on which the wireless bridge will be built;
- *Remote MAC* — MAC address of the radio interface of the oncoming device to which the wireless bridge is configured;
- *Fixed Transmit Rate* — fixed wireless data transmission rate which defined by IEEE 802.11 standards and selected individually for each link.

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

5.8 "Z-Wave" menu

5.8.1 "Z-Wave" submenu

For WEP-30L-Z only.



Enable ☑

Smart Control System Server: smart.eltex-co.ru

Smart Control System Port: 8072

Secure Connection ☑

Reset Z-Wave Configuration: ✖ Reset

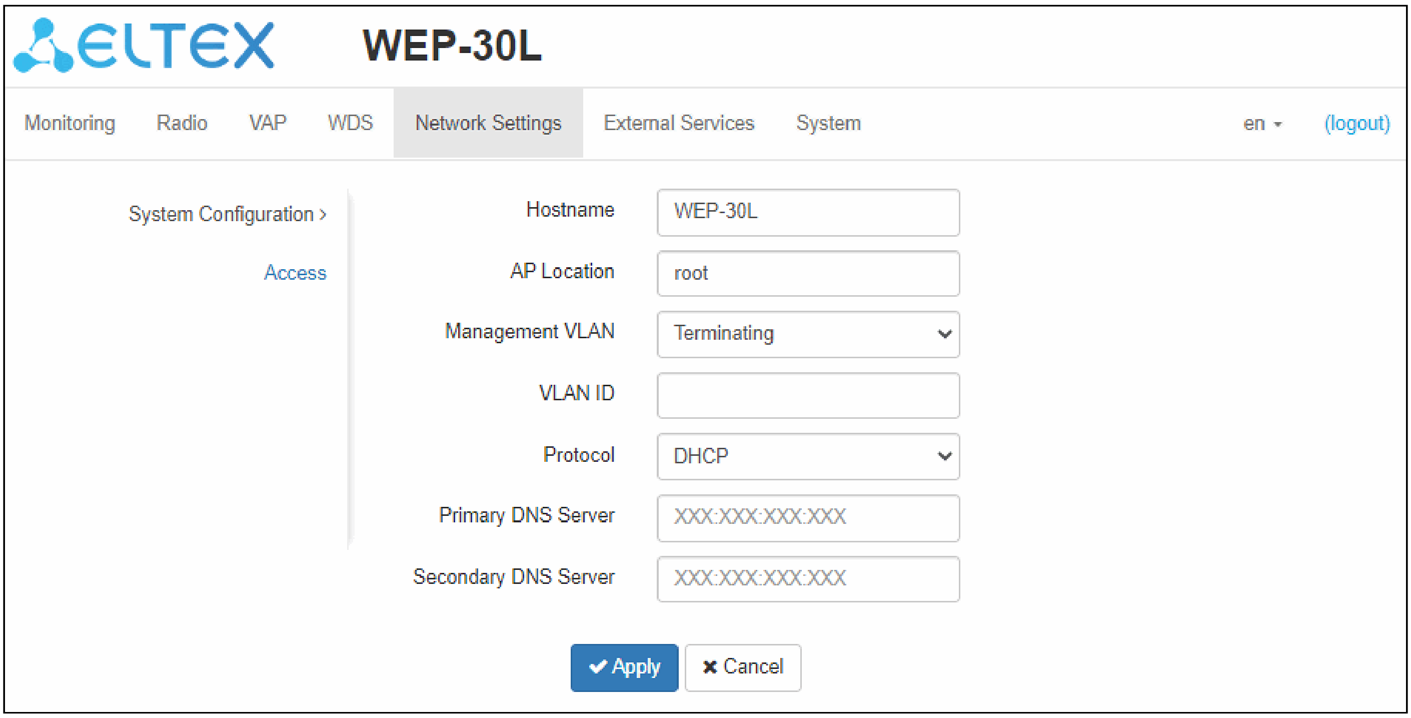
✔ Apply ✖ Cancel

- *Enable* — when the checkbox is selected, the function is enabled. By default the feature is disabled;
- *Smart Control System Server* — Eltex Smart Control (Eltex SC) server address. Default value: smart.eltex-co.ru;
- *Smart Control System Port* — port for communication with the Eltex Smart Home platform. When the *Secure Connection* checkbox is not selected, port 8070 should be specified. Default value: port 8072;
- *Secure connection* — when the checkbox is selected, the SSL encryption protocol is used. By default the feature is enabled;
- *Reset Z-Wave configuration* — restart the Z-Wave Hub and delete all devices connected via the Z-Wave protocol.

To apply a new configuration and save settings to non-volatile memory, click "Apply". Click "Cancel" to discard the changes.

5.9 “Network Settings” menu

5.9.1 “System Configuration” submenu



Hostname	WEP-30L
AP Location	root
Management VLAN	Terminating
VLAN ID	
Protocol	DHCP
Primary DNS Server	XXX:XXX:XXX:XXX
Secondary DNS Server	XXX:XXX:XXX:XXX

- *Hostname* — network 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* — 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* — 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, default gateway and other parameters required for operation are obtained from DHCP server automatically;
  - *Static* — operation mode, when 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* — IP address of the device WAN interface 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 addresses of DNS servers. If addresses of DNS servers are not automatically assigned via DHCP, set them manually.

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

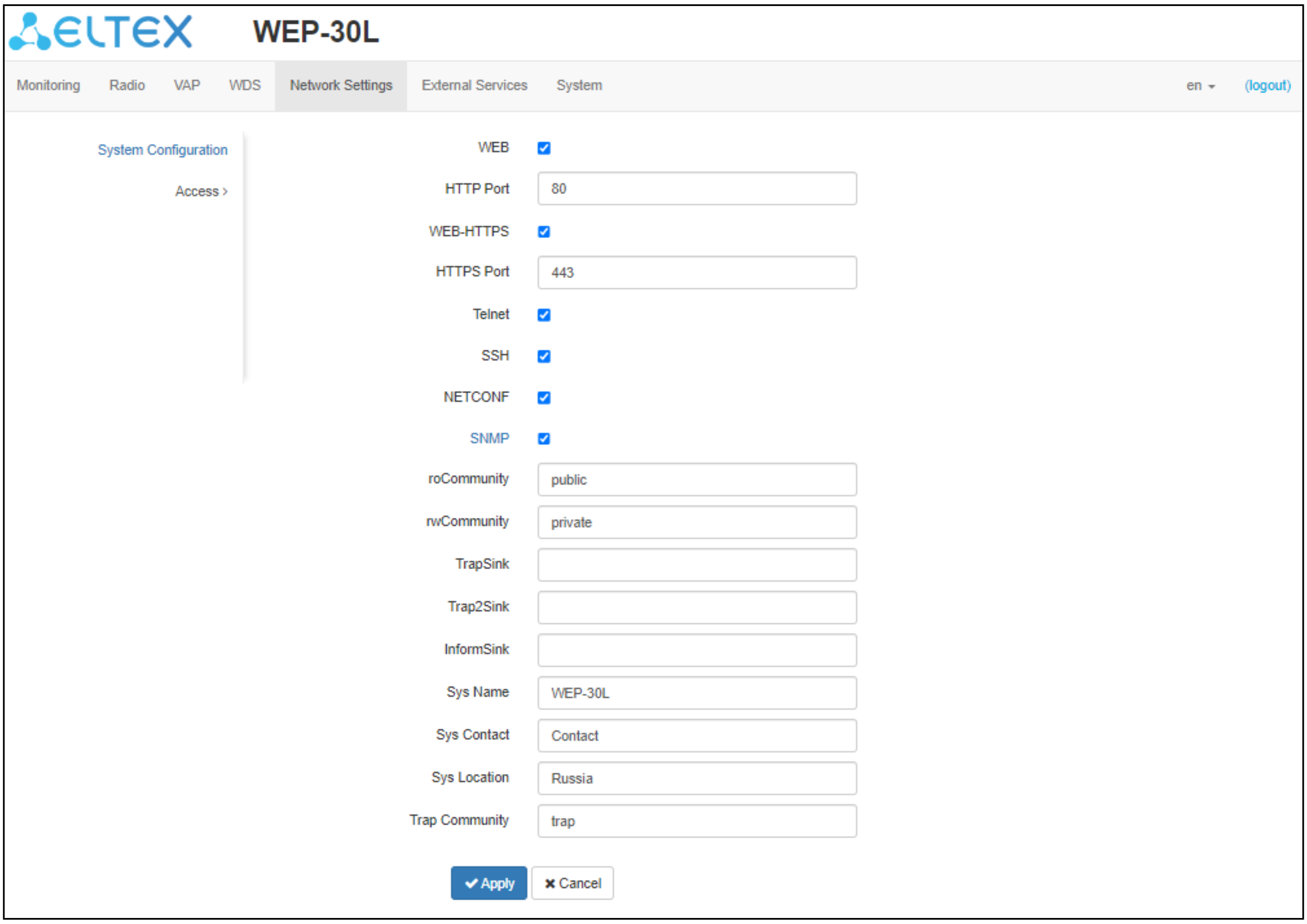
5.9.2 “Access” submenu

In the **“Access”** submenu, the access to the device via Web interface, Telnet, SSH, NETCONF and SNMP can be configured.

- 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”.



WEB	☑
HTTP Port	80
WEB-HTTPS	☑
HTTPS Port	443
Telnet	☑
SSH	☑
NETCONF	☑
SNMP	☑
roCommunity	public
rwCommunity	private
TrapSink	
Trap2Sink	
InformSink	
Sys Name	WEP-30L
Sys Contact	Contact
Sys Location	Russia
Trap Community	trap

The WEP-30L software allows changing the device configuration, monitoring the status of the access point and its sensors, as well as managing the device using the SNMP protocol.
To change the SNMP settings, check the box next to “SNMP”, the following SNMP agent options become available:

- *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 configuring via SNMP is given below:

- eltexLtd.1.127.1 — monitoring of access point parameters and connected client devices;
- eltexLtd.1.127.3 — access point management;
- eltexLtd.1.127.5 — access point configuring.

where eltexLtd — 1.3.6.1.4.1.35265 is Eltex Enterprise ID.

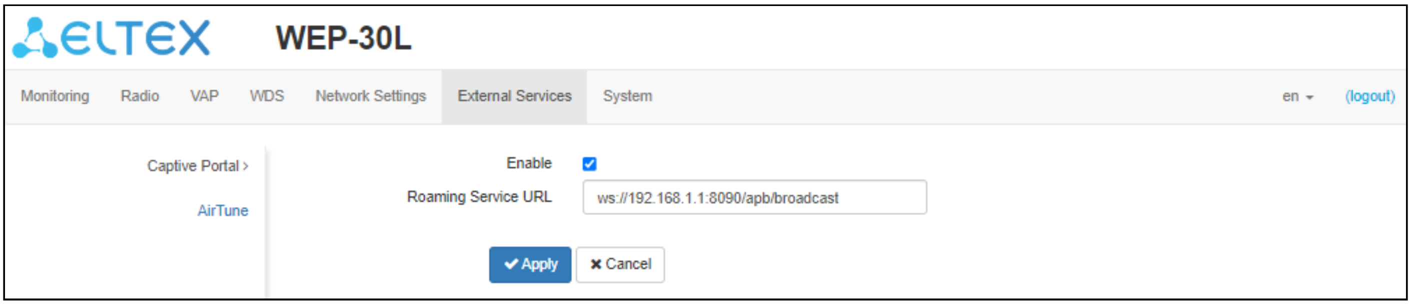
To apply a new configuration and save settings to non-volatile memory, click “Apply”. Click “Cancel” to discard the changes.

5.10 “External Services” menu

5.10.1 “Captive Portal” submenu

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

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



Enable ☑

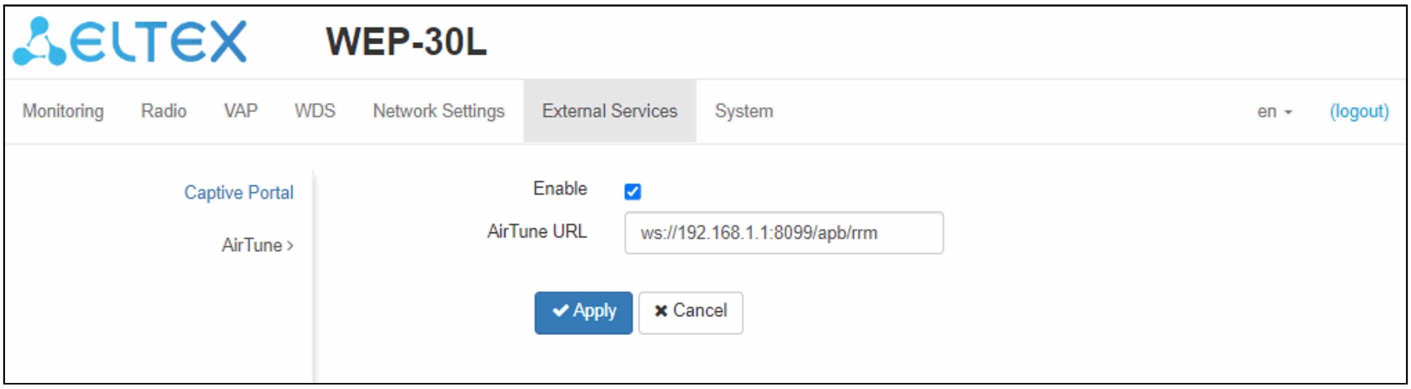
Roaming Service URL: ws://192.168.1.1:8090/apb/broadcast

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

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

5.10.2 "Airtune" submenu

The “AirTune” submenu is intended to enable and configure the AirTune service on the access point.



Enable ☑

AirTune URL ws://192.168.1.1:8099/apb/rrm

- *Enable* — when checked, the point will connect to the AirTune service, the address of which is specified in the “AirTune Service Address” field, to provide Radio Resource Management functions and/or 802.11 k/r roaming;
- *AirTune URL* — AirTune service address. It is specified in the format: “ws://<host>:<port>/apb/rrm”.

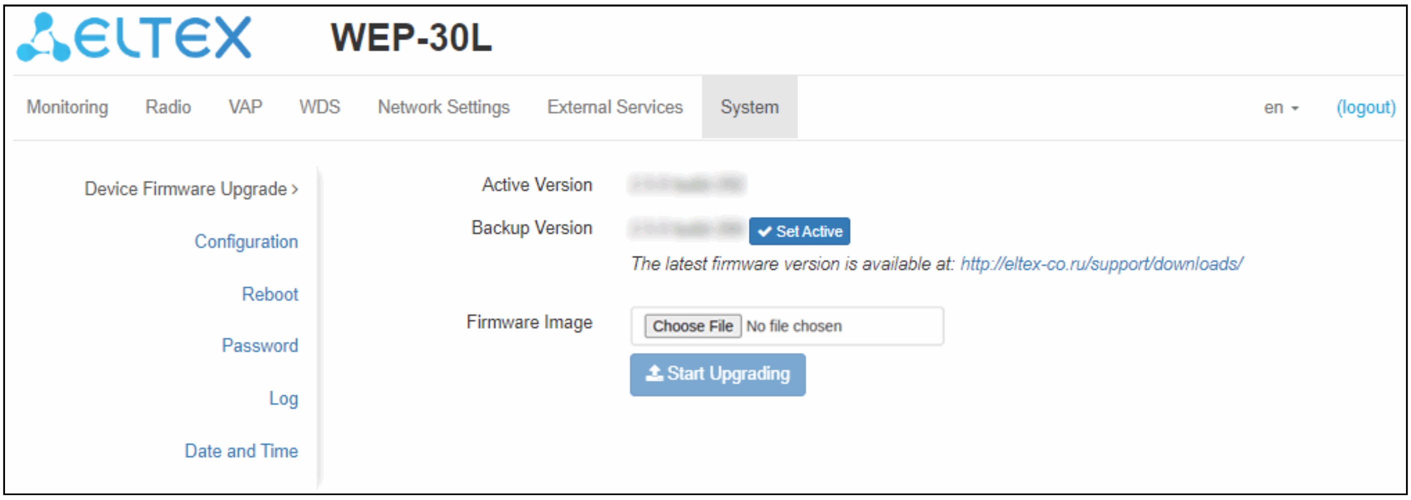
To apply a new configuration and save settings to non-volatile memory, click “Apply”. Click “Cancel” to discard the changes.

5.11 “System” menu

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

5.11.1 “Device Firmware Upgrade” submenu

The **“Device Firmware Upgrade”** submenu is intended for upgrading the device firmware.



Active Version [redacted]

Backup Version [redacted]

The latest firmware version is available at: http://eltex-co.ru/support/downloads/

Firmware Image: No file chosen

- *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;
  - *Set active* — button that allows one to make a backup version of the firmware active, this will require a device reboot. The active firmware version will not be set as a backup.

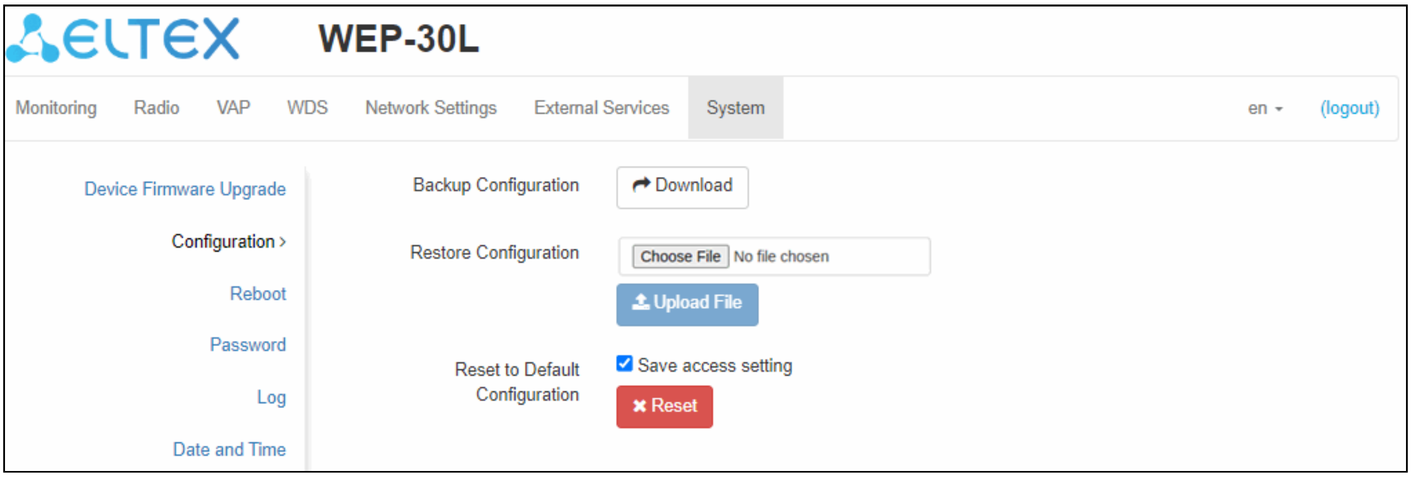
Firmware upgrade

Download the firmware file from *http://eltex-co.com/support/downloads/*. To do this, select WEP-30L from the list of devices and save the file on your computer. After that, click “Choose File” in the Firmware Image field and specify the path to the firmware file in .tar.gz format.
To start the update process, 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 upgrade is completed.

> Do not switch off or reboot the device during a firmware upgrade.

5.11.2 “Configuration” submenu

In the **“Configuration”** submenu, the current configuration can be saved and updated.



☑ Save access setting

<u>Backup Configuration</u>

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

<u>Restore Configuration</u>

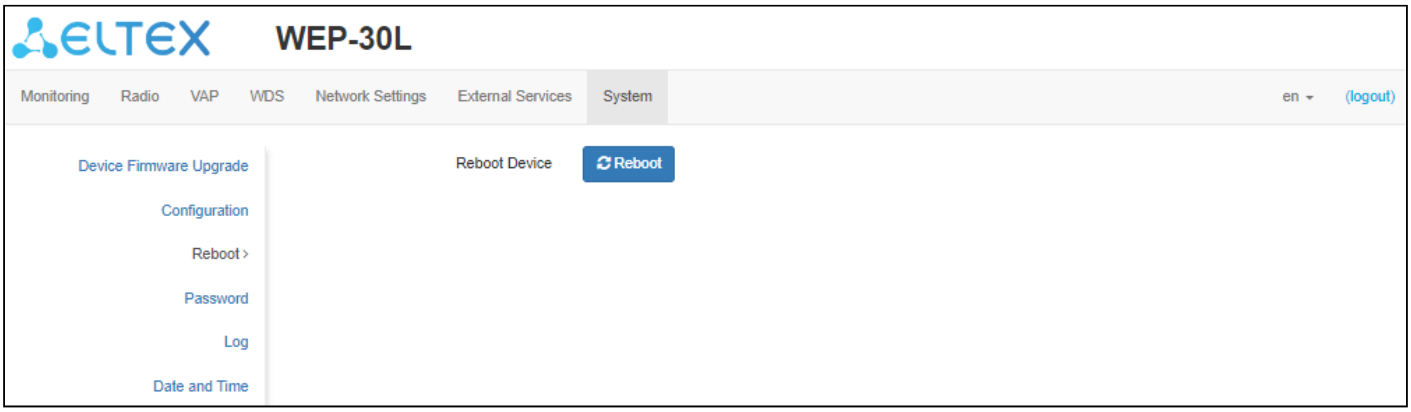
To upload the configuration file saved on the local computer, use the *Restore Configuration* item. To update the device configuration click on the “Browse” button, specify a file (in .tar.gz format) and click on the “Upload” button. Uploaded configuration will be applied automatically and does not require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

<u>Reset to Default Configuration</u>

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

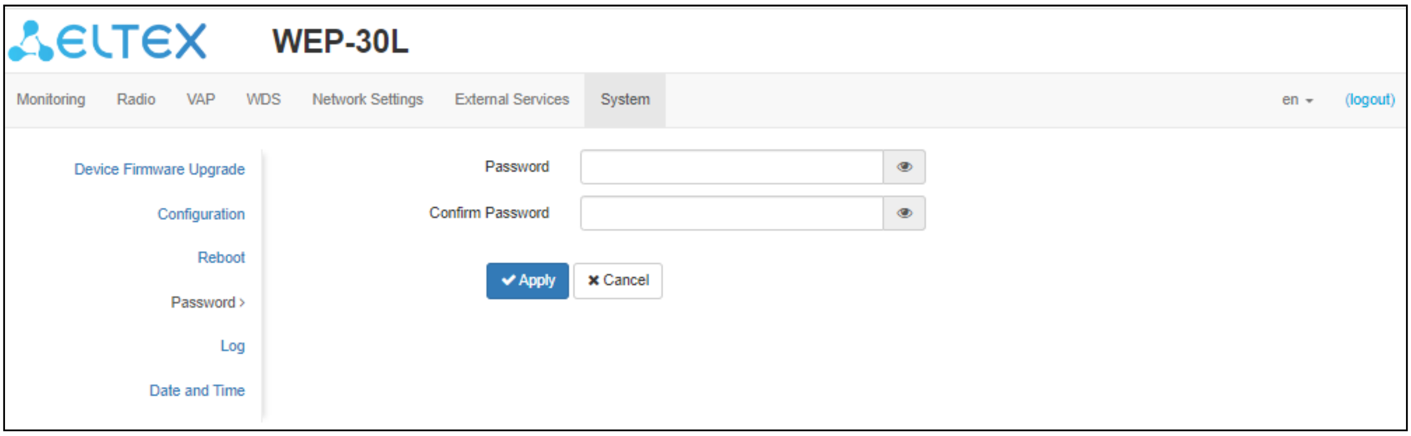
5.11.3 “Reboot” submenu

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



5.11.4 “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 on the “Apply” button to save the new password.

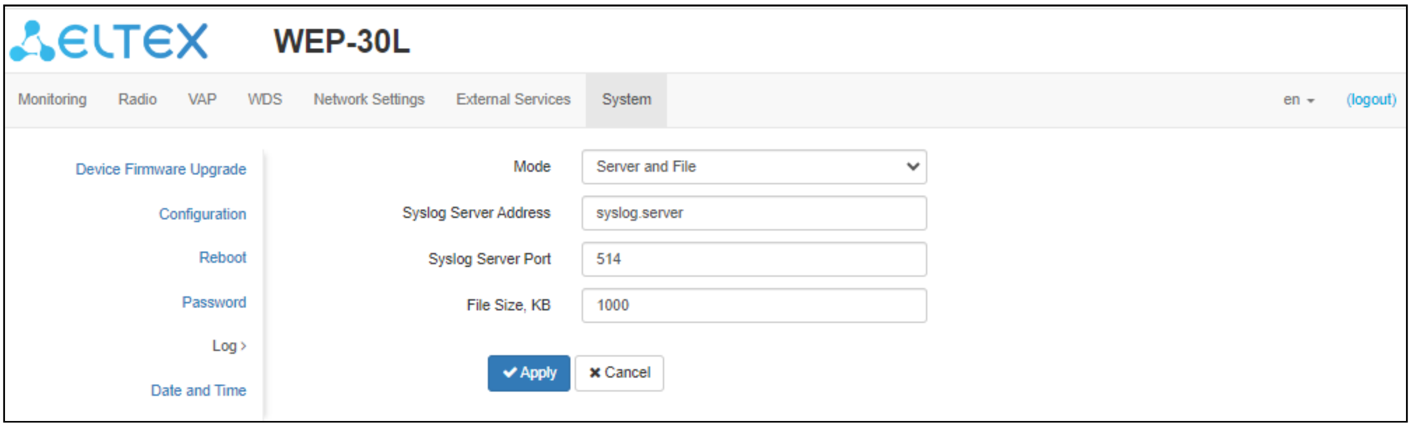


Password

Confirm Password

5.11.5 “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	Server and File
Syslog Server Address	syslog.server
Syslog Server Port	514
File Size, KB	1000

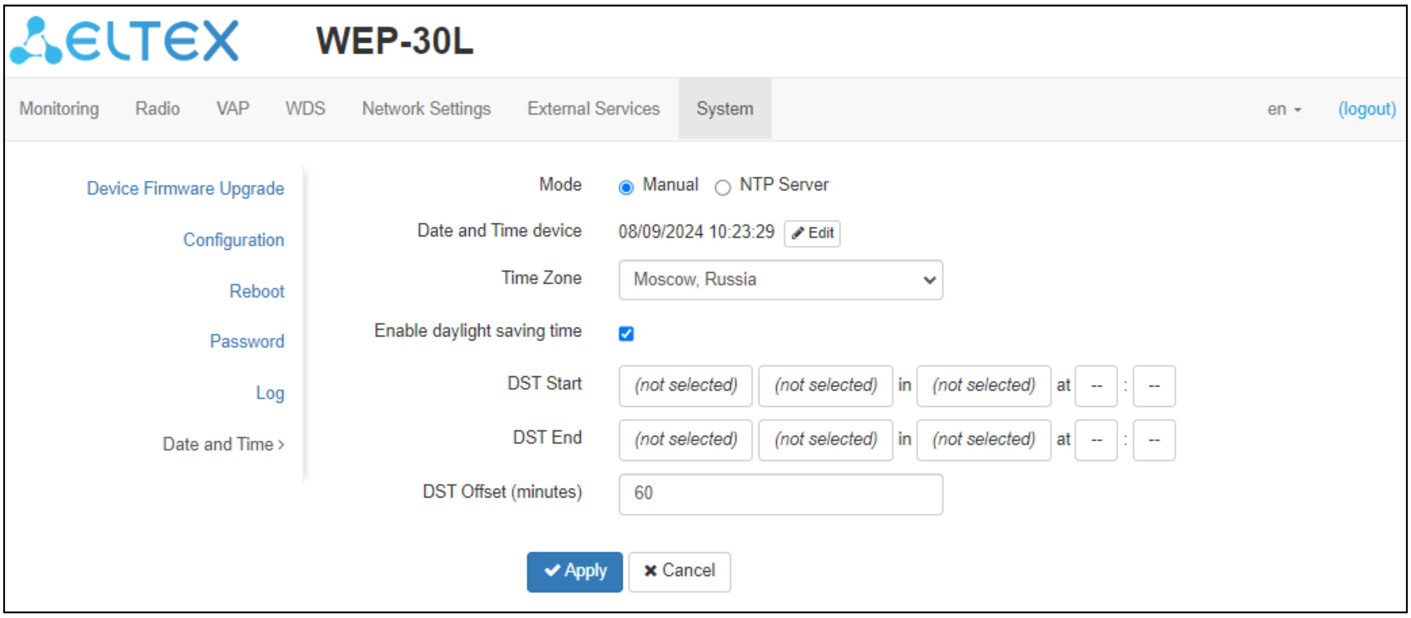
- *Mode* — Syslog agent operation mode:
    - *Local File* — log information is stored in a local file and is available in the device web interface on the “Events” submenu;
    - *Server and File* — log information is sent to a remote Syslog server and stored in a local file.
- *Syslog Server Address* — 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, KB* — maximum size of the log file (valid values: 1–1000 kB).

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

5.11.6 “Date and Time” submenu

In the **“Date and Time”** submenu, it is possible to set the time manually or using the time synchronization protocol (NTP).

5.11.6.1 Manual



Mode ● Manual ○ NTP Server

Date and Time device 08/09/2024 10:23:29

Time Zone Moscow, Russia

Enable daylight saving time ☑

DST Start (not selected) (not selected) in (not selected) at -- : --

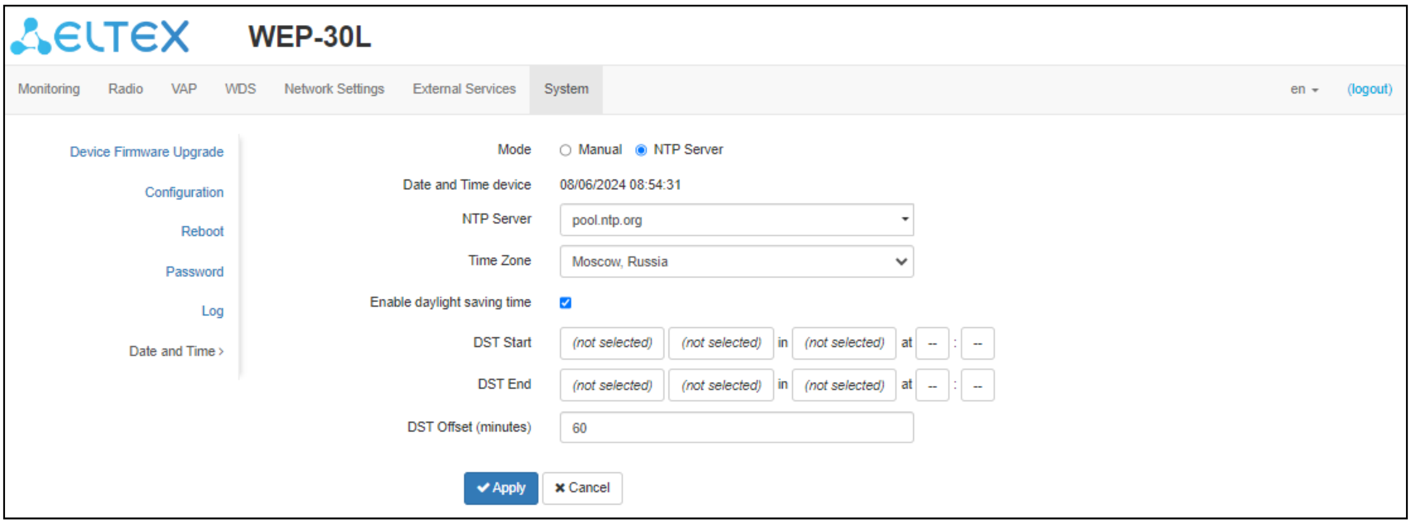
DST End (not selected) (not selected) in (not selected) at -- : --

DST Offset (minutes) 60

- *Date and Time* — date and time on the device at the current moment. Click the “Edit” button to make corrections:
  - *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;
- *Enable Daylight Saving Time* — 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. The parameter can take a value from 0 to 720 minutes.

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

5.11.6.2 NTP server



Mode ○ Manual ● NTP Server

Date and Time device 08/06/2024 08:54:31

NTP Server pool.ntp.org

Time Zone Moscow, Russia

Enable daylight saving time ☑

DST Start (not selected) (not selected) in (not selected) at -- : --

DST End (not selected) (not selected) in (not selected) at -- : --

DST Offset (minutes) 60

- *Date and Time* — 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;
- *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. The parameter can take a value from 0 to 720 minutes.

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

6 Managing the device using the command line

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

6.1 Connection to the device

By default, WEP-30L/WEP-30L-Z 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-30L factory default IP address: **192.168.1.10**, subnet mask: **255.255.255.0**.

Connection to the device is performed via SSH/Telnet:

```
ssh admin@<IP address of the device>, then enter the password
telnet <IP address of the device>, enter login and password
```

6.2 Network parameters configuration

Configuring the static network parameters of the access point

```
WEP-30L(root):/# configure
WEP-30L(config):/# interface
WEP-30L(config):/interface# br0
WEP-30L(config):/interface/br0# common
WEP-30L(config):/interface/br0/common# static-ip X.X.X.X (where X.X.X.X —  WEP-30L IP address)
WEP-30L(config):/interface/br0/common# netmask X.X.X.X (where X.X.X.X — subnet mask)
WEP-30L(config):/interface/br0/common# dns-server-1 X.X.X.X (where X.X.X.X — IP address of the dns server №1)
WEP-30L(config):/interface/br0/common# dns-server-2 X.X.X.X (where X.X.X.X — IP address of the dns server №2)
WEP-30L(config):/interface/br0/common# protocol static-ip (change operation mode from DHCP to Static-IP)
WEP-30L(config):/interface/br0/common# save (save changes)
```

Adding a static route

```
WEP-30L(config):/interface/br0/common# exit
WEP-30L(config):/interface/br0# exit
WEP-30L(config):/interface# exit
WEP-30L(config):/# route
WEP-30L(config):/route# add default (where default — route name)
WEP-30L(config):/route# default
WEP-30L(config):/route/default# destination X.X.X.X (where X.X.X.X — IP address of the network or destination node, for default route — 0.0.0.0)
WEP-30L(config):/route/default# netmask X.X.X.X (where X.X.X.X — destination network mask, for default route — 0.0.0.0)
WEP-30L(config):/route/default# gateway X.X.X.X (where X.X.X.X — gateway IP address)
WEP-30L(config):/route/default# save (save changes)
```

Configuring the reception of network parameters via DHCP

```
WEP-30L(root):/# configure
WEP-30L(config):/# interface
WEP-30L(config):/interface# br0
WEP-30L(config):/interface/br0# common
WEP-30L(config):/interface/br0/common# protocol dhcp
WEP-30L(config):/interface/br0/common# save (save changes)
```

Configuring IPv4 access settings

```
WEP-30L(root):/# configure
WEP-30L(config):/# interface
WEP-30L(config):/interface# br0
WEP-30L(config):/interface/br0# common
WEP-30L(config):/interface/br0/common# access-rules (go to the section of access settings via IPv4 protocol)
WEP-30L(config):/interface/br0/common/access-rules# telnet false (where false — restriction of access via the TELNET protocol to the device by its IPv4 address. This setting applies only to the connection to the device via IPv4, access via IPv6 will remain if the corresponding prohibition setting has not been made in the section for IPv6. To remove the restriction, enter true)
WEP-30L(config):/interface/br0/common/access-rules# save (save changes)
```

Starting from firmware version 2.2.0, it is possible to set MTU via DHCP (option 26). The MTU value obtained via DHCP takes precedence over the configured setting.

The MTU size for a bridge should be no larger than the smallest MTU size on the interfaces within this bridge.

Configuring MTU size on the interface

```
WEP-30L(root):/# configure
WEP-30L(config):/# interface
WEP-30L(config):/interface# br0
WEP-30L(config):/interface/br0# common
WEP-30L(config):/interface/br0/common# mtu X (where X — MTU size in bytes. Acceptable values: 1–2490)
WEP-30L(config):/interface/br0/common# save (save changes)
```

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

Untagged access

Obtaining the network parameters via DHCP:

```
WEP-30L(root):/# set-management-vlan-mode off protocol dhcp
```

Static settings:

```
WEP-30L(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

Obtaining the network parameters via DHCP:

```
WEP-30L(root):/# set-management-vlan-mode terminating vlan-id X protocol dhcp (where X — VLAN ID used
for access to the device. Acceptable values: 1–4094)
```

Static settings:

```
WEP-30L(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. Acceptable 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

Obtaining the network parameters via DHCP:

```
WEP-30L(root):/# set-management-vlan-mode forwarding vlan-id X protocol dhcp (where X — VLAN ID used
for access to the device. Acceptable values: 1–4094)
```

Static settings:

```
WEP-30L(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. Acceptable values:
1–4094;  X.X.X.X — static IP address, Y.Y.Y.Y — subnet mask, Z.Z.Z.Z — gateway)
```

Completing and saving settings

```
WEP-30L(root):/# save (save changes)
```

6.2.2 IPv6 network parameters configuration

Access to the device via IPv6 protocol is disabled by default.

Enabling access to the device via IPv6 protocol

```
WEP-30L(root):/# configure
WEP-30L(config):/# interface
WEP-30L(config):/interface# br0
WEP-30L(config):/interface/br0# common
WEP-30L(config):/interface/br0/common# ipv6
WEP-30L(config):/interface/br0/common/ipv6# protocol dhcp (obtaining IPv6 network parameters via DHCP)
WEP-30L(config):/interface/br0/common/ipv6# enabled true (enabling access to the device via IPv6 protocol.
To disable, enter false)
WEP-30L(config):/interface/br0/common/ipv6# save (save changes)
```

Configuring static IPv6 network settings for the access point

```
WEP-30L(root):/# configure
WEP-30L(config):/# interface
WEP-30L(config):/interface# br0
WEP-30L(config):/interface/br0# common
WEP-30L(config):/interface/br0/common# ipv6
WEP-30L(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-30L device)
WEP-30L(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-30L(config):/interface/br0/common/ipv6# gateway  XXXX:XXXX:XXXX:XXXX::/64 (IPv6 prefix is specified, for example 3211:0:0:1234::/64)
WEP-30L(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-30L(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-30L(config):/interface/br0/common/ipv6# protocol static-ip (enable use of static IPv6 networks parameters. For obtaining the IPv6 network parameters via DHCP enter dhcp)
WEP-30L(config):/interface/br0/common/ipv6# enabled true (enable access to the device via IPv6 protocol. To disable enter false)
WEP-30L(config):/interface/br0/common/ipv6# save (save changes)
```

Configuring IPv6 access settings

```
WEP-30L(root):/# configure
WEP-30L(config):/# interface
WEP-30L(config):/interface# br0
WEP-30L(config):/interface/br0# common
WEP-30L(config):/interface/br0/common# ipv6
WEP-30L(config):/interface/br0/common/ipv6# access-rules (go to the section of access settings)
WEP-30L(config):/interface/br0/common/ipv6/access-rules# telnet false (where false — restriction of access via the TELNET protocol to the device by its IPv6 address. This setting applies only to connection to the device via IPv6, access via IPv4 will remain if the corresponding prohibition setting has not been made in the section for IPv4. To remove the restriction, enter true)
WEP-30L(config):/interface/br0/common/ipv6/access-rules# save (save changes)
```

Similar to restricting access to the device via the TELNET protocol, you can restrict the ability to connection to the device by its IPv6 address using the following protocols: SSH, SNMP, NETCONF, web, web-HTTPS.

6.3 Virtual Wi-Fi access points (VAP) configuration

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

Table 8 — Commands for configuring security mode on VAP

Security mode	Command to set the security mode
Without password	mode off
WPA	mode WPA
WPA2	mode WPA2
WPA/WPA2	mode WPA_WPA2
WPA3	mode WPA3
WPA2/WPA3	mode WPA2_WPA3
OWE	mode OWE
WPA-Enterprise	mode WPA_1X
WPA2-Enterprise	mode WPA2_1X
WPA/WPA2-Enterprise	mode WPA_WPA2_1X
WPA2/WPA3-Enterprise	mode WPA2_WPA3_1X
WPA3-Enterprise	mode WPA3_1X

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

6.3.1 Configuration of VAP without encryption

Creating a VAP without encryption with periodic sending of accounting to a RADIUS server

```
WEP-30L(root):/# configure
WEP-30L(config):/# interface
WEP-30L(config):/interface# wlan1-va0
WEP-30L(config):/interface/wlan1-va0# vap
WEP-30L(config):/interface/wlan1-va0/vap# ssid 'SSID_WEP-30L_open' (change SSID name)
WEP-30L(config):/interface/wlan1-va0/vap# ap-security
WEP-30L(config):/interface/wlan1-va0/vap# ap-security# mode off (encryption mode off — without password)
WEP-30L(config):/interface/wlan1-va0/vap# ap-security# exit
WEP-30L(config):/interface/wlan1-va0/vap# radius
WEP-30L(config):/interface/wlan1-va0/vap/radius# acct-enable true (enable sending of "Accounting" messages to the RADIUS server. By default: false)
WEP-30L(config):/interface/wlan1-va0/vap/radius# acct-address X.X.X.X (where X.X.X.X — IP address of RADIUS server used for accounting)
WEP-30L(config):/interface/wlan1-va0/vap/radius# acct-password secret (where secret — password for RADIUS server used for accounting)
WEP-30L(config):/interface/wlan1-va0/vap/radius# acct-periodic true (enable periodic sending of "Accounting" messages to the RADIUS server. By default: false)
WEP-30L(config):/interface/wlan1-va0/vap/radius# acct-interval 600 (interval for sending "Accounting" messages to the RADIUS server)
WEP-30L(config):/interface/wlan1-va0/vap/radius# exit
WEP-30L(config):/interface/wlan1-va0/vap# exit
WEP-30L(config):/interface/wlan1-va0# common
WEP-30L(config):/interface/wlan1-va0/common# enabled true (enable VAP)
WEP-30L(config):/interface/wlan1-va0/common# save (save changes)
```

6.3.2 Configuration of VAP with OWE encryption

Configuration of VAP with OWE encryption

```
WEP-30L(root):/# configure
WEP-30L(config):/# interface
WEP-30L(config):/interface# wlan1-va0
WEP-30L(config):/interface/wlan1-va0# vap
WEP-30L(config):/interface/wlan1-va0/vap# ssid 'SSID_WEP-30L_owe' (change SSID name)
WEP-30L(config):/interface/wlan1-va0/vap# ap-security
WEP-30L(config):/interface/wlan1-va0/vap/ap-security# mode OWE (encryption mode OWE — encrypted connection without entering a password. In this mode, only Wi-Fi 6 clients will be able to connect)
WEP-30L(config):/interface/wlan1-va0/vap/ap-security# exit
WEP-30L(config):/interface/wlan1-va0/vap# radius
WEP-30L(config):/interface/wlan1-va0/vap/radius# acct-enable true (enable sending of "Accounting" messages to the RADIUS server. By default: false)
WEP-30L(config):/interface/wlan1-va0/vap/radius# acct-address X.X.X.X (where X.X.X.X — IP address of RADIUS server used for accounting)
WEP-30L(config):/interface/wlan1-va0/vap/radius# acct-password secret (where secret — password for RADIUS server used for accounting)
WEP-30L(config):/interface/wlan1-va0/vap/radius# acct-periodic true (enable periodic sending of "Accounting" messages to the RADIUS server. By default: false)
WEP-30L(config):/interface/wlan1-va0/vap/radius# acct-interval 600 (interval for sending "Accounting" messages to the RADIUS server)
WEP-30L(config):/interface/wlan1-va0/vap/radius# exit
WEP-30L(config):/interface/wlan1-va0/vap# exit
WEP-30L(config):/interface/wlan1-va0# common
WEP-30L(config):/interface/wlan1-va0/common# enabled true (enable VAP)
WEP-30L(config):/interface/wlan1-va0/common# save (save changes)
```

6.3.3 Configuration of VAP with OWE and OWE Transition Mode

Only Wi-Fi 6 clients can connect to a VAP with OWE security mode. In order for other clients to be able to connect to such a VAP, it is required to configure OWE Transition Mode. In this mode, Wi-Fi 6 clients will be connected in OWE security mode, and all other clients will be connected in open mode.

Creating a VAP with OWE and OWE Transition Mode

```
WEP-30L(root):/# configure
WEP-30L(config):/# interface
WEP-30L(config):/interface# wlan1-va0 (set up a hidden VAP with OWE encryption. Wi-Fi 6 clients will implicitly
connect to it)
WEP-30L(config):/interface/wlan1-va0# vap
WEP-30L(config):/interface/wlan1-va0/vap# ssid 'SSID_WEP-30L_owe' (change SSID name)
WEP-30L(config):/interface/wlan1-va0/vap# hidden true (hide VAP)
WEP-30L(config):/interface/wlan1-va0/vap# ap-security
WEP-30L(config):/interface/wlan1-va0/vap/ap-security# mode OWE (encryption mode OWE — encrypted
connection without entering a password. Only Wi-Fi 6 clients can connect in this mode)
WEP-30L(config):/interface/wlan1-va0/vap/ap-security# owe-transition-interface wlan1-va1 (specify an open
VAP to which the connection will occur. The Wi-Fi 6 clients will implicitly work with the current VAP with OWE
encryption, and other clients will work with the open VAP)
WEP-30L(config):/interface/wlan1-va0/vap/ap-security# exit
WEP-30L(config):/interface/wlan1-va0/vap# exit
WEP-30L(config):/interface/wlan1-va0# common
WEP-30L(config):/interface/wlan1-va0/common# enabled true (enable VAP)
WEP-30L(config):/interface/wlan1-va0/common# exit
WEP-30L(config):/interface/wlan1-va0# exit
WEP-30L(config):/interface# wlan1-va1 (set up VAP without encryption)
WEP-30L(config):/interface/wlan1-va1# vap
WEP-30L(config):/interface/wlan1-va1/vap# ssid 'SSID_WEP-30L_open' (change SSID name)
WEP-30L(config):/interface/wlan1-va1/vap# ap-security (go to the security settings block on the VAP)
WEP-30L(config):/interface/wlan1-va1/vap/ap-security# mode off (encryption mode off — without password)
WEP-30L(config):/interface/wlan1-va1/vap/ap-security# owe-transition-interface wlan1-va0 (specify a VAP
with OWE encryption mode, to which Wi-Fi 6 clients will be implicitly connected, other clients will be connected
to the VAP without encryption)
WEP-30L(config):/interface/wlan1-va1/vap/ap-security# exit
WEP-30L(config):/interface/wlan1-va1/vap# exit
WEP-30L(config):/interface/wlan1-va1# common
WEP-30L(config):/interface/wlan1-va1/common# enabled true (enable VAP)
WEP-30L(config):/interface/wlan1-va1/common# exit
WEP-30L(config):/interface/wlan1-va1# save (save changes)
```

6.3.4 Configuration of VAP with WPA-Personal security mode

Creation of VAP with WPA-Personal security mode with periodic sending of accounting to a RADIUS server

```
WEP-30L(root):/# configure
WEP-30L(config):/# interface
WEP-30L(config):/interface# wlan1-va0
WEP-30L(config):/interface/wlan1-va0# vap
WEP-30L(config):/interface/wlan1-va0/vap# ssid 'SSID_WEP-30L_Wpa2' (change SSID name)
WEP-30L(config):/interface/wlan1-va0/vap# ap-security
WEP-30L(config):/interface/wlan1-va0/vap#ap-security# mode WPA_WPA2 (encryption mode — WPA/WPA2)
WEP-30L(config):/interface/wlan1-va0/vap/ap-security# key-wpa password123 (key/password required to
connect to the virtual access point. The key must be between 8 and 63 characters long)
WEP-30L(config):/interface/wlan1-va0/vap/ap-security# exit
WEP-30L(config):/interface/wlan1-va0/vap# radius
WEP-30L(config):/interface/wlan1-va0/vap/radius# acct-enable true (enable sending of "Accounting" messages
to the RADIUS server. By default:  false)
WEP-30L(config):/interface/wlan1-va0/vap/radius# acct-address X.X.X.X (where X.X.X.X — IP address of RADIUS
server used for accounting)
WEP-30L(config):/interface/wlan1-va0/vap/radius# acct-password secret (where secret — password for RADIUS
server used for accounting)
WEP-30L(config):/interface/wlan1-va0/vap/radius# acct-periodic true (enable periodic sending of "Accounting"
messages to the RADIUS server. By default:  false)
WEP-30L(config):/interface/wlan1-va0/vap/radius# acct-interval 600 (interval for sending "Accounting"
messages to the RADIUS server)
WEP-30L(config):/interface/wlan1-va0/vap/radius# exit
WEP-30L(config):/interface/wlan1-va0/vap# exit
WEP-30L(config):/interface/wlan1-va0# common
WEP-30L(config):/interface/wlan1-va0/common# enabled true (enable VAP)
WEP-30L(config):/interface/wlan1-va0/common# save (save changes)
```

6.3.5 Configuration of VAP with Enterprise authorization

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

```
WEP-30L(root):/# configure
WEP-30L(config):/# interface
WEP-30L(config):/interface# wlan1-va0
WEP-30L(config):/interface/wlan1-va0# vap
WEP-30L(config):/interface/wlan1-va0/vap# ssid 'SSID_WEP-30L_enterprise' (change SSID name)
WEP-30L(config):/interface/wlan1-va0/vap# ap-security
WEP-30L(config):/interface/wlan1-va0/vap/ap-security # mode WPA_WPA2_1X (encryption mode — WPA/WPA2-Enterprise)
WEP-30L(config):/interface/wlan1-va0/vap/ap-security# exit
WEP-30L(config):/interface/wlan1-va0/vap# radius
WEP-30L(config):/interface/wlan1-va0/vap/radius# domain root (where root — user domain)
WEP-30L(config):/interface/wlan1-va0/vap/radius# auth-address X.X.X.X (where X.X.X.X — IP address of RADIUS server)
WEP-30L(config):/interface/wlan1-va0/vap/radius# auth-port X (where X — port of RADIUS server used for authentication and authorization. By default: 1812)
WEP-30L(config):/interface/wlan1-va0/vap/radius# auth-password secret (where secret — password for RADIUS server used for authentication and authorization)
WEP-30L(config):/interface/wlan1-va0/vap/radius# acct-enable true (enable sending of "Accounting" messages to the RADIUS server. By default: false)
WEP-30L(config):/interface/wlan1-va0/vap/radius# acct-address X.X.X.X (where X.X.X.X — IP address of RADIUS server used for accounting)
WEP-30L(config):/interface/wlan1-va0/vap/radius# acct-password secret (where secret — password for RADIUS server used for accounting)
WEP-30L(config):/interface/wlan1-va0/vap/radius# acct-periodic true (enable periodic sending of "Accounting" messages to the RADIUS server. By default: false)
WEP-30L(config):/interface/wlan1-va0/vap/radius# acct-interval 600 (interval for sending "Accounting" messages to the RADIUS server)
WEP-30L(config):/interface/wlan1-va0/vap/radius# exit
WEP-30L(config):/interface/wlan1-va0/vap# exit
WEP-30L(config):/interface/wlan1-va0# common
WEP-30L(config):/interface/wlan1-va0/common# enabled true (enable VAP)
WEP-30L(config):/interface/wlan1-va0/common# save (save changes)
```

6.3.6 Configuration of VAP with Captive Portal

Commands to configure portal authorization with sending accounting to the Radius server

```
WEP-30L(root):/# configure
WEP-30L(config):/# interface
WEP-30L(config):/interface# wlan1-va0
WEP-30L(config):/interface/wlan1-va0# vap
WEP-30L(config):/interface/wlan1-va0/vap# vlan-id X (where X — VLAN-ID on VAP)
WEP-30L(config):/interface/wlan1-va0/vap# ap-security
WEP-30L(config):/interface/wlan1-va0/vap/ap-security# mode off (encryption mode off — no password)
WEP-30L(config):/interface/wlan1-va0/vap/ap-security# exit
WEP-30L(config):/interface/wlan1-va0/vap# ssid 'Portal_WEP-30L' (change SSID name)
WEP-30L(config):/interface/wlan1-va0/vap# captive-portal
WEP-30L(config):/interface/wlan1-va0/vap/captive-portal# scenarios
WEP-30L(config):/interface/wlan1-va0/vap/captive-portal/scenarios# scenario-redirect
WEP-30L(config):/interface/wlan1-va0/vap/captive-portal/scenarios/scenario-redirect# redirect-url  http://<IP>:<PORT>/eltex_portal/ (specify URL of virtual portal)
WEP-30L(config):/interface/wlan1-va0/vap/captive-portal/scenarios/scenario-redirect# index 1
WEP-30L(config):/interface/wlan1-va0/vap/captive-portal/scenarios/scenario-redirect# virtual-portal-name default (specify portal name. By default: default)
WEP-30L(config):/interface/wlan1-va0/vap/captive-portal/scenarios/scenario-redirect# exit
WEP-30L(config):/interface/wlan1-va0/vap/captive-portal/scenarios# exit
WEP-30L(config):/interface/wlan1-va0/vap/captive-portal# enabled true
WEP-30L(config):/interface/wlan1-va0/vap/captive-portal# exit
WEP-30L(config):/interface/wlan1-va0/vap# radius
WEP-30L(config):/interface/wlan1-va0/vap/radius# domain root (where root — user domain)
WEP-30L(config):/interface/wlan1-va0/vap/radius# acct-enable true (enable sending of "Accounting" messages to the RADIUS server. By default:false)
WEP-30L(config):/interface/wlan1-va0/vap/radius# acct-address X.X.X.X (where X.X.X.X — IP address of RADIUS server used for accounting)
WEP-30L(config):/interface/wlan1-va0/vap/radius# acct-password secret (where secret — password for RADIUS server used for accounting)
WEP-30L(config):/interface/wlan1-va0/vap/radius# acct-periodic true (enable periodic sending of "Accounting" messages to the RADIUS server. By default: false)
WEP-30L(config):/interface/wlan1-va0/vap/radius# acct-interval 600 (interval for sending "Accounting" messages to the RADIUS server)
WEP-30L(config):/interface/wlan1-va0/vap/radius# exit
WEP-30L(config):/interface/wlan1-va0/vap# exit
WEP-30L(config):/interface/wlan1-va0# common
WEP-30L(config):/interface/wlan1-va0/common# enabled true (enable VAP)
WEP-30L(config):/interface/wlan1-va0/common# save (save changes)
```

6.3.7 Configuration of VAP with external Captive Portal

Commands to configure the external Captive Portal

```
WEP-30L(root):/# configure
WEP-30L(config):/# interface
WEP-30L(config):/interface# wlan1-va0
WEP-30L(config):/interface/wlan1-va0# vap
WEP-30L(config):/interface/wlan1-va0/vap# vlan-id X (where X — VLAN-ID on VAP)
WEP-30L(config):/interface/wlan1-va0/vap# ap-security
WEP-30L(config):/interface/wlan1-va0/vap/ap-security# mode off (encryption mode off — no password)
WEP-30L(config):/interface/wlan1-va0/vap/ap-security# exit
WEP-30L(config):/interface/wlan1-va0/vap# ssid 'Portal_WEP-30L' (change SSID name)
WEP-30L(config):/interface/wlan1-va0/vap# captive-portal
WEP-30L(config):/interface/wlan1-va0/vap/captive-portal# scenarios
WEP-30L(config):/interface/wlan1-va0/vap/captive-portal/scenarios# scenario-redirect
WEP-30L(config):/interface/wlan1-va0/vap/captive-portal/scenarios/scenario-redirect# redirect-url "https://
X.X.X.X/<NAS_ID>/switch_url<SWITCH_URL>&ap_mac=<AP_MAC>&client_mac=<CLIENT_MAC>
&wlan=<SSID>&original-url=<ORIGINAL_URL>" (specify the URL of the external virtual portal according to the
table 9)
WEP-30L(config):/interface/wlan1-va0/vap/captive-portal/scenarios/scenario-redirect# exit
WEP-30L(config):/interface/wlan1-va0/vap/captive-portal/scenarios# exit
WEP-30L(config):/interface/wlan1-va0/vap/captive-portal# enabled true
WEP-30L(config):/interface/wlan1-va0/vap/captive-portal# exit
WEP-30L(config):/interface/wlan1-va0/vap# radius
WEP-30L(config):/interface/wlan1-va0/vap/radius# auth-address X.X.X.X (where X.X.X.X — IP address of the
RADIUS server used for authorization)
WEP-30L(config):/interface/wlan1-va0/vap/radius# auth-password secret (where secret — password for the
RADIUS server used for authorization)
WEP-30L(config):/interface/wlan1-va0/vap# save (save changes)
```

Table 9 — Setting up a URL template for external Captive Portal

Parameter	Description
<NAS_ID>	NAS ID set on VAP or in the system. If neither of these parameters is set, then the MAC address of the access point will be used as NAS ID in RADIUS and HTTP(S) packets
<SWITCH_URL>	Domain name that is shown to the client when redirected
<AP_MAC>	MAC address of the access point
<CLIENT_MAC>	MAC address of the client
<SSID>	SSID
<ORIGINAL_URL>	URL that the client originally requested

6.3.8 Advanced VAP settings

Assignment of VLAN-ID on VAP
WEP-30L(config):/interface/wlan1-va0/vap# **vlan-id X** (where X — VLAN-ID number on VAP)

Enabling Band Steer mode
WEP-30L(config):/interface/wlan1-va0/vap# **band-steer-mode true** (enabling Band Steer mode. To disable, enter **false**)

Enabling VLAN trunk on VAP
WEP-30L(config):/interface/wlan1-va0/vap# **vlan-trunk true** (enabling VLAN trunk on VAP. To disable, enter **false**)

Enabling General VLAN on VAP

WEP-30L(config):/interface/wlan1-va0/vap# **general-vlan-mode true** (enabling General VLAN on SSID. To disable, enter **false**)
WEP-30L(config):/interface/wlan1-va0/vap# **general-vlan-id X** (where X — General VLAN number)

Selection of the prioritization method
WEP-30L(config):/interface/wlan1-va0/vap# **priority-by-dscp false** (priority analysis from CoS field (Class of Service) of the tagged packets. Value by default: **true**. In this case, the priority from DSCP header field of the IP packet is analyzed)

Enabling MFP (802.11W)
WEP-30L(config):/interface/wlan1-va0/vap/ap-security# **mfp required** (enable management frame protection. **required** — requires MFP support from client, clients without an MFP support will not be able to connect. **capable** — compatible with MFP, clients without an MFP support can connect. To disable, enter **off**)

Enabling use of TLS at authorization
WEP-30L(config):/interface/wlan1-va0/vap/radius# **tls-enable true** (use TLS for authorization process. To disable, enter **false**)

Enabling hidden SSID
WEP-30L(config):/interface/wlan1-va0/vap# **hidden true** (enabling hidden SSID. To disable, enter **false**)

Enabling client isolation on VAP

WEP-30L(config):/interface/wlan1-va0/vap# **station-isolation true** (enable traffic isolation between clients within a single VAP. To disable, enter **false**)

Client limitation on VAP

WEP-30L(config):/interface/wlan1-va0/vap# **sta-limit X** (where X — maximum allowable number of clients connected to the virtual network)

Enabling multicast replication on VAP

WEP-30L(config):/interface/wlan1-va0/vap# **wmf-bss-enable true** (enable multicast traffic replication on VAP. To disable, enter **false**)

Enabling Minimal Signal and Roaming Signal

WEP-30L(config):/interface/wlan1-va0/vap# **check-signal-enable true** (enable the use of Minimal Signal functionality. To disable, enter **false**)
WEP-30L(config):/interface/wlan1-va0/vap# **min-signal X** (where X — RSSI threshold value, when reached, the point will disconnect the client from the VAP. The parameter can take values from -100 to -1)
WEP-30L(config):/interface/wlan1-va0/vap# **check-signal-timeout X** (where X — time period in seconds, after which the decision is made to disconnect the client equipment from the virtual network)
WEP-30L(config):/interface/wlan1-va0/vap# **roaming-signal X** (where X — RSSI threshold value, when reached, the client equipment is switched to another access point. The parameter can take values from -100 to -1.
The **roaming-signal** parameter should be lower than **min-signal**: if **min-signal**= -75 dBm, then **roaming-signal** should be equal to -70 dBm, for example)
WEP-30L(config):/interface/wlan1-va0/vap# **save** (save changes)

Enabling subscribers traffic transmission outside of GRE tunnel

WEP-30L(config):/interface/wlan1-va0/vap# **local-switching true** (enabling subscribers traffic transmission outside of GRE tunnel. To disable, enter **false**. By default: disabled)

Configuring speed limit

Configuring traffic shaper from the clients (each separately) connected to this VAP towards the access point:

```
WEP-30L(config):/interface/wlan1-va0/vap# shaper-per-sta-rx
WEP-30L(config):/interface/wlan1-va0/vap/shaper-per-sta-rx# value X (where X — maximum speed in kbps)
WEP-30L(config):/interface/wlan1-va0/vap/shaper-per-sta-rx# mode kbps (enabling shaper. To disable, enter off)
WEP-30L(config):/interface/wlan1-va0/vap/shaper-per-sta-rx# exit
WEP-30L(config):/interface/wlan1-va0/vap# save (save changes)
```

Configuring traffic shaper from the access point towards the clients (each separately) connected to this VAP:

```
WEP-30L(config):/interface/wlan1-va0/vap# shaper-per-sta-tx
WEP-30L(config):/interface/wlan1-va0/vap/shaper-per-sta-tx# value X (where X — maximum speed in kbps)
WEP-30L(config):/interface/wlan1-va0/vap/shaper-per-sta-tx# mode kbps (enabling shaper. To disable, enter off)
WEP-30L(config):/interface/wlan1-va0/vap/shaper-per-sta-tx# exit
WEP-30L(config):/interface/wlan1-va0/vap# save (save changes)
```

Configuring shaper from the clients (in total) connected to this VAP towards the access point:

```
WEP-30L(config):/interface/wlan1-va0/vap# shaper-per-vap-rx
WEP-30L(config):/interface/wlan1-va0/vap/shaper-per-vap-rx# value X (where X — maximum speed in kbps)
WEP-30L(config):/interface/wlan1-va0/vap/shaper-per-vap-rx# mode kbps (enabling shaper. To disable, enter off)
WEP-30L(config):/interface/wlan1-va0/vap/shaper-per-vap-rx# exit
WEP-30L(config):/interface/wlan1-va0/vap# save (save changes)
```

Configuring shaper from the access point towards the clients (in total) connected to this VAP:

```
WEP-30L(config):/interface/wlan1-va0/vap# shaper-per-vap-tx
WEP-30L(config):/interface/wlan1-va0/vap/shaper-per-vap-tx# value X (where X — maximum speed in kbps)
WEP-30L(config):/interface/wlan1-va0/vap/shaper-per-vap-tx# mode kbps (enabling shaper. To disable, enter off)
WEP-30L(config):/interface/wlan1-va0/vap/shaper-per-vap-tx# exit
WEP-30L(config):/interface/wlan1-va0/vap# save (save changes)
```

Configuring MAC access control

```
WEP-30L(config):/interface/wlan1-va0/vap# acl
WEP-30L(config):/interface/wlan1-va0/vap/acl# mac
WEP-30L(config):/interface/wlan1-va0/vap/acl/mac# add XX:XX:XX:XX:XX:XX (where XX:XX:XX:XX:XX:XX — MAC
address of the device, to which it is required to allow/deny access. To remove an address from the list,
use the del command)
WEP-30L(config):/interface/wlan1-va0/vap/acl/mac# exit
WEP-30L(config):/interface/wlan1-va0/vap/acl# policy allow (policy selection. Possible values: allow — allow
connections only to those clients whose MAC addresses are in the list; deny — deny connections to clients
whose MAC addresses are in the list. By default: deny)
WEP-30L(config):/interface/wlan1-va0/vap/acl# enable true (enabling MAC access control. To disable,
enter false)
```

Configuring connection blocking for users who spoof the MAC address of a wired network device

If, for security reasons, it is necessary to implement protection against connections of users duplicating the MAC address of a wired device (gateway, PC, etc.), use the **fdb-filtering** setting, which has the following operating modes:
on-connect mode blocks all devices connection attempts via Wi-Fi if the MAC address has already been learned on the Ethernet port of the access point;
by-eth-event mode disconnects a connected client via Wi-Fi if its MAC address has been learned on the Ethernet port of the access point (the mode helps clear the old client record when roaming);
full mode combines all the previous ones, that is, it blocks the connection of a new user via Wi-Fi and disconnects the previously connected one if its MAC address matches with the device connected to the Ethernet interface.

> When setting the **full** and **on-connect** modes, the roaming of Wi-Fi clients may deteriorate. So, during operation, all broadcast packets from a client reach the other access points of the network and its MAC is learned on all network access points, so when the client roaming, if its MAC address is in the Ethernet port list, reconnection may take a long time.

```
WEP-30L(config):/interface/wlan1-va0/vap# fdb-filtering
WEP-30L(config):/interface/wlan1-va0/vap/fdb-filtering# enabled true (enabling function. To disable,
enter false. Default: false)
WEP-30L(config):/interface/wlan1-va0/vap/fdb-filtering# mode full (operating mode selection.
Default: by-eth-event)
```

802.11r configuration

This type of roaming is available only for client devices supporting 802.11r.

802.11r roaming is possible only between VAPs with WPA2/WPA3-Personal and WPA2/WPA3-Enterprise security modes.

See instructions for configuring VAP with WPA2-Personal security mode and others in Configuration of VAP with WPA-Personal security mode section.

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-30L(config):/interface/wlan1-va0/vap/ft-config# enabled false
WEP-30L(config):/interface/wlan1-va0/vap/ft-config# r1-key-holder-id E8:28:C1:FC:D6:80 (MAC address of the VAP. Can be viewed in ifconfig command output)
WEP-30L(config):/interface/wlan1-va0/vap/ft-config# r0-key-holder-id 12345 (unique key for this VAP)
WEP-30L(config):/interface/wlan1-va0/vap/ft-config# mobility-domain 100 (domain should match on remote VAPs)
WEP-30L(config):/interface/wlan1-va0/vap/ft-config# mac
WEP-30L(config):/interface/wlan1-va0/vap/ft-config/mac# add E4:5A:D4:E2:C4:B0 (MAC address of VAP interface of remote access point — AP2)
WEP-30L(config):/interface/wlan1-va0/vap/ft-config/mac# E4:5A:D4:E2:C4:B0
WEP-30L(config):/interface/wlan1-va0/vap/ft-config/mac/E4:5A:D4:E2:C4:B0# r0-kh-id 23456 (unique key of remote VAP access point AP2 — r0-key-holder-id)
WEP-30L(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 remote VAP on AP2)
WEP-30L(config):/interface/wlan1-va0/vap/ft-config/mac/E4:5A:D4:E2:C4:B0# r0-kh-key 0102030405060708 (random key. It shouldn't match with r1-kh-key of AP1, but it should match with r1-kh-key of remote AP2)
WEP-30L(config):/interface/wlan1-va0/vap/ft-config/mac/E4:5A:D4:E2:C4:B0# r1-kh-key 0001020304050607 (random key. It shouldn't match with r0-kh-key of AP1, but it should match with r0-kh-key of remote AP2)
WEP-30L(config):/interface/wlan1-va0/vap/ft-config/mac/E4:5A:D4:E2:C4:B0# exit
WEP-30L(config):/interface/wlan1-va0/vap/ft-config/mac# exit
WEP-30L(config):/interface/wlan1-va0/vap/ft-config# enabled true (enable access point operation by 802.11r protocol)
WEP-30L(config):/interface/wlan1-va0/vap/ft-config# save (save changes)
```

Configuring 802.11r on AP2

```
WEP-30L(config):/interface/wlan1-va0/vap/ft-config# enabled false
WEP-30L(config):/interface/wlan1-va0/vap/ft-config# r1-key-holder-id E4:5A:D4:E2:C4:B0 (MAC address of the VAP. Can be viewed in ifconfig command output)
WEP-30L(config):/interface/wlan1-va0/vap/ft-config# r0-key-holder-id 23456 (unique key for this VAP)
WEP-30L(config):/interface/wlan1-va0/vap/ft-config# mobility-domain 100 (domain should match on remote VAPs)
WEP-30L(config):/interface/wlan1-va0/vap/ft-config# mac
WEP-30L(config):/interface/wlan1-va0/vap/ft-config/mac# add E8:28:C1:FC:D6:80 (MAC address of VAP interface of remote access point — AP1)
WEP-30L(config):/interface/wlan1-va0/vap/ft-config/mac# E8:28:C1:FC:D6:80
WEP-30L(config):/interface/wlan1-va0/vap/ft-config/mac/E8:28:C1:FC:D6:80# r0-kh-id 12345 (unique key of remote VAP on access point AP1 — r0-key-holder-id)
WEP-30L(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 remote VAP on AP1)
WEP-30L(config):/interface/wlan1-va0/vap/ft-config/mac/E8:28:C1:FC:D6:80# r0-kh-key 0001020304050607 (random key. It shouldn't match with r1-kh-key of AP2, but it should match with r1-kh-key of remote AP1)
WEP-30L(config):/interface/wlan1-va0/vap/ft-config/mac/E8:28:C1:FC:D6:80# r1-kh-key 0102030405060708 (random key. It shouldn't match with r0-kh-key of AP2, but it should match with r0-kh-key of remote AP1)
WEP-30L(config):/interface/wlan1-va0/vap/ft-config/mac/E8:28:C1:FC:D6:80# exit
WEP-30L(config):/interface/wlan1-va0/vap/ft-config/mac# exit
WEP-30L(config):/interface/wlan1-va0/vap/ft-config# enabled true (enable access point operation by 802.11r protocol)
WEP-30L(config):/interface/wlan1-va0/vap/ft-config# save (save changes)
```

802.11k configuration

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

The use of 802.11k allows to reduce the time for finding another network when roaming, since the client 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 client 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-30L(config):/interface/wlan1-va0/vap/w80211kv-config# enabled false
WEP-30L(config):/interface/wlan1-va0/vap/w80211kv-config# mac
WEP-30L(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-30L(config):/interface/wlan1-va0/vap/w80211kv-config/mac# E8:28:C1:FC:D6:90
WEP-30L(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-30L(config):/interface/wlan1-va0/vap/w80211kv-config/mac/E8:28:C1:FC:D6:90# exit
WEP-30L(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-30L(config):/interface/wlan1-va0/vap/w80211kv-config/mac# E8:28:C1:FC:D6:70
WEP-30L(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-30L(config):/interface/wlan1-va0/vap/w80211kv-config/mac/E8:28:C1:FC:D6:70# exit
WEP-30L(config):/interface/wlan1-va0/vap/w80211kv-config/mac# exit
WEP-30L(config):/interface/wlan1-va0/vap/w80211kv-config# enabled true (enabling access point operation via 802.11k protocol)
WEP-30L(config):/interface/wlan1-va0/vap/w80211kv-config# save (save changes)
```

6.4 Radio configuration

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

Change of operation channel and radio interface power

```
WEP-30L(root):/# configure
WEP-30L(config):/# interface
WEP-30L(config):/interface# wlan0
WEP-30L(config):/interface/wlan0# wlan
WEP-30L(config):/interface/wlan0/wlan# radio
WEP-30L(config):/interface/wlan0/wlan/radio# channel X (where X is the number of the static channel on which the point will operate)
WEP-30L(config):/interface/wlan0/wlan/radio# auto-channel false (disabling Auto Channel. To enable, enter true)
WEP-30L(config):/interface/wlan0/wlan/radio# use-limit-channels false (disable Use Limit Channels. To enable, enter true)
WEP-30L(config):/interface/wlan0/wlan/radio# bandwidth X (where X — channel width. Parameter can take the following value: for Radio 1: 20, 40; Radio 2: 20, 40, 80)
WEP-30L(config):/interface/wlan0/wlan/radio# tx-power X (where X — power level, dBm. Parameter can take the following value: for Radio 1: 0-16 dBm; for Radio 2: 0-19 dBm)
WEP-30L(config):/interface/wlan0/wlan/radio# tx-power-min X (where X — minimum power level, dBm. Parameter can take the following value: for Radio 1: 0–16 dBm; for Radio 2: 0–19 dBm)
WEP-30L(config):/interface/wlan0/wlan/radio# tx-power-max X (where X — maximum power level, dBm. Parameter can take the following value: for Radio 1: 0–16 dBm; for Radio 2: 0–19 dBm)
WEP-30L(config):/interface/wlan0/wlan/radio# 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.

6.4.1 Advanced Radio settings

Configuring the limited list of channels

```
WEP-30L(config):/interface/wlan0/wlan/radio# use-limit-channels true (enabling use of limited list of channels in channel autoselection operation. To disable, enter false)
WEP-30L(config):/interface/wlan0/wlan/radio# 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-30L(config):/interface/wlan0/wlan/radio# 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-30L(config):/interface/wlan0/wlan/radio# sgi true (enabling the use of a Short Guard Interval for data transmission of 400 ns instead of 800 ns. To disable, enter false)
```

Enabling STBC

```
WEP-30L(config):/interface/wlan0/wlan/radio# stbc true (enabling the Space-Time Block Coding (STBC) method, aimed at improving the reliability of data transmission. To disable, enter false)
```

Enabling aggregation

```
WEP-30L(config):/interface/wlan0/wlan/radio# aggregation true (enabling aggregation on Radio — support for AMPDU/AMSDU. To disable, enter false)
```

Enabling the short preamble

```
WEP-30L(config):/interface/wlan0/wlan/radio# short-preamble true (enabling the short packet preamble. To disable, enter false)
```

Enabling the Wi-Fi Multimedia (WMM)

```
WEP-30L(config):/interface/wlan0/wlan/radio# 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-30L(config):/interface/wlan1/wlan/radio# **dfs X** (where X — DFS mechanism operating mode. Possible values: **forced** — the mechanism is disabled, DFS channels are available for selection; **auto** — the mechanism is enabled; **disabled** — the mechanism is disabled, DFS channels are unavailable for selection)

Enabling automatic channel width switch mode

WEP-30L(config):/interface/wlan0/wlan/radio# **obss-coex true** (enabling automatic channel width switch mode from 40 MHz to 20 MHz with a loaded radio environment. To disable, enter **false**)

Enabling Broadcast/Multicast shaper

WEP-30L(config):/interface/wlan0/wlan/radio-2g# **tx-broadcast-limit X** (where X — restricting broadcast/multicast traffic over the wireless network, the limit for broadcast traffic is specified, packets/s)

Enabling QoS and parameter changes

WEP-30L(config):/interface/wlan0/wlan/radio# **qos**

WEP-30L(config):/interface/wlan0/wlan/radio/qos# **enable true** (enabling the use of Quality of Service functions. To disable, enter **false**)

WEP-30L(config):/interface/wlan0/wlan/radio/qos# **edca-ap** (configuring QoS parameters of the access point, traffic is transmitted from the access point to the client)

WEP-30L(config):/interface/wlan0/wlan/radio/qos/edca-ap# **bk** (configuring QoS parameters for low-priority high-bandwidth queues (802.1p priorities: cs1, cs2))

WEP-30L(config):/interface/wlan0/wlan/radio/qos/edca-ap/bk# **aifs X** (where X — waiting time for frames of data, measured in slots. Takes the values 1–255)

WEP-30L(config):/interface/wlan0/wlan/radio/qos/edca-ap/bk# **cwmin X** (X — the initial value of the time to wait before resending a frame, specified in milliseconds. Accepts values: 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023. The cwMin value cannot exceed the cwMax value)

WEP-30L(config):/interface/wlan0/wlan/radio/qos/edca-ap/bk# **cwmax X** (where X — maximum timeout value before resending a frame, specified in milliseconds. Accepts values: 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023. The cwMax value must be greater than the cwMin value)

WEP-30L(config):/interface/wlan0/wlan/radio/qos/edca-ap/bk# **txop X** (where X — the time interval in milliseconds when the WME client station has the right to initiate data transmission over the wireless medium to the access point. Max value 65535 milliseconds)

WEP-30L(config):/interface/wlan0/wlan/radio/qos/edca-ap/bk# **exit**

WEP-30L(config):/interface/wlan0/wlan/radio/qos/edca-ap# **exit**

WEP-30L(config):/interface/wlan0/wlan/radio/qos# **edca-sta** (configuring QoS parameters of the client station (traffic is transmitted from the client station to the access point))

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

6.5 Configuring DHCP option 82

DHCP option 82 is configured separately for each radio interface. This section provides examples of configuring option 82 for Radio 2.4 GHz — wlan0.

DHCP snooping operating modes:

- **ignore** – option 82 processing is disabled. Default value;
- **replace** – access point substitutes or replaces the value of option 82;
- **remove** – access point removes the value of option 82.

Changing the operating mode of DHCP option 82

```
WEP-30L(root):/# configure
WEP-30L(config):/# interface
WEP-30L(config):/interface# wlan0 (configuring will be done for Radio 2.4 GHz. To configure option 82 on Radio 5 GHz, enter wlan1)
WEP-30L(config):/interface/wlan0# common
WEP-30L(config):/interface/wlan0/common# dhcp-snooping
WEP-30L(config):/interface/wlan0/common/dhcp-snooping# dhcp-snooping-mode replace (selection of DHCP snooping operation in the mode of replacement or substitution of option 82)
```

If on the radio interface the 82 option processing policy is configured to **replace**, the following parameters become available for configuration:

Configuring Option 82 parameters

```
WEP-30L(config):/interface/wlan0/common/dhcp-snooping# dhcp-option-82-CID-format custom (where custom — replacement of the CID content with the value specified in the dhcp-option-82-custom-CID parameter. The parameter can take values: APMAC-SSID — replacement of the CID content with <MAC address of the access point>-<SSID name>. SSID — replacement of the CID content with SSID name, to which the client is connected. By default: APMAC-SSID)
WEP-30L(config):/interface/wlan0/common/dhcp-snooping# dhcp-option-82-RID-format custom (where custom — replacement of the RID content with the value specified in the dhcp-option-82-custom-RID parameter. The parameter can take values: ClientMAC — replacement of the RID content with MAC address of the client device.  APMAC — replacement of the RID content with MAC address of the access point. APdomain — replacement of the RID content with the domain where the access point is located. By default: ClientMAC)
WEP-30L(config):/interface/wlan0/common/dhcp-snooping# dhcp-option-82-custom-CID longstring (where longstring — value from 1 to 52 characters, which will be transmitted in CID. If the value of dhcp-option-82-custom-CID parameter is not defined, the access point will change the CID to the default value: <MAC address of the access point>-<SSID name>)
WEP-30L(config):/interface/wlan0/common/dhcp-snooping# dhcp-option-82-custom-RID longstring (where longstring — value from 1 to 63 characters, which will be transmitted in RID. If the value of dhcp-option-82-custom-RID parameter is not defined, the access point will change the RID to the default value: MAC address of the client device)
WEP-30L(config):/interface/wlan0/common/dhcp-snooping# dhcp-option-82-MAC-format radius (selecting octet delimiter of the MAC address which is transmitted in RID and CID. radius — a dash is used as a delimiter: AA-BB-CC-DD-EE-FF; default — a colon is used as a delimiter: AA:BB:CC:DD:EE:FF)
```

6.6 Configuring WDS

When configuring a WDS connection, it is necessary that the devices connected via WDS have the same channel and channel width selected in the radio interface settings. More detailed information on configuring the radio interface via the command line can be found in the Radio Configuration section.

The configuration of a WDS connection on the 5 GHz Radio interface (wlan1) is described below.

Configuring WDS

```
WEP-30L(root):/# configure
WEP-30L(config):/# interface
WEP-30L(config):/interface# wlan1-wds0 (WDS link selection. Possible values for Radio 2.4 GHz: wlan0–wds0 – wlan0–wds3; for Radio 5 GHz: wlan1–wds0 – wlan1–wds3)
WEP-30L(config):/interface/wlan1-wds0# wds
WEP-30L(config):/interface/wlan1-wds0/wds# mac-addr XX:XX:XX:XX:XX:XX (MAC address of the Radio interface of the remote access point, which can be found by entering the monitoring radio-interface command on the remote access point)
WEP-30L(config):/interface/wlan1-wds0/wds# exit
WEP-30L(config):/interface/wlan1-wds0# common
WEP-30L(config):/interface/wlan1-wds0/common# enabled true (enable WDS link. To disable, enter false)
WEP-30L(config):/interface/wlan1-wds0/common# exit
WEP-30L(config):/interface/wlan1-wds0# exit
WEP-30L(config):/interface# wlan1 (when configuring WDS on Radio 2.4 GHz, enter wlan0)
WEP-30L(config):/interface/wlan1# wlan
WEP-30L(config):/interface/wlan1/wlan# wds
WEP-30L(config):/interface/wlan1/wlan/wds# security-mode WPA2 (select WPA2 security mode. Possible values: WPA2, off — no password)
WEP-30L(config):/interface/wlan1/wlan/wds# key-wpa password123 (key/password required to connect to the remote access point. The key length should be between 8 and 63 characters)
WEP-30L(config):/interface/wlan1/wlan/wds# enabled true (enable WDS. To disable, enter false)
WEP-30L(config):/interface/wlan1/wlan/wds# save
```

The configuration of the **remote access point** is done in a similar way.

6.7 Configuring Z-Wave

✓ For WEP-30L-Z only.

Configuring Z-Wave

```
WEP-30L-Z(root):/# configure
WEP-30L-Z(config):/# z-wave
WEP-30L-Z(config):/z-wave# enabled true (where true — enable the Z-Wave Hub. Default: false)
WEP-30L-Z(config):/z-wave# platform-address smart.eltex-co.ru (where smart.eltex-co.ru — "Eltex Smart Control" platform address. Default: smart.eltex-co.ru)
WEP-30L-Z(config):/z-wave# platform-port 8072 (where 8072 — communication port for "Eltex Smart Control". When the "Secure connection" is unchecked, specify the port 8070. Default: 8072)
WEP-30L-Z(config):/z-wave# secure true (where true — enable the secure connection. To disable, enter false)
WEP-30L-Z(config):/z-wave# syslog true (where true — enable logging. To disable, enter false)
WEP-30L-Z(config):/z-wave# manage-config zway-reconfigure (apply settings for Z-Wave Hub)
WEP-30L-Z(config):/z-wave# save (save changes)
```

Resetting Z-Wave Hub

```
WEP-30L-Z(root):/# manage-config zway-reset (reset the Z-Wave Hub and delete the connected devices)
```

6.8 System settings

6.8.1 Device firmware update

Device firmware update via tftp

WEP-30L(root):/# **firmware upload tftp <ip address of tftp server> <Firmware file name>** (example: firmware upload tftp 192.168.1.15 WEP-30L-2.5.2_build_X.tar.gz)

WEP-30L(root):/# **firmware upgrade**

Device firmware update via http

WEP-30L(root):/# **firmware upload http <URL for firmware uploading>** (example: firmware upload http http://192.168.1.100:8080/files/WEP-30L-2.5.2_build_X.tar.gz)
WEP-30L(root):/# **firmware upgrade**

Switching to access point firmware backup

WEP-30L(root):/# **firmware switch**

6.8.2 Device configuration management

Restoring the default configuration without saving the access parameters

WEP-30L(root):/# **manage-config reset-to-default**

Restoring the default configuration with saving the access parameters

WEP-30L(root):/# **manage-config reset-to-default-without-management**

Download the device configuration file to TFTP server

WEP-30L(root):/# **manage-config download tftp <tftp server ip address>** (example: manage-config download tftp 192.168.1.15)

Upload configuration file from TFTP server to the device

WEP-30L(root):/# **manage-config upload tftp <tftp server ip address> <Configuration file name>** (example: manage-config upload tftp 192.168.1.15 config.json)
WEP-30L(root):/# **manage-config apply** (apply configuration to the access point)

6.8.3 Device reboot

The command to reboot the device

```
WEP-30L(root):/# reboot
```

6.8.4 Configuring the authentication mode

The device has a factory user account of *admin* with a password of *password*. This account cannot be deleted. You can change your password using the following commands.

Changing the password for admin account

```
WEP-30L(root):/# configure
WEP-30L(config):/# authentication
WEP-30L(config):/authentication# admin-password <A new password for admin account> (from 1 to 64
characters, including Latin letters and digits)
WEP-30L(config):/authentication# save
```

It is possible to create additional users for local authentication as well as authentication via RADIUS.

New users should be assigned one of two roles:
admin — a user with this role will have full access to configure and monitor the base station;
viewer — a user with this role will only have access to base station monitoring.

Adding new users

```
WEP-30L(root):/# configure
WEP-30L(config):/# authentication
WEP-30L(config):/authentication# user
WEP-30L(config):/authentication/user# add userX (where userX — new account name. To delete, use the
command del)
WEP-30L(config):/authentication/user# userX
WEP-30L(config):/authentication/user/userX# login userX (where userX — new account name)
WEP-30L(config):/authentication/user/userX# password <A new password for userX account> (from 1 to 64
characters, including Latin letters and digits)
WEP-30L(config):/authentication/user/userX# role admin (the user is given configuration rights. Acceptable
value: viewer — the account will only have access to monitoring)
WEP-30L(config):/authentication/user/userX# save
```

To authenticate via a RADIUS server, you need to configure access parameters to it.

Configuring access parameters to the RADIUS server

```
WEP-30L(root):/# configure
WEP-30L(config):/# authentication
WEP-30L(config):/authentication# radius
WEP-30L(config):/authentication/radius# auth-address X.X.X.X (where X.X.X.X — IP address of the RADIUS server)
WEP-30L(config):/authentication/radius# auth-port X (where X — port of the RADIUS server, which is used for authentication and authorization. Default: 1812)
WEP-30L(config):/authentication/radius# auth-password secret (where secret — key of the RADIUS server, which is used for authentication and authorization)
WEP-30L(config):/authentication/radius# exit
WEP-30L(config):/authentication# radius-auth true (enabling authentication mode via RADIUS server. To disable, enter false)
WEP-30L(config):/authentication# save
```

When the authentication via the RADIUS server is used, it is required to create a local account that will be similar to the account on the RADIUS server.
In this case, the local account should have a specified role with access rights (admin or viewer).
If the RADIUS server is unavailable, authentication will take place using a local account.

6.8.5 Setting the date and time

Commands to configure NTP server time synchronization

```
WEP-30L(root):/# configure
WEP-30L(config):/# date-time
WEP-30L(config):/date-time# mode ntp (enable NTP operation mode)
WEP-30L(config):/date-time# ntp
WEP-30L(config):/date-time/ntp# server <NTP server IP address> (NTP server configuration)
WEP-30L(config):/date-time/ntp# alt-servers (configuring additional NTP servers)
WEP-30L(config):/date-time/ntp/alt-servers# add <Domain name/IP address of NTP server in the configuration> (creating a configuration section for an additional NTP server. Maximum number: 8. To delete, enter the del command)
WEP-30L(config):/date-time/ntp/alt-servers# exit
WEP-30L(config):/date-time/ntp# exit
WEP-30L(config):/date-time# common
WEP-30L(config):/date-time/common# timezone 'Asia/Novosibirsk (Novosibirsk)' (timezone configuration)
WEP-30L(config):/date-time/common# save (save changes)
```

6.8.6 Advanced system settings

Enabling global isolation

```
WEP-30L(root):/# configure
WEP-30L(config):/# system
WEP-30L(config):/system# global-station-isolation true (enabling global traffic isolation between clients of different VAPs and different radio interfaces. To disable, enter false)
WEP-30Lconfig):/system# save (save changes)
```

Changing device name

```
WEP-30L(root):/# configure
WEP-30L(config):/# system
WEP-30L(config):/system# hostname WEP-30L_room2 (where WEP-30L_room2 is a new device name. The parameter can accept values from 1 to 63 characters: capital and lowercase Latin letters, digits, hyphen character “-” (hyphen can not be the last character in name). By default: WEP-30L)
WEP-30L(config):/system# save (save changes)
```

Changing geographical domain

```
WEP-30L(root):/# configure
WEP-30L(config):/# system
WEP-30L(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-30L(config):/system# save (save changes)
```

Changing Radius NAS-ID

```
WEP-30L(root):/# configure
WEP-30L(config):/# system
WEP-30L(config):/system# nas-id Lenina_1.Novovsibirsk.root (where Lenina_1.Novovsibirsk.root — identifier of this access point. The parameter is intended to identify the device on the RADIUS server if RADIUS expects a value other than the MAC address. Default: MAC address of the access point)
WEP-30L(config):/system# save (save changes)
```

Configuring LLDP

```
WEP-30L(root):/# configure
WEP-30L(config):/# lldp
WEP-30L(config):/lldp# enabled true (enable the LLDP. To disable, enter false. Default: true)
WEP-30L(config):/lldp# tx-interval 60 (changing the period for sending LLDP messages. Default: 30)
WEP-30L(config):/lldp# system-name WEP-30L_reserv (where WEP-30L_reserv — new device name. Default: WEP-30L)
WEP-30L(config):/lldp# save (save changes)
```

Changing password

```
WEP-30L(root):/# configure
WEP-30L(config):/# authentication
WEP-30L(config):/authentication# admin-password newpassword (where newpassword — new password to login to the access point. By default: password)
WEP-30L(config):/authentication# save (save changes)
```

6.9 Configuring Captive Portal

Configuring parameters of Captive Portal

```
WEP-30L(root):/# configure
WEP-30L(config):/# captive-portal
WEP-30L(config):/captive-portal# ap-ip-alias <Domain name> (domain name, to which clients will be redirected. By default: redirect.loc)
WEP-30L(config):/captive-portal# tinyproxy-https true (enable client redirection via HTTPS. To redirect via HTTP, enter false. By default: false)
```

A DNS request for the domain name specified in ap-ip-alias will be intercepted by the access point. A response will be sent to this request, and the response will contain the IP address of the access point.

Configuring the names of parameters passed by the authorization web server

```
WEP-30L(root):/# configure
WEP-30L(config):/# captive-portal
WEP-30L(config):/captive-portal# web-redirector
WEP-30L(config):/captive-portal/web-redirector# param-names
WEP-30L(config):/captive-portal/web-redirector/param-names# redirect_url original_url (setting the name of the parameter containing the original URL requested by the client. The client will be redirected to this URL if the authorization is successful)
WEP-30L(config):/captive-portal/web-redirector/param-names# error_url err_url (setting the name of the parameter containing the URL where the client will be redirected in case of an authorization error)
WEP-30L(config):/captive-portal/web-redirector/param-names# username login (setting the name of the parameter containing the login for the client)
WEP-30L(config):/captive-portal/web-redirector/param-names# password pass (setting the name of the parameter containing the password for the client)
```

The setting is needed if the parameter names in the http response with code 302 differ from the default names accepted by the access point.

6.9.1 Portal Certificate Management

Uploading certificate for HTTPS redirect via TFTP

```
WEP-30L(root):/# manage-certificates portal upload tftp <IP address of TFTP server> <File name>
(example: manage-certificates portal upload tftp 192.168.1.15 portal.pem)
```

Uploading certificate for HTTPS redirect via http

```
WEP-30L(root):/# manage-certificates portal upload http <URL for uploading the firmware file>
(example: manage-certificates portal upload http http://192.168.1.100:8080/files/portal.pem)
```

Erasing the certificate

```
WEP-30L(root):/# manage-certificates portal erase
```

6.10 Configuring APB service

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

Commands for APB service configuration

```
WEP-30L(root):/# configure
WEP-30L(config):/# captive-portal
WEP-30L(config):/captive-portal# apbd
WEP-30L(config):/captive-portal/apbd# roam_service_url <APB service address>
(example: roam_service_url ws://192.168.1.100:8090/apb/broadcast)
WEP-30L(config):/captive-portal/apbd# enabled true (enabling APB service. To disable, enter false)
WEP-30L(config):captive-portal/apbd# save (save changes)
```

6.11 Configuring remote traffic dump capture

The remote-capture section performs remote recording of a traffic dump.
The device supports the RPCAP protocol, which allows recording a traffic dump from the device interface on a remote machine in online mode.

✓ To remotely capture packets from radio interfaces, it is required to connect the interfaces **radio0** and **radio1**
WEP-30L(root):/#**ifconfig radio0 up** (radio0 — interface corresponds to the 2.4 GHz range (wlan0));
WEP-30L(root):/#**ifconfig radio1 up** (radio1 — interface corresponds to the 5 GHz range (wlan1)).

✓ For successful remote packet capture, one VAP should be enabled in each of the respective 2.4 GHz and 5 GHz bands.

Commands for configuring remote-capture

```
WEP-30L(root):/# configure
WEP-30L(config):/# remote-capture
WEP-30L(config):/remote-capture# enabled true (true — enabling. To disable, enter false)
WEP-30L(config):/remote-capture# port 2002 (2002 — port number used to connect the remote machine. The parameter takes values from 1025 to 65530. By default: 2002)
WEP-30L(config):/remote-capture# save (save changes)
```

For remote connection, use the RPCAP protocol, specify the device IP address and port. For this, for example, one can use the Wireshark program. Then it is required to get a list of interfaces for sniffing from the device, select one of them and start dumping from the remote interface.

6.12 Monitoring

6.12.1 Wi-Fi clients

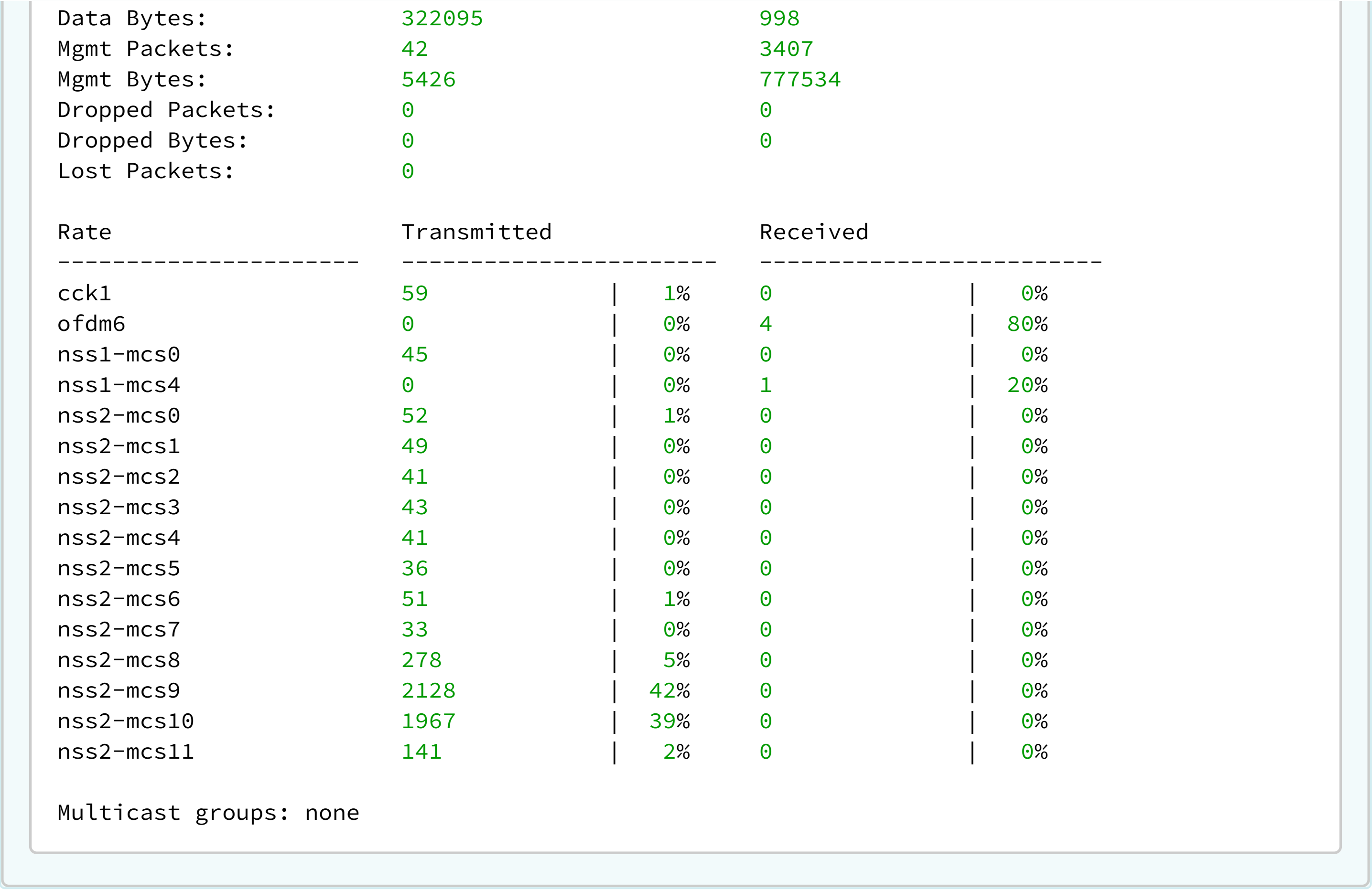
WEP-30L(root):/# **monitoring associated-clients**

```
index                       | 0
interface                   | wlan1-va0
state                       | ASSOC SLEEP AUTH_SUCCESS
hw-addr                     | 0a:03:42:63:73:f5
ssid                        | Enterprise
ip-addr                     | 10.24.80.78
username                    | user
domain                      | enterprise.service.root
authorized                  | true
captive-portal-vap          | false
enterprise-vap              | true
rx-retry-count              | 903
tx-fails                    | 2
tx-period-retry             | 1887
tx-retry-count              | 13063
rssi-1                      | -28
rssi-2                      | -44
rssi-3                      | -28
rssi-4                      | -25
snr-1                       | 13
snr-2                       | 12
snr-3                       | 12
snr-4                       | 15
tx-rate                     | VHT NSS2-MCS8 SGI 173.3
rx-rate                     | VHT NSS2-MCS8 NO SGI 156
rx-bw                       | 20M
rx-bw-all                   | 20M
tx-bw                       | 20M
uptime                      | 00:01:04
multicast-groups-count      | 1
wireless-mode               | ac
perftest-capable            | false
link-capacity               | 90
link-quality                | 97
link-quality-common         | 96
actual-tx-rate              | 1736
actual-rx-rate              | 1014
shaped-rx-rate              | 70075
actual-tx-pps               | 2625
actual-rx-pps               | 89
shaped-rx-pps               | 6020
name                        | 0

Rate                      Transmitted             Received
----------------------------------------------------------------------
Total Packets:          | 174133                | 136050                |
TX success:             | 99                    |                       |
Total Bytes:            | 211056771             | 113905486             |
Data Packets:           | 174126                | 2857                  |
Data Bytes:             | 211055846             | 1689787               |
 Mgmt Packets:          | 7                      | 133193                 |
 Mgmt Bytes:            | 353                    | 112052138              |
----------------------------------------------------------------------

 Rate                     Transmitted             Received
----------------------------------------------------------------------
 ofdm6                  | 26               |    0%|              33 |    0%|
 ofdm24                 | 0                |    0%|             324 |    0%|
 nss2-mcs4              | 0                |    0%|               1 |    0%|
 nss2-mcs5              | 0                |    0%|              44 |    0%|
 nss2-mcs6              | 0                |    0%|            1205 |    0%|
 nss2-mcs8              | 174107           |   99%|          134442 |   98%|
---------------------------------------------------------------------


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

6.12.2 WDS

WEP-30L(root):/# **monitoring wds-entries**

```
 index                    | 0
 hw-addr                  | 68:13:e2:35:d6:48
 interface                | wlan1
 rfid                     | -1
 wid                      | -1
 band                     | 5
 state                    | WIFI_WDS WIFI_WDS_RX_BEACON
 ip-addr                  | 100.109.1.207
 dhcp-request-status      | not requested
 authorized               | false
 captive-portal-vap       | false
 enterprise-vap           | false
 rx-retry-count           | 0
 tx-fails                 | 0
 tx-period-retry          | 0
 tx-retry-count           | 134
 rssi-1                   | -42
 rssi-2                   | -26
 rssi                     | -26
 snr-1                    | 33
 snr-2                    | 33
 snr                      | 33
 noise-1                  | -9
 noise-2                  | 7
 noise                    | 7
 tx-rate                  | HE NSS2 MCS9 SGI 229.4
 rx-rate                  | HE NSS1 MCS4 SGI 51.6
 rx-bw                    | 20M
 rx-bw-all                | 20M
 tx-bw                    | 20M
 uptime                   | 00:06:08
 mfp                      | false
 wireless-mode            | ax
 perftest-capable         | false
 link-quality             | 97
 link-quality-common      | 97
 actual-tx-rate           | 2
 actual-rx-rate           | 0
 shaped-rx-rate           | 0
 actual-tx-pps            | 14
 actual-rx-pps            | 0
 shaped-rx-pps            | 0
 link-capacity            | 1 (not changed)
 multicast-groups-count   | 0
 twt-support              | none
 name                     | 0

Rate                     Transmitted               Received
----------------------   -----------------------   -------------------------
Total Packets:           5006                      3412
TX success:              100
Total Bytes:             327521                    778532
Data Packets:            4964                      5
```



```
Data Bytes:              322095                    998
Mgmt Packets:            42                        3407
Mgmt Bytes:              5426                      777534
Dropped Packets:         0                         0
Dropped Bytes:           0                         0
Lost Packets:            0

Rate                     Transmitted               Received
----------------------   -----------------------   -------------------------
cck1                     59             |   1%     0              |   0%
ofdm6                    0              |   0%     4              |  80%
nss1-mcs0                45             |   0%     0              |   0%
nss1-mcs4                0              |   0%     1              |  20%
nss2-mcs0                52             |   1%     0              |   0%
nss2-mcs1                49             |   0%     0              |   0%
nss2-mcs2                41             |   0%     0              |   0%
nss2-mcs3                43             |   0%     0              |   0%
nss2-mcs4                41             |   0%     0              |   0%
nss2-mcs5                36             |   0%     0              |   0%
nss2-mcs6                51             |   1%     0              |   0%
nss2-mcs7                33             |   0%     0              |   0%
nss2-mcs8                278            |   5%     0              |   0%
nss2-mcs9                2128           |  42%     0              |   0%
nss2-mcs10               1967           |  39%     0              |   0%
nss2-mcs11               141            |   2%     0              |   0%

Multicast groups: none
```

6.12.3 Device info

WEP-30L(root):/# **monitoring information**

```
system-time                     | 12:50:37 27.09.2023
uptime                          | 00:04:25
hostname                        | WEP-30L
software-version                | 2.5.2 build X
secondary-software-version      | 2.5.2 build X
boot-version                    | 2.1.0 build X
memory-usage                    | 43
memory-free                     | 137
memory-used                     | 104
memory-total                    | 241
cpu-load                        | 9.5
cpu-average                     | 6.70
is-default-config               | false
board-type                      | WEP-30L
hw-platform                     | WEP-30L
factory-wan-mac                 | 68:13:E2:35:C7:10
factory-lan-mac                 | 68:13:E2:35:C7:10
factory-serial-number           | WP52000345
hw-revision                     | 1v2
session-password-initialized    | false
ott-mode                        | false
last-reboot-reason              | firmware update
test-changes-mode               | false
```

6.12.4 Certificate information

WEP-30L(root):/# **monitoring certificate**

```
  ott:
      status: present
      url:

      file 'cert.pem':
         correctness: true
         issuer: /CN=OTT Certification Root/O=Eltex Enterprise Ltd./OU=Wi-Fi/C=RU/
L=Novosibirsk
         serial: 6813E201D050D05FC2D0332908C0F9FF
         subject: /CN=68:13:E2:01:D0:50/O=eltex
         not-before: Jan  1 00:00:00 1999 GMT
         not-after: Jan  1 00:00:00 2100 GMT
      file 'key.pem':
         correctness: false
  wlc:
      status: not present
  web:
      status: present
      file 'host.pem':
         correctness: true
         issuer: /C=RU/ST=Novosibirsk Region/L=Novosibirsk/O=Eltex Ent/CN=192.168.1.1
         serial: C010F45A63AC10E2
         subject: /C=RU/ST=Novosibirsk Region/L=Novosibirsk/O=Eltex Ent/CN=192.168.1.1
         not-before: Jan  1 00:00:58 1999 GMT
         not-after: Jan 18 00:00:58 2038 GMT
  portal:
      status: not present
  redirector:
      status: present
      file 'redirector.pem':
         correctness: true
         issuer: /CN=*.*/O=Eltex Ent
         serial: B36922FCDE841612
         subject: /CN=*.*/O=Eltex Ent
         not-before: Jan  1 00:00:21 1999 GMT
         not-after: Jan  1 00:00:21 2000 GMT
```

6.12.5 Network information

WEP-30L(root):/# **monitoring wan-status**

```
Common information:

 interface                | br0
 mac                      | cc:9d:a2:e9:14:70
 rx-bytes                 | 456875
 rx-packets               | 5835
 tx-bytes                 | 24328
 tx-packets               | 241

IPv4 information:

 protocol                 | dhcp
 ip-address               | 100.111.66.29
 netmask                  | 255.255.255.0
 gateway                  | 100.111.66.1
 DNS-1                    | 100.111.66.15
 DNS-2                    | 8.8.8.8

IPv6 information:

 addresses                | 2002::8/128 Global
                          | fe80::ce9d:a2ff:fee9:1470/64 Link
 dns-servers              | 2002::4144
                          | 2002::8844
                          | 2222::4144
```

WEP-30L(root):/# **monitoring ethernet**

```
   link: up
   speed: 2500
   duplex: enabled
   rx-bytes: 4872597
   rx-packets: 13844
   tx-bytes: 2477091
   tx-packets: 20923
```

WEP-30L(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-30L(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
```

WEP-30L(root):/# **monitoring lldp**

```
WEP-30L(root):/# monitoring lldp

Port        Device ID           Port ID             System Name         Capabilities   TTL
---------   -----------------   -----------------   -----------------   ------------   ---
eth0        e0:d9:e3:eb:66:80   gi1/0/16                                               120
```

6.12.6 Wireless interfaces

WEP-30L(root):/# **monitoring radio-interface**

```
   name                    | wlan0
   rfid                    | 0
   status                  | on
   band                    | 2.4 GHz
   hwaddr                  | 68:13:E2:xx:xx:xx
   tx-power                | 16 dBm
   noise-1                 | -100 dBm
   noise-2                 | -100 dBm
   channel                 | 11
   frequency               | 2462 MHz
   bandwidth               | 20 MHz
   utilization             | 0%
   thermal                 | 31
   thermalA                | 31
   thermalB                | 30

   name                    | wlan1
   rfid                    | 1
   status                  | on
   band                    | 5 GHz
   hwaddr                  | 68:13:E2:xx:xx:xx
   tx-power                | 19 dBm
   noise-1                 | -100 dBm
   noise-2                 | -100 dBm
   channel                 | 48
   frequency               | 5240 MHz
   bandwidth               | 20 MHz
   utilization             | 0%
   thermal                 | 35
   thermalA                | 35
   thermalB                | 35
```

6.12.7 Event logging

WEP-30L(root):/# **monitoring events**

```
Jan 23 00:00:07 WEP-30L daemon.info syslogd[925]: started: BusyBox v1.21.1

Jan 23 00:00:09 WEP-30L daemon.info configd[955]: The AP startup configuration was loaded
successfully.

Jan  1 03:00:14 WEP-30L daemon.info networkd[987]: Networkd started

Jan  1 03:01:17 WEP-30L daemon.info networkd[987]: DHCP-client: Interface br0 obtained
lease on 192.168.1.15.

Jan 23 07:17:14 WEP-30L daemon.info monitord[1055]: event: 'associated' mac:
E4:0E:EE:BD:AE:6B ssid: 'WEP-30L_2.4GHz' int0
```

6.12.8 Environment scan

While scanning the environment, the device radio interface will be disabled, which will make it impossible to transfer data to Wi-Fi clients during scanning.

WEP-30L(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-30L_ZN_Personal    |AP   |wpa     |E0:D9:E3:49:79:06 |44     |-16      |20
WEP-30L_ZN_Open        |AP   |off     |E0:D9:E3:49:79:07 |44     |-17      |20
WEP-30L_ZN_OWE         |AP   |owe     |E0:D9:E3:49:79:08 |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
```

6.12.9 Spectrum analyzer

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

While the spectrum analyzer is running, all clients are disconnected from the access point. Clients will only reconnect when the spectrum analyzer has finished its work. The analysis time for all radio channels of two bands is approximately 5 minutes.

The spectrum analyzer operates 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 configuration section.

WEP-30L(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%
```

7 Auxiliary utilities

7.1 traceroute utility

The utility shows which nodes (routers) the packet passes through, how much time it takes to process the packet at each node.

Command to start tracing

WEP-30L(root):/# **traceroute <tested host>**

Example of use

WEP-30L(root):/# traceroute eltex-co.ru

```
traceroute to eltex-co.ru (62.109.1.166), 30 hops max, 38 byte packets
 1  100.109.0.1 (100.109.0.1)  0.346 ms  0.233 ms  0.184 ms
 2  *  192.168.48.1 (192.168.48.1)  0.651 ms  *
 3  95.167.221.129 (95.167.221.129)  0.576 ms  0.486 ms  0.410 ms
 4  b-internet.92.125.152.57.snt.ru (92.125.152.57)  1.427 ms  2.621 ms  1.604 ms
```

7.2 tcpdump utility

The tcpdump utility allows capturing packets on the specified interface.

To get a hint on how to work with the utility use the command:

WEP-30L(config):/# **tcpdump --help**

7.2.1 Traffic capture from any active interface

For example, it is possible to enable packet capture on the Ethernet interface.

Example of command

WEP-30L(root):/# **tcpdump -i eth0**

7.2.2 Environment sniffer

On the access point, any VAP should be enabled in the range from which the traffic will be captured.

It is necessary to enable a special interface that catches all packets from the air on the working channel of the AP.

Commands

```
WEP-30L(root):/# configure
WEP-30L(config):/# interface
WEP-30L(config):/interface# radioX (for 2.4 GHz range — radio0, for 5 GHz — radio1)
WEP-30L(config):/interface/radioX# common
WEP-30L(config):/interface/radioX/common# enabled true
```

Example of command

```
WEP-30L(root):/# tcpdump -i radio1
```

7.3 iperf utility

This utility is used to start a traffic flow from one device to another. The sending side is called the client, the receiving side is called the server.

To get a hint on how to work with the utility use the command:

```
WEP-30L(root):/# iperf --help
```

Example of starting a traffic flow from the access point to the server:

Configuring the server to receive traffic

```
root@server:/# iperf -s
```

Starting traffic from the AP-client towards the server

```
WEP-30L(root):/# iperf -c X.X.X.X (where X.X.X.X — IP address of the server)
```

8 The list of changes

Document version	Issue date	Revisions
Version 1.4	06.2024	Synchronization with firmware version 2.5.2 Added: 5.4.2 "WDS" submenu 5.7 "WDS" menu 5.7.1 "WDS" submenu 5.8 "Z-Wave" menu 5.8.1 "Z-Wave" submenu 6.3.7 Configuration of VAP with external Captive Portal 6.6 Configuring WDS 6.7 Configuring Z-Wave 6.9 Configuring Captive Portal 6.9.1 Portal Certificate Management 6.11 Configuring remote traffic dump capture 6.12.2 WDS 7 Auxiliary utilities 7.1 traceroute utility 7.2 tcpdump utility 7.2.1 Traffic capture from any active interface 7.2.2 Environment sniffer 7.3 iperf utility Changed: 2.2 Device specification 2.4 Radiation patterns 6.3.8 Advanced VAP settings 6.4 Radio settings 6.8.5 Setting the date and time 6.12.4 Certificate information 6.12.6 Wireless interfaces 6.12.9 Spectrum analyzer

Version 1.3	01.2024	Synchronization with firmware version 2.3.1 Added: 2. New device WEP-30L-Z is supported 5.7 "Z-Wave" menu 5.7.1 "Z-Wave" submenu 6.6 Configuring Z-Wave Changed: 2.1 Purpose 2.2 Device specification 2.3 Technical parameters
Version 1.2	12.2023	Synchronization with firmware version 2.3.0 Added: 6.3.2 Configuration of VAP with OWE encryption 6.3.3 Configuration of VAP with OWE and OWE Transition Mode 6.8.3 Certificate information Changed: 2.2 Device specification 2.3 Technical parameters 5.4.7 "Device information" submenu 5.5.1 "Radio 2.4 GHz" submenu 5.6.2 "VAP" submenu 6.3 Virtual Wi-Fi access points (VAP) configuration 6.3.1 Configuration of VAP without encryption 6.3.4 Configuration of VAP with WPA-Personal security mode 6.3.5 Configuration of VAP with Enterprise authorization 6.3.6 Configuration of VAP with Captive Portal 6.3.7 Advanced VAP settings 6.8.2 Device info

Version 1.1	09.2023	Synchronization with firmware version 2.2.0 Added: 5.8.2 "Airtune" submenu 6.6.4 Setting the authentication mode Changed: 2.3 Technical parameters 5.5 "Radio" menu 5.4.2 "Traffic statistics" submenu 5.6.2 "VAP" submenu 6.2 Network parameters configuration 6.3 Virtual Wi-Fi access points (VAP) configuration 6.3.5 Advanced VAP settings 6.6.6 Advanced system settings 6.8.1 Wi-Fi clients 6.8.3 Network information
Version 1.0	05.2023	First issue
Firmware version 2.5.2		

TECHNICAL SUPPORT

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

https://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.

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

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