Wireless access point

WEP-3ax

User manual

Firmware version 1.12.0

IP address: 192.168.1.10

Username: admin

Password: password

Contents

1 Introduction

1.1 Annotation

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

WEP-3ax are dedicated to be installed inside buildings as an access points and to create a seamless wireless network using several identical access points ("Roaming") on a large area.

This manual specifies intended purpose, main technical parameters, design, safe operation rules, installation and configuration recommendations for WEP-3ax.

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 WEP-3ax wireless access points are designed to provide users with access to high-speed and safe network.

The devices are dedicated to create L2 wireless networks interfacing with a wired network. WEP-3ax is connected to a wired network via 100/1000/2500M Ethernet interface and arranges high-speed access to the Internet for devices supporting Wi-Fi technology at 2.4 and 5 GHz.

The devices have two radio interfaces to organize two physical wireless networks.

WEP-3ax supports up-to-date requirements to service quality and allow transmitting more important traffic in higher priorities queues. Prioritization is based on the main 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 to fully manage service quality and restrictions, both for all subscribers and for everyone in particular.

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

2.2 Device specification

Interfaces:

- 1 port of Ethernet 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.

Functions:

WLAN capabilities:

- Support for IEEE 802.11a/b/g/n/ac/ax standards;
- Support for roaming IEEE 802.11r/k/v;
- Data aggregation, including A-MPDU (Tx/Rx) and A-MSDU (Rx);
- WMM-based priorities and packet planning;
- Wireless bridges (WDS);
- Dynamic frequency selection (DFS);
- Support for hidden SSID;
- 32 virtual access points;
- Third-party access point detection;
- Spectrum analyzer;
- Channel auto-selection;
- BSS coloring.

Network functions:

- Auto-negotiation of speed, duplex mode and switching between MDI and MDI-X modes;
- Support for VLAN;
- NTP;
- GRE;
- DHCP client.

QoS functions:

- Bandwidth limiting for each SSID;
- Client data rate limiting for each SSID;
- Support for prioritization by CoS and DSCP.

Security:

- Centralized authorization via RADIUS server (802.1X WPA/WPA2/WPA3 Enterprise);
- WPA/WPA2/OWE/WPA3 data encryption;
- Support for Captive Portal;
- Support for WIDS/WIPS[1].

✓ [1] Support for WIDS/WIPS functionality is provided under the license.

Figure 1 shows WEP-3ax application diagram.

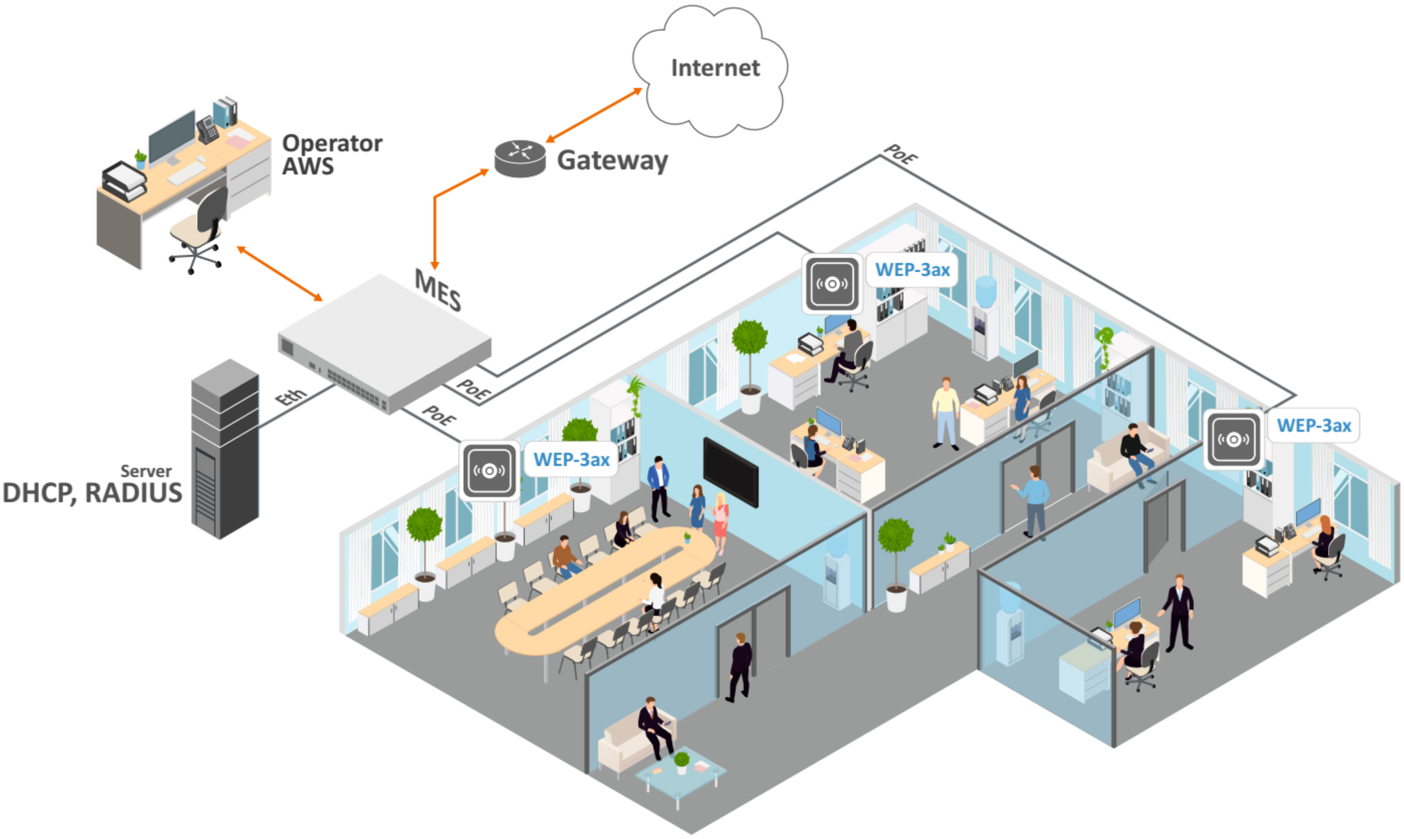


Figure 1 – WEP-3ax application diagram

2.3 Device technical parameters

Table 1 – Main specifications

WAN Ethernet interface parameters	
Number of ports	1
Electrical connector	RJ-45
Data rate	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)
Speed of data transmission	2.4 GHz, 802.11ax: 574 Mbps 5 GHz, 802.11ax: 1201 Mbps
Maximum number of concurrent sessions	2.4 GHz: 512 5 GHz: 512
Maximum transmitter power	2.4 GHz: 22.5 dBm 5 GHz : 24 dBm
Antenna gain	2.4 GHz: ~ 3 dBi 5 GHz : ~ 3 dBi
Receiver sensitivity	2.4 GHz: up to -92 dBm 5 GHz: up to -93 dBm

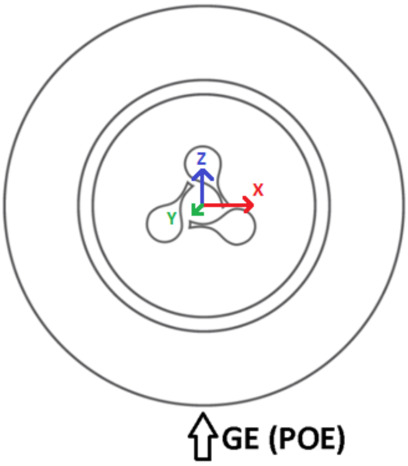
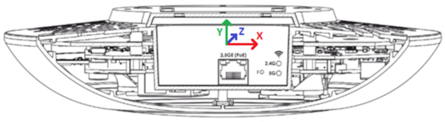
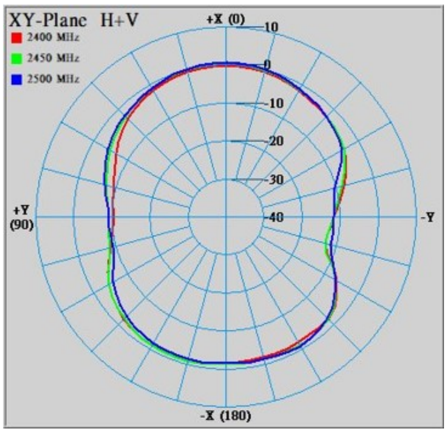
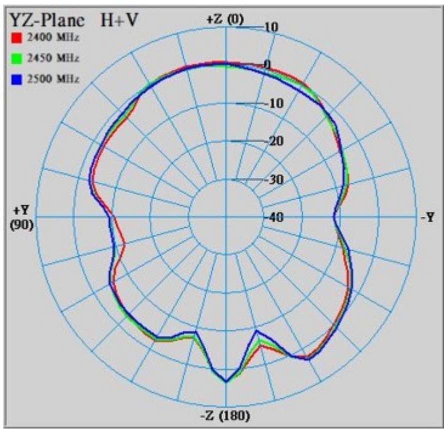
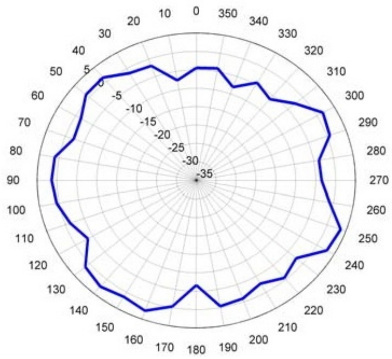
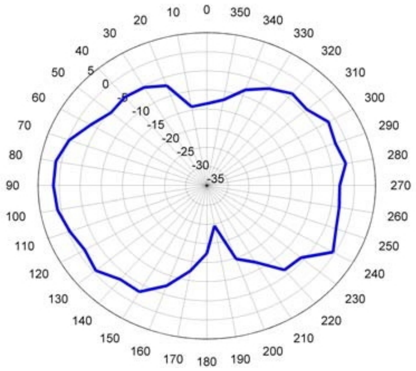
Security	centralized authorization via RADIUS server (802.1X WPA/WPA2/ WPA3 Enterprise) WPA/WPA2/OWE/WPA3 data encryption Captive Portal WIDS/WIPS[1] support
Support for OFDMA and MU-MIMO 2×2	
Control	
Remote control	web interface, Telnet, SSH, CLI, SNMP, NETCONF
Access restriction	by password
General parameters	
Flash memory	256 MB NAND Flash
RAM	1 GB DDR4 RAM
Power supply	PoE+ 48 V/56 V (IEEE 802.3at-2009)
Power consumption	no more than 13 W
Range of operation temperatures	from +5 to +40 °C
Relative humidity at 25 °C	up to 80 %
Dimensions (Diameter x Height)	230 × 56 mm
Weight	0.56 kg
Lifetime	no less than 15 years

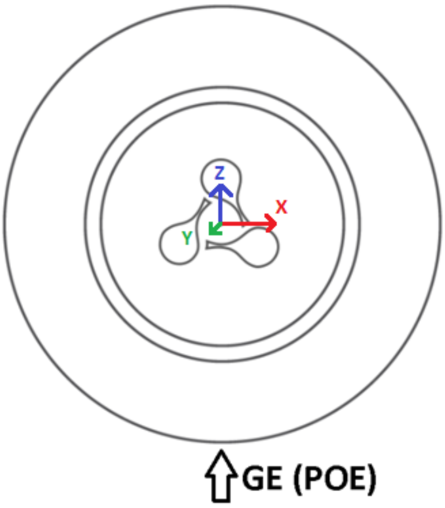
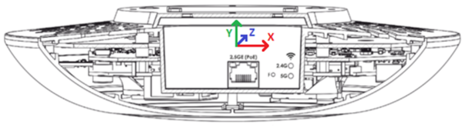
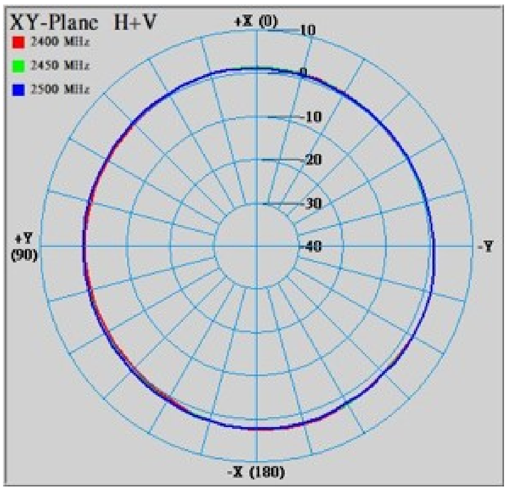
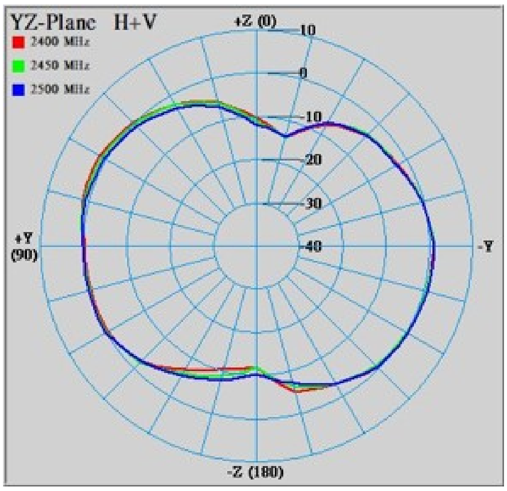
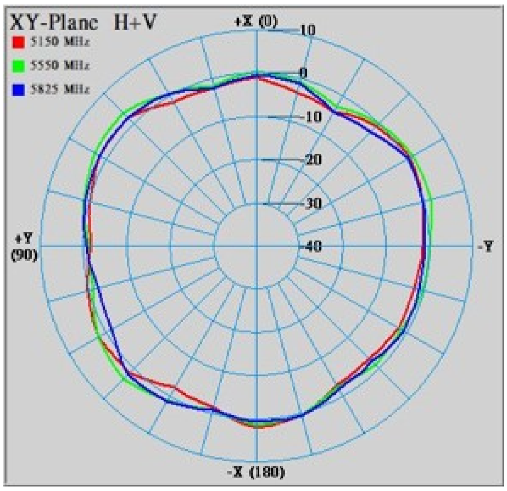
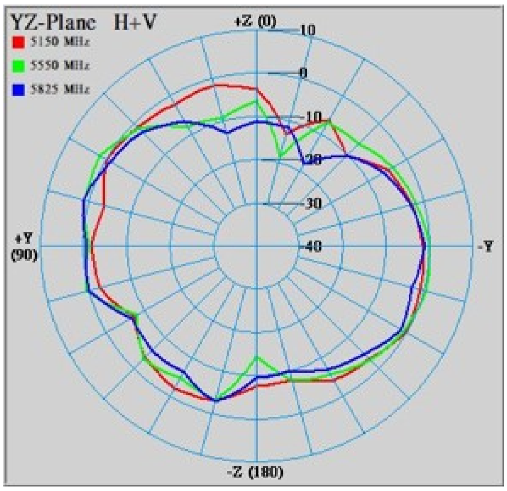
[1] WIDS/WIPS support is provided under the license.

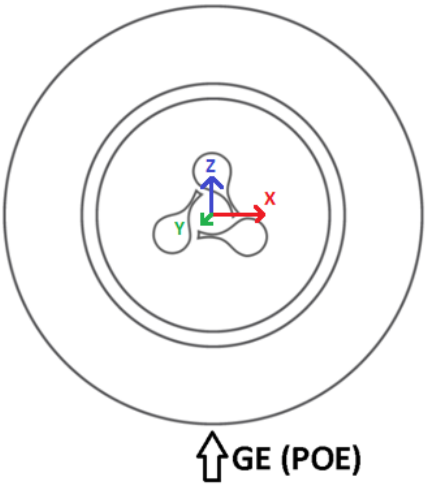
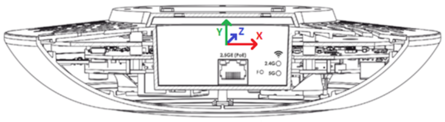
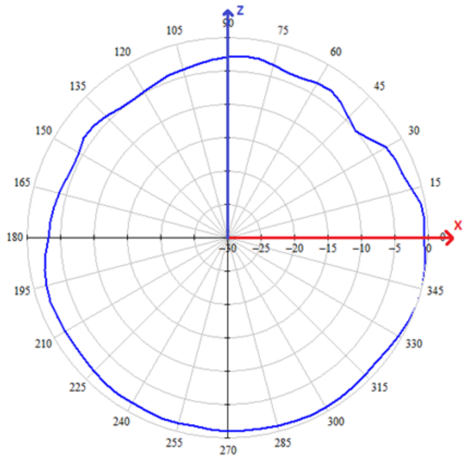
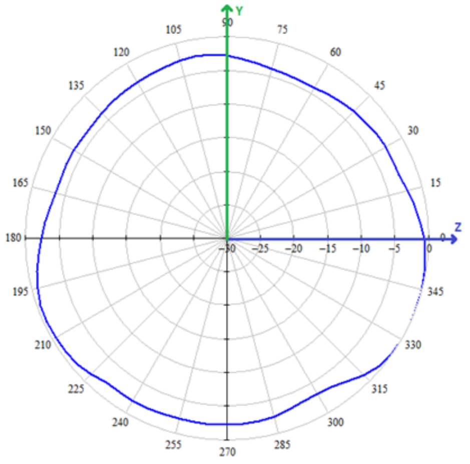
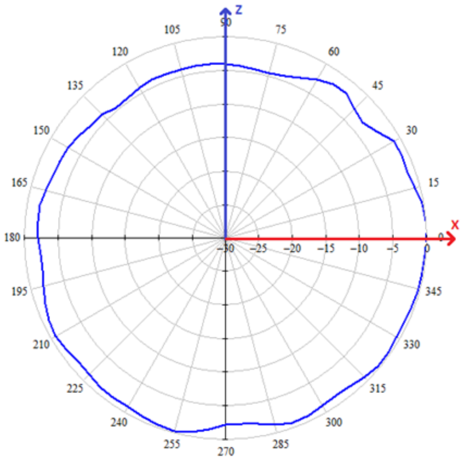
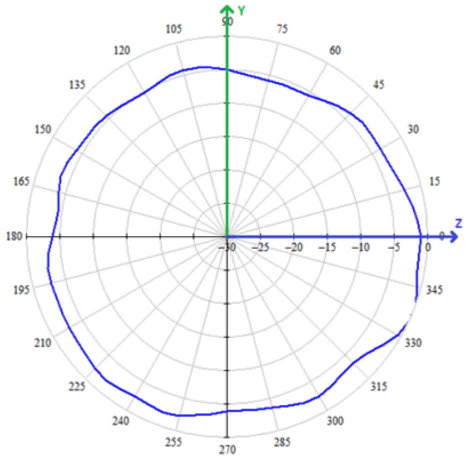
2.4 Radiation patterns

Radiation patterns for the embedded antennas are given below.

> ✓ Radiation patterns for 2v1 and 2v2 board revisions are different.

<table>
<tr><th colspan="2">WEP-3ax 2v1</th></tr>
<tr><th>AZIMUTH (XY)</th><th>ELEVATION (YZ)</th></tr>
<tr><td>
</td><td>
</td></tr>
<tr><th colspan="2">2.4 GHz</th></tr>
<tr><td>
</td><td>
</td></tr>
<tr><th colspan="2">5 GHz</th></tr>
<tr><td>
</td><td>
</td></tr>
</table>

<table>
<tr><th colspan="2">WEP-3ax 2v2</th></tr>
<tr><td>AZIMUTH (XY)
 </td><td>ELEVATION (YZ)
 </td></tr>
<tr><th colspan="2">2.4 GHz</th></tr>
<tr><td> </td><td> </td></tr>
<tr><th colspan="2">5 GHz</th></tr>
<tr><td> </td><td> </td></tr>
</table>

WEP-3ax 4v1	
AZIMUTH (XY)	**ELEVATION (YZ)**
	
2.4 GHz	
	
5 GHz	
	

2.5 Design

WEP-3ax is enclosed in a plastic case.

2.5.1 Device main panel

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

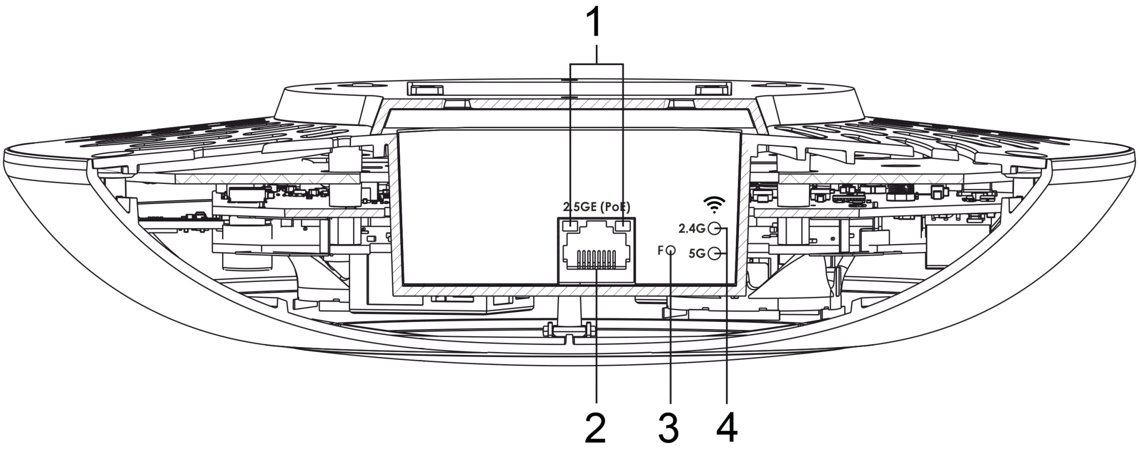


Figure 2 – Main panel of the device

The following light indicators, connectors and controls are located on the main panel of WEP-3ax (Table 2).

Table 2 – Description of indicators, ports and controls

Front panel element		Description
1	LAN	2.5GE (PoE) port status light indication
2	2.5GE (PoE)	2.5GE port for Ethernet cable and PoE+ power supply
3	F	Factory reset button
4	Wi-Fi	Status LEDs of Wi-Fi modules

2.6 Light indication

The current device state is displayed by **Wi-Fi, LAN, Power** indicators. The possible states of indicators are described in Table 3.

Table 3 – Light indication of device state

Indicator	**Indicator status**	**Device state**
Wi-Fi	Solid green	Wi-Fi network is active
	Flashing green	The process of data transmission trough a wireless network
LAN	Solid green (100 Mbps)/ Solid orange (1000, 2500 Mbps)	The link with the connected network device is established
	Flashing green	The process of packet data transmission through LAN interface
Power (on the device top panel)	Solid green	The device is powered on, normal operation
	Solid orange	The device is loaded but IP address is not received via DHCP
	Solid red	The device is loading

2.7 Reset to the default configuration

The device can be reset to the factory configuration using the "F" button. Press and hold the "F" button until the "Power" indicator starts flashing. The device will automatically reboot. DHCP client will be launched by default. If the address is not obtained via DHCP, the device will have the default IP address — *192.168.1.10*, and the following netmask — *255.255.255.0*.

2.8 Delivery package

The delivery package includes:

- WEP-3ax wireless access point;
- Mounting kit;
- User manual on a CD (optionally);
- Technical passport.

3 Rules and recommendations for device installation

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

3.1 Safety rules

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

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

3.2 Installation recommendations

1. Recommended mounting 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 the 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 the 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. During the device installation, follow these rules to ensure the best Wi-Fi coverage:
   a. Install the device at the center of a wireless network;
   b. Minimize the number of obstacles (walls, ceilings, furniture and etc.) between access point and other wireless network devices;
   c. Do not install the device near (about 2 m) electrical and radio devices;
   d. It is not recommended to use radiophone and other equipment operating at the frequency of 2.4 GHz, 5 GHz in Wi-Fi effective radius;
   e. Obstacles in the form of glass/metal constructions, brick/concrete walls, water cans and mirrors can significantly reduce Wi-Fi action radius. It is not recommended to place the device inside a false ceiling as metal frame causes multipath signal propagation and signal attenuation.
5. When installing several access points, cell action radius should 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 a more accurate assessment, it is necessary to make a radio examination of the room. Approximate coverage radius of confident reception of WEP-3ax access points when mounted on the ceiling in a typical office space: 2.4 GHz — 40–50 m, 5 GHz — 20–30 m. If there are no obstacles, the coverage area is up to 100 m for the 2.4 GHz band and up to 60 m for the 5 GHz band.
Table 4 describes approximate attenuation values.

Table 4 – Attenuation values

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

3.4 Channel selection for neighboring access points

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

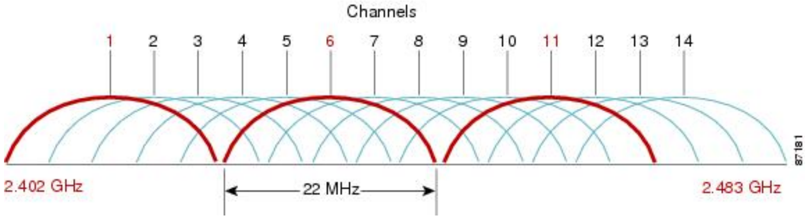


Figure 3 – General diagram of frequency channel overlap in the range of 2.4 GHz

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

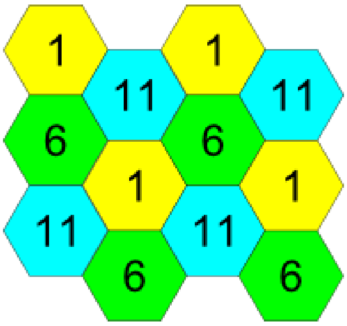


Figure 4 – Scheme of channel allocation among neighboring access points in the 2.4 GHz band when channel width is 20 MHz

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

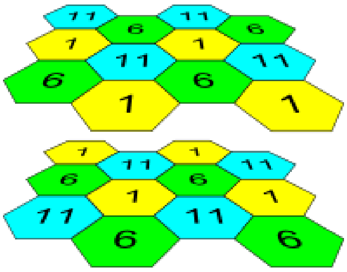


Figure 5 – Scheme of channel allocation between neighboring access points that are located between floors

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

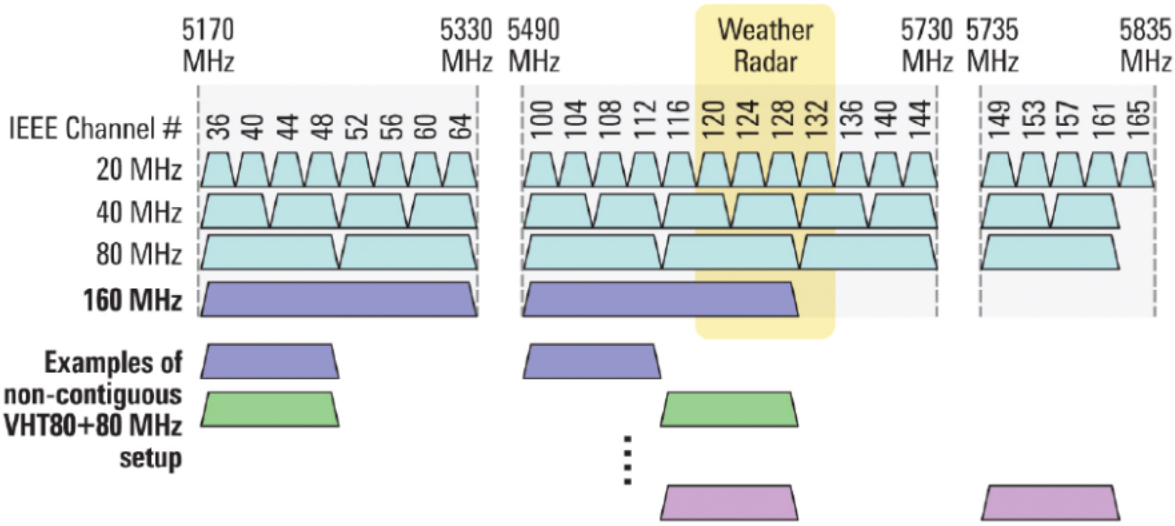


Figure 6 – Channels used in the 5 GHz band when channel width is 20, 40 or 80 MHz

4 Device installation

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

4.1 Wall mounting procedure

1. Fix the plastic bracket (included in the delivery package) to the wall. An example of placing the plastic bracket is shown in Figure 7.

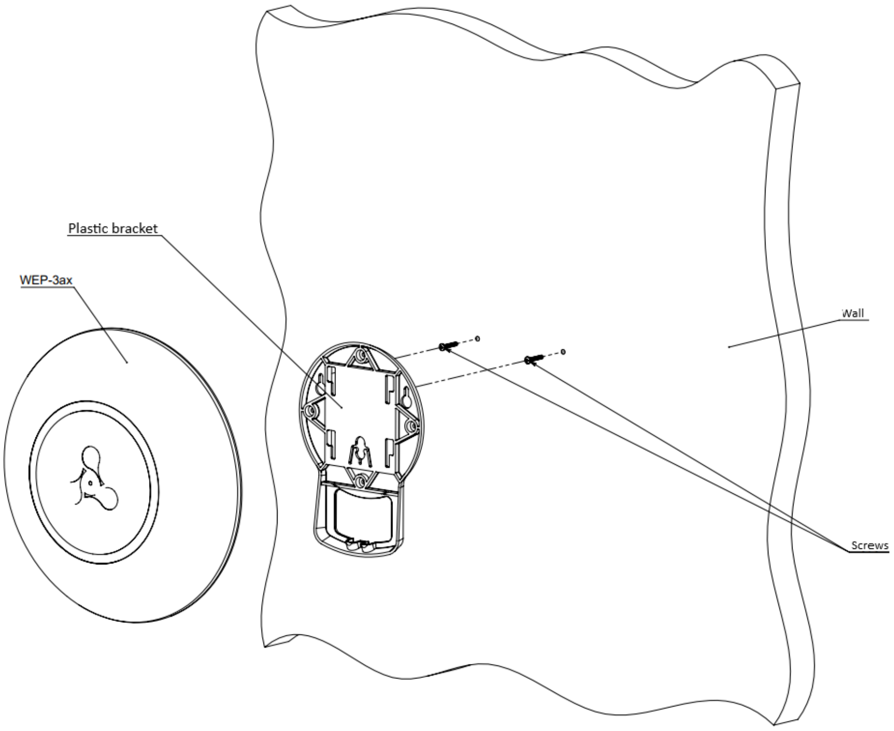


Figure 7 – Attaching the bracket to a wall

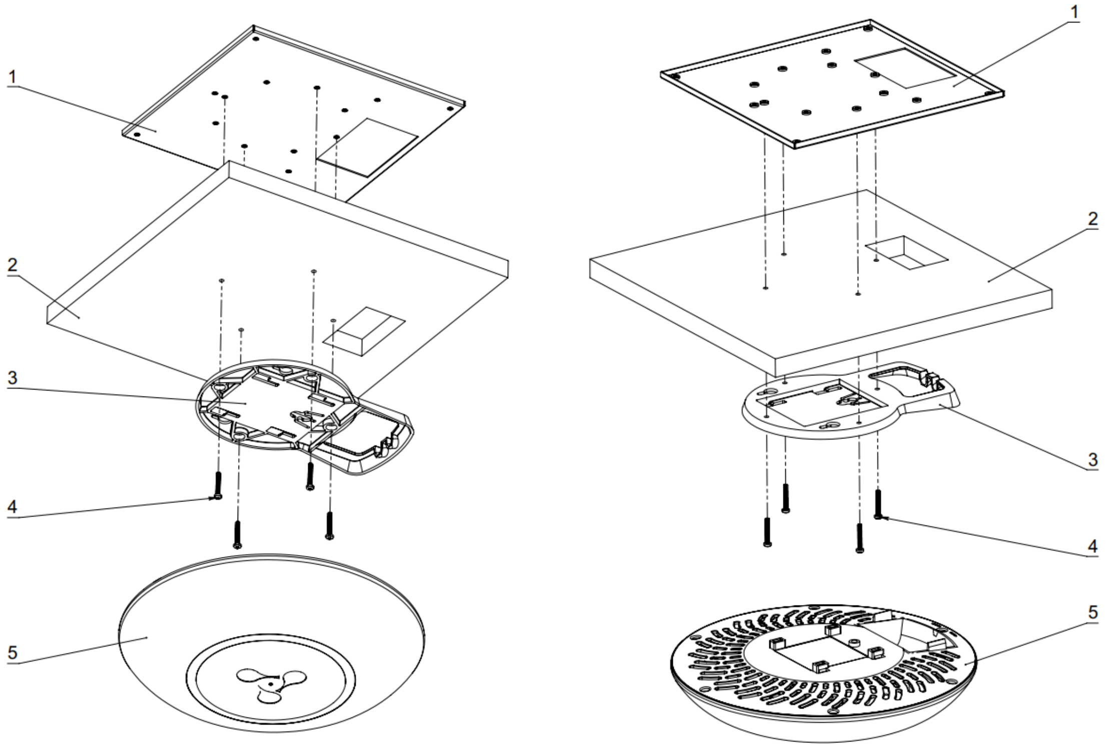
- When installing the bracket, pass wires through the corresponding channels on the bracket, see Figure 7.
- Align the screw holes on the bracket with the same holes on the surface. Using a screwdriver, secure the bracket with screws to the surface.

2. Install the device.

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

4.2 False ceiling mounting procedure

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



1 — metal bracket; 2 — Armstrong panel; 3 — plastic bracket; 4 — screws; 5 — device.

Figure 8 – Mounting on a false ceiling

1. Attach metal and plastic brackets to a ceiling as shown in Figure 8.

   - Fasten the plastic bracket (3) with the metal bracket (1) on the false ceiling in the following order: metal bracket -> Armstrong panel -> plastic bracket.
   - Cut the hole in the Armstrong panel. The size of the hole should be equal to a hole of the metal bracket. Pass the wires through the hole.
   - Align holes in the metal bracket with holes of the Armstrong panel and the 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 the corresponding connectors of the device. Description of the connectors is given in the Design section.
   - 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 7).
2. Remove the device.

5 Device management via the web interface

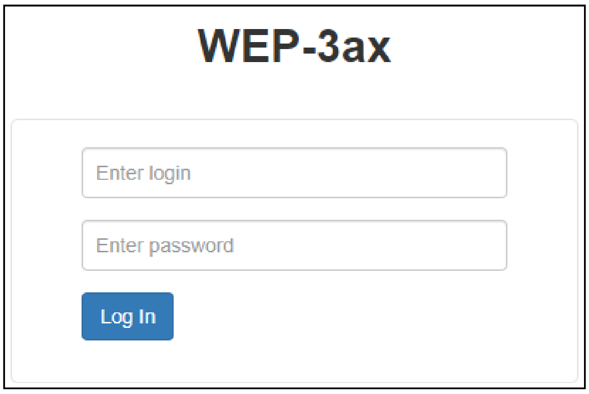
5.1 Getting started

To get started, 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.

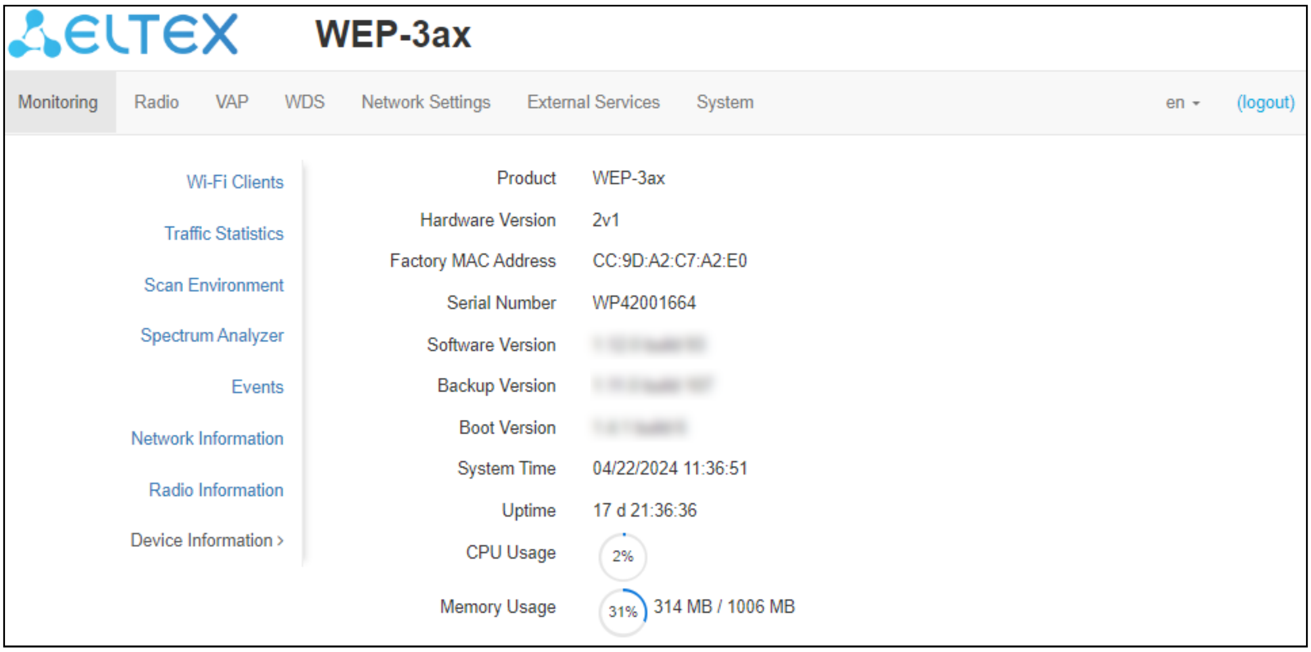
When the device is successfully detected, username and password request page will be shown in the browser window:



3. Enter username into "Login" and password into "Password" field.

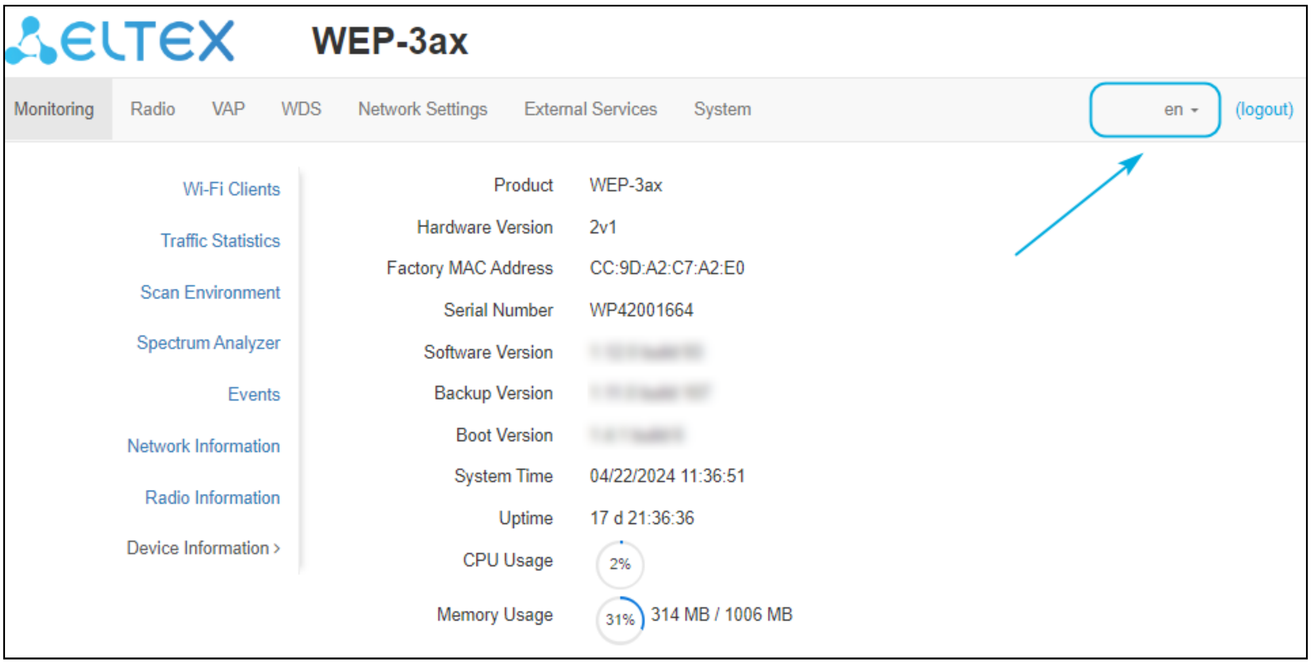
> ✓ Factory settings: login: *admin*, password: *password*.

4. Click "Log In". A menu for monitoring the status of the device will open in a browser window.



Product	WEP-3ax
Hardware Version	2v1
Factory MAC Address	CC:9D:A2:C7:A2:E0
Serial Number	WP42001664
Software Version	[redacted]
Backup Version	[redacted]
Boot Version	[redacted]
System Time	04/22/2024 11:36:51
Uptime	17 d 21:36:36
CPU Usage	2%
Memory Usage	31% 314 MB / 1006 MB

5. If necessary, select the information display language. Russian and English languages are available for web interface of WEP-3ax.



Product	WEP-3ax
Hardware Version	2v1
Factory MAC Address	CC:9D:A2:C7:A2:E0
Serial Number	WP42001664
Software Version	[redacted]
Backup Version	[redacted]
Boot Version	[redacted]
System Time	04/22/2024 11:36:51
Uptime	17 d 21:36:36
CPU Usage	2%
Memory Usage	31% 314 MB / 1006 MB

5.2 Applying configuration and discarding changes

1. Applying configuration

Clicking ✓ Apply 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-3ax web interface has a visual indication of the current status of the setting applying process (Table 5).

Table 5 – 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.

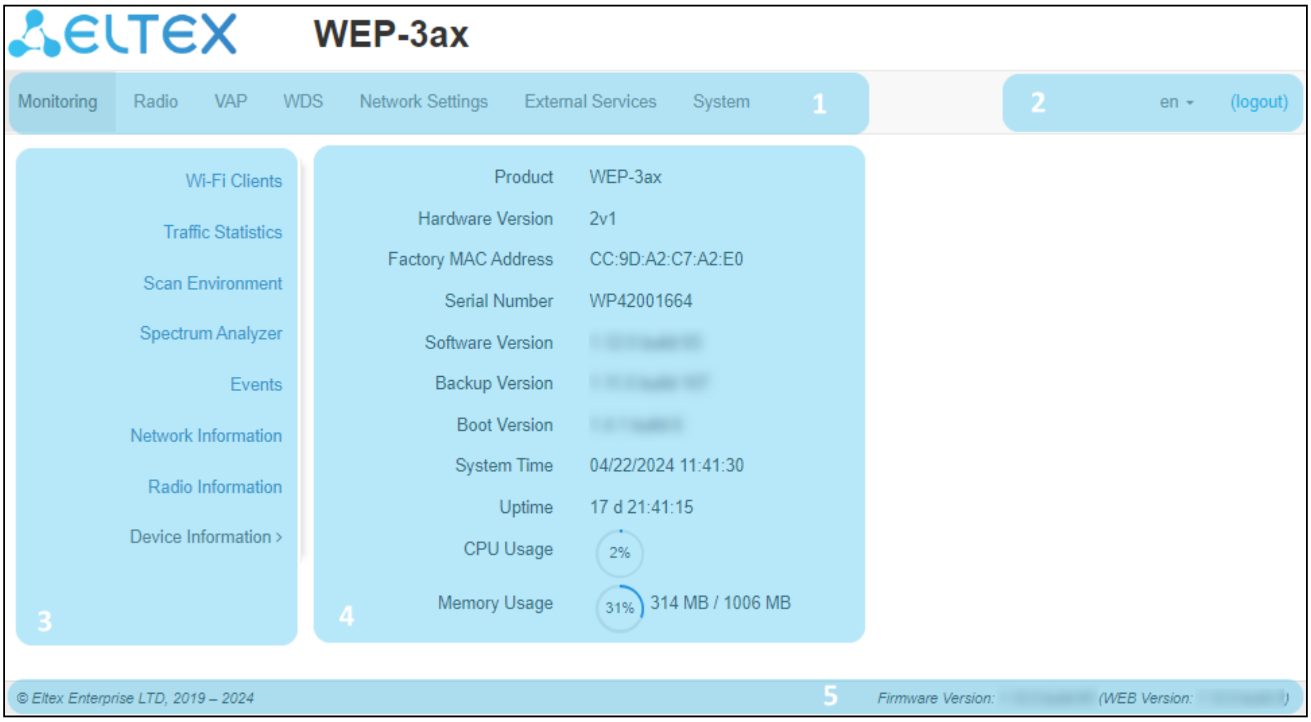
2. Discarding changes

The changes can be discarded only before clicking “Apply”. If you click “Apply”, all the changed parameters will be applied and saved to the device memory. After clicking "Apply", 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-3ax
Hardware Version 2v1
Factory MAC Address CC:9D:A2:C7:A2:E0
Serial Number WP42001664
Software Version [redacted]
Backup Version [redacted]
Boot Version [redacted]
System Time 04/22/2024 11:41:30
Uptime 17 d 21:41:15
CPU Usage 2%
Memory Usage 31% 314 MB / 1006 MB

© Eltex Enterprise LTD, 2019 – 2024
Firmware Version: [redacted] (WEB Version: [redacted])

User interface window is divided into five general areas:

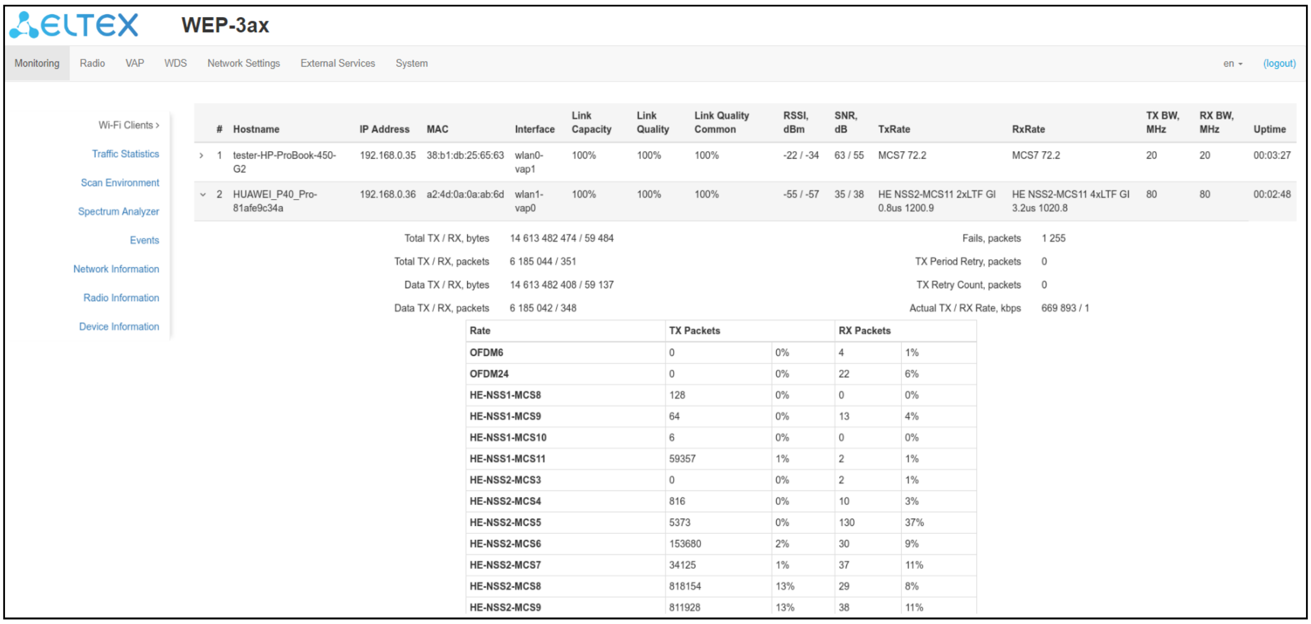
1. Menu tabs categorize the submenu tabs: **Monitoring, Radio, VAP, WDS, Network Settings, External Services, System.**
2. Interface language selection and Logout button designed to end a session in the web interface under a given user.
3. Submenu tabs allow one to control settings field.
4. Device configuration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

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.



	#	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	tester-HP-ProBook-450-G2	192.168.0.35	38:b1:db:25:65:63	wlan0-vap1	100%	100%	100%	-22 / -34	63 / 55	MCS7 72.2	MCS7 72.2	20	20	00:03:27
⌄	2	HUAWEI_P40_Pro-81afe9c34a	192.168.0.36	a2:4d:0a:0a:ab:6d	wlan1-vap0	100%	100%	100%	-55 / -57	35 / 38	HE NSS2-MCS11 2xLTF GI 0.8us 1200.9	HE NSS2-MCS11 4xLTF GI 3.2us 1020.8	80	80	00:02:48

Total TX / RX, bytes	14 613 482 474 / 59 484	Fails, packets	1 255
Total TX / RX, packets	6 185 044 / 351	TX Period Retry, packets	0
Data TX / RX, bytes	14 613 482 408 / 59 137	TX Retry Count, packets	0
Data TX / RX, packets	6 185 042 / 348	Actual TX / RX Rate, kbps	669 893 / 1

Rate	TX Packets		RX Packets	
OFDM6	0	0%	4	1%
OFDM24	0	0%	22	6%
HE-NSS1-MCS8	128	0%	0	0%
HE-NSS1-MCS9	64	0%	13	4%
HE-NSS1-MCS10	6	0%	0	0%
HE-NSS1-MCS11	59357	1%	2	1%
HE-NSS2-MCS3	0	0%	2	1%
HE-NSS2-MCS4	816	0%	10	3%
HE-NSS2-MCS5	5373	0%	130	37%
HE-NSS2-MCS6	153680	2%	30	9%
HE-NSS2-MCS7	34125	1%	37	11%
HE-NSS2-MCS8	818154	13%	29	8%
HE-NSS2-MCS9	811928	13%	38	11%

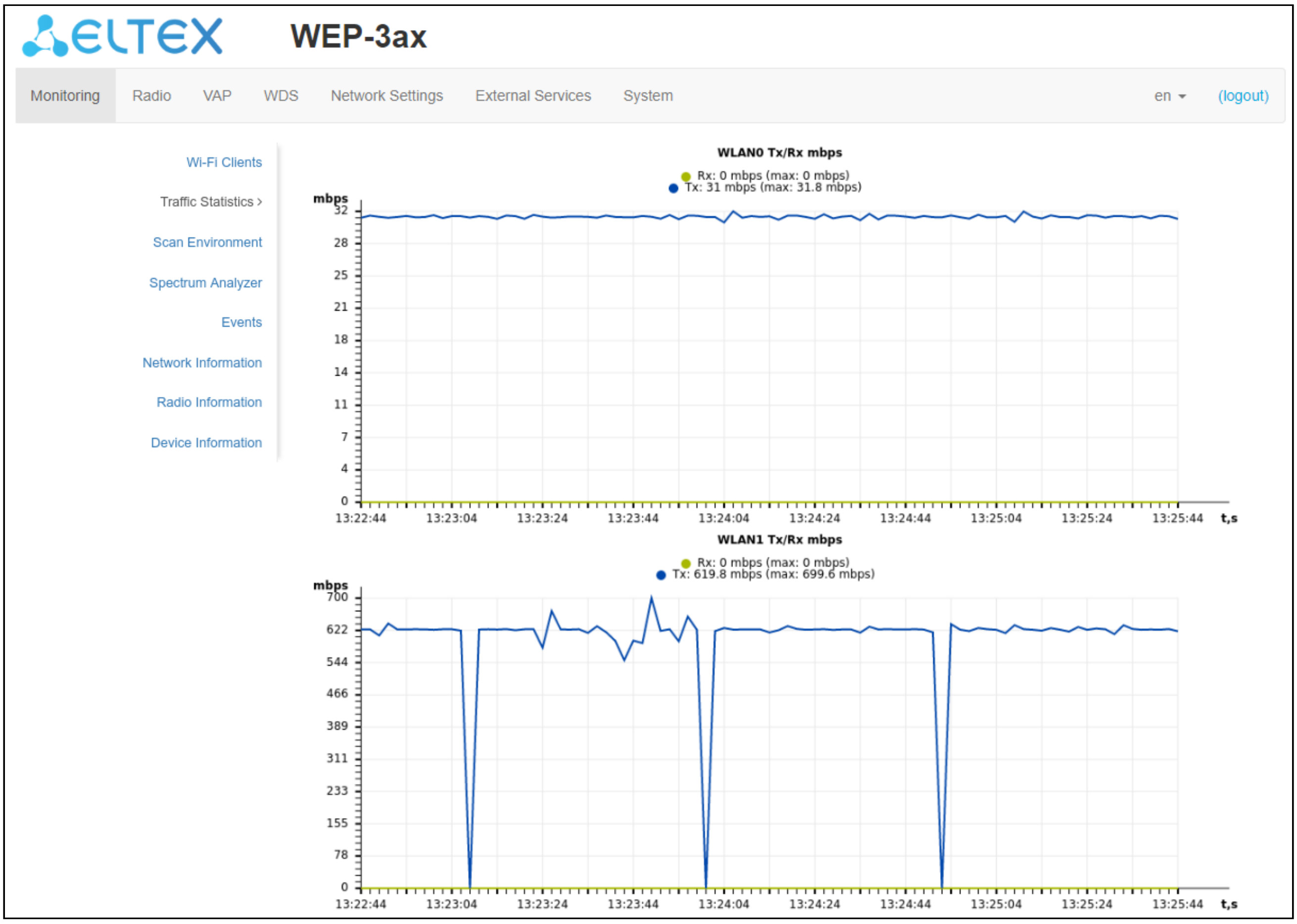
- *#* – number of the connected device in the list;
- *Hostname* – network name of the device;
- *IP Address* – IP address of the connected device;
- *MAC* – MAC address of the connected device;
- *Interface* – WEP-3ax interface for interaction with the connected device;
- *Link Capacity* – parameter that displays how effectively the access point uses modulation to transmit. It is calculated based on the number of packets transmitted on each modulation to the client, and reduction factors. The maximum value is 100 % (it 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 case when packets are transmitted on nss1mcs0 modulation for a client with MIMO support). The parameter value is calculated for the last 10 seconds;
- *Link Quality* – parameter that displays the state 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 seconds;
- *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 time of the client connection;
- *RSSI* – received signal level, dBm;
- *SNR* – signal/noise ratio, dB;
- *TxRate* – channel data rate of transmission, Mbps;
- *RxRate* – channel data rate of reception, Mbps;
- *Tx BW* – transmission bandwidth, MHz;
- *Rx BW* – reception bandwidth, MHz;
- *Uptime* – Wi-Fi client connection uptime.

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

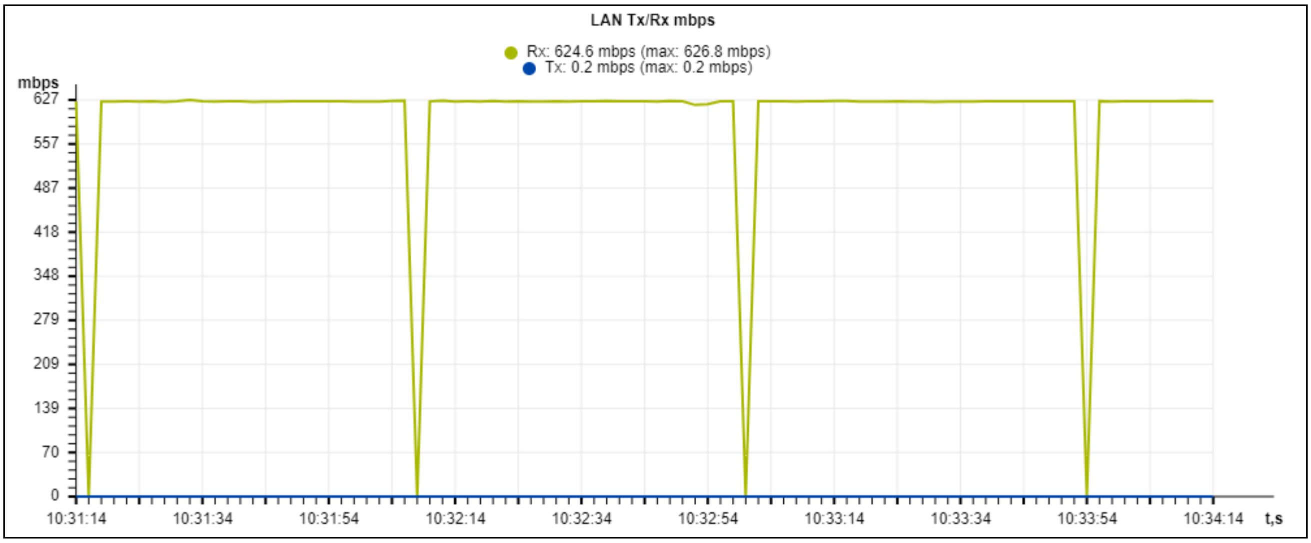
- *Total TX/RX, bytes* – number of bytes sent/received on the connected device;
- *Total TX/RX, packets* – number of packets sent/received on the connected device;
- *Data TX/RX, bytes* – number of data bytes sent/received on the connected device;
- *Data TX/RX, packets* – number of data packets sent/received 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 for 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 "Traffic Statistics" submenu

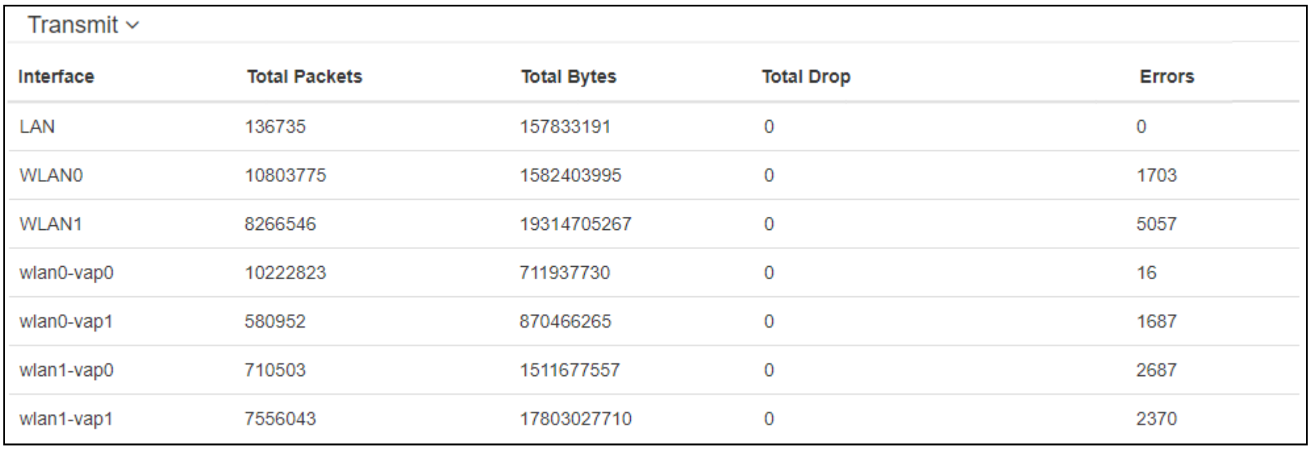
The **"Traffic Statistics"** section displays the graphs of the transmitted/received traffic speed for the last 3 minutes, as well as statistics on the amount of transmitted/received traffic since the access point was turned on.



The WLAN0 and WLAN1 Tx/Rx graphs show the rate of transmitted/received traffic via Radio 2.4 GHz (WLAN0) and Radio 5 GHz (WLAN1) interfaces for the last 3 minutes. The gragh is automatically updated every 2 seconds.



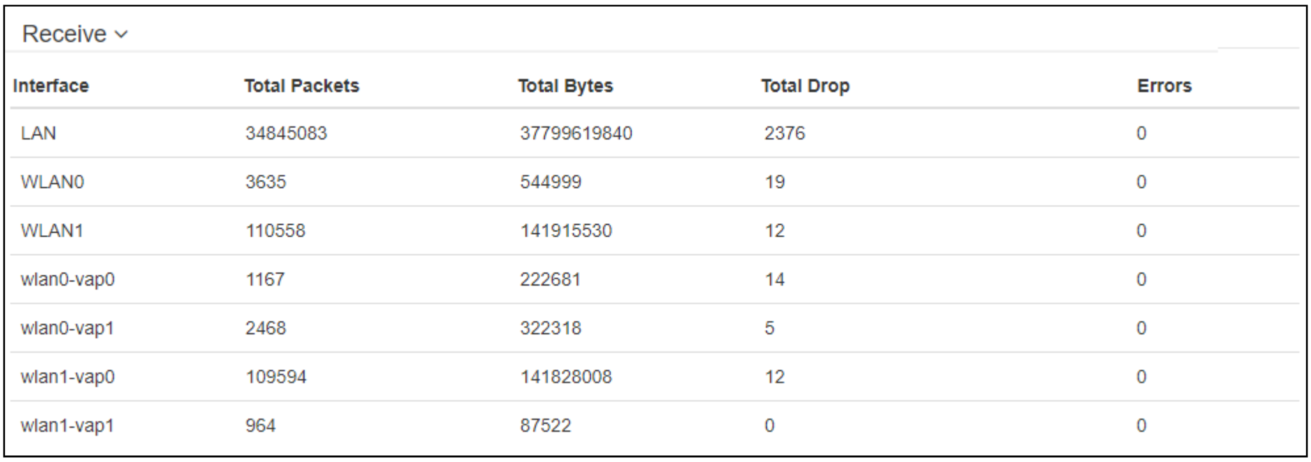
The LAN Tx/Rx graph shows the speed of the transmitted/received traffic via Ethernet interface of the access point for the last 3 minutes. The graph is automatically updated every 2 seconds.



Interface	Total Packets	Total Bytes	Total Drop	Errors
LAN	136735	157833191	0	0
WLAN0	10803775	1582403995	0	1703
WLAN1	8266546	19314705267	0	5057
wlan0-vap0	10222823	711937730	0	16
wlan0-vap1	580952	870466265	0	1687
wlan1-vap0	710503	1511677557	0	2687
wlan1-vap1	7556043	17803027710	0	2370

"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.



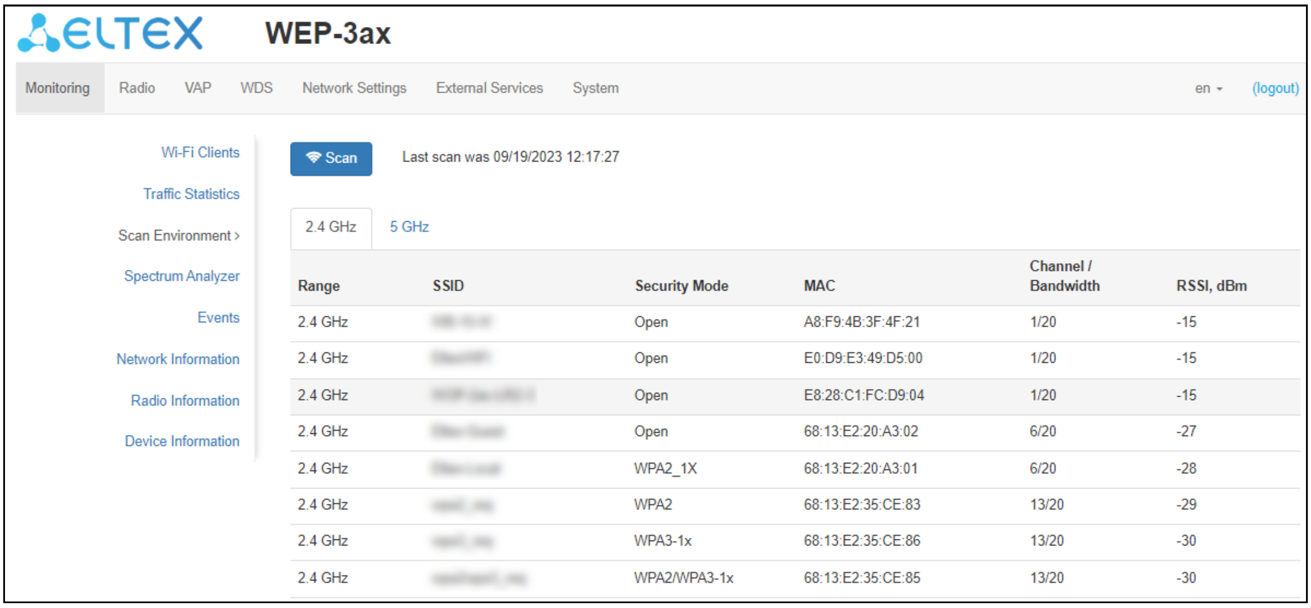
Interface	Total Packets	Total Bytes	Total Drop	Errors
LAN	34845083	37799619840	2376	0
WLAN0	3635	544999	19	0
WLAN1	110558	141915530	12	0
wlan0-vap0	1167	222681	14	0
wlan0-vap1	2468	322318	5	0
wlan1-vap0	109594	141828008	12	0
wlan1-vap1	964	87522	0	0

"Receive" table description:

- *Interface* – name of the interface;
- *Total Packets* – number of successfully received packets;
- *Total Bytes* – number of successfully received bytes;
- *Total Drop* – number of rejected packets;
- *Errors* – number of errors.

5.4.3 "Scan Environment" submenu

The **"Scan Environment"** submenu allows scanning the surrounding radio to detect neighboring access points.



Last scan was 09/19/2023 12:17:27

Range	SSID	Security Mode	MAC	Channel / Bandwidth	RSSI, dBm
2.4 GHz	[redacted]	Open	A8:F9:4B:3F:4F:21	1/20	-15
2.4 GHz	[redacted]	Open	E0:D9:E3:49:D5:00	1/20	-15
2.4 GHz	[redacted]	Open	E8:28:C1:FC:D9:04	1/20	-15
2.4 GHz	[redacted]	Open	68:13:E2:20:A3:02	6/20	-27
2.4 GHz	[redacted]	WPA2_1X	68:13:E2:20:A3:01	6/20	-28
2.4 GHz	[redacted]	WPA2	68:13:E2:35:CE:83	13/20	-29
2.4 GHz	[redacted]	WPA3-1x	68:13:E2:35:CE:86	13/20	-30
2.4 GHz	[redacted]	WPA2/WPA3-1x	68:13:E2:35:CE:85	13/20	-30

Click "Scan" to start the environment scanning process. When the process is completed, the page will display a list of detected access points and information about them:

- *Last scan was...* – last scan date and time;
- *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.

✓ Please note that 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.

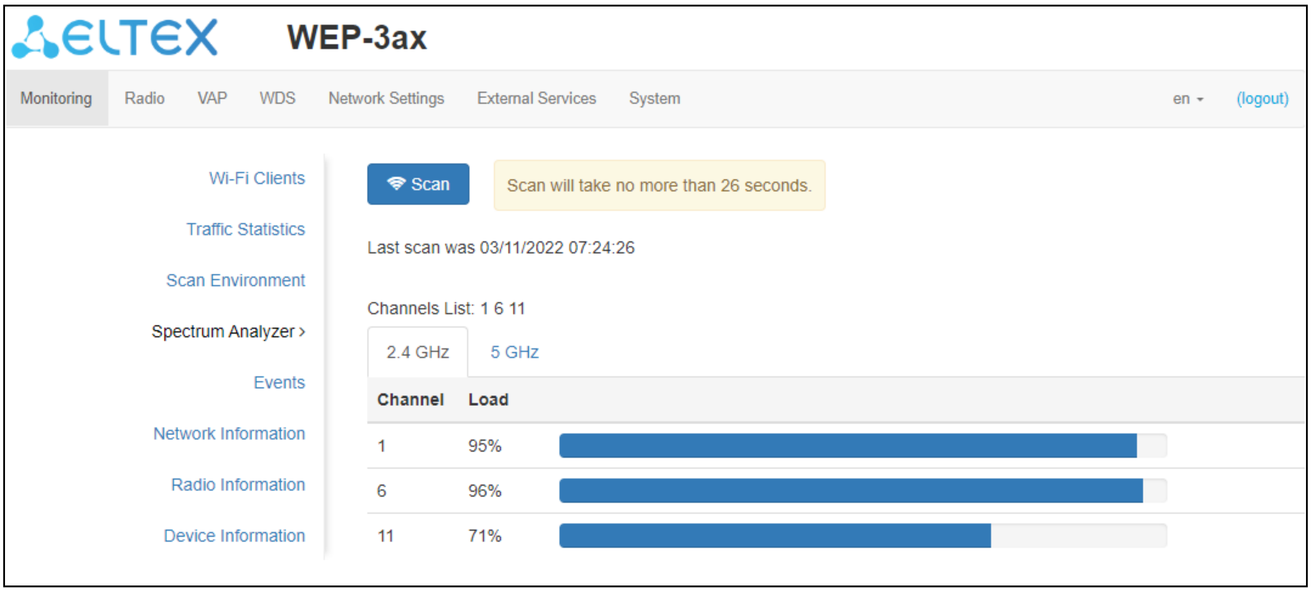
5.4.4 "Spectrum Analyzer" submenu

In the **"Spectrum Analyzer"** submenu, the spectrum analyzer is started and monitored.

The WEP-3ax devices have the ability to run a spectrum analyzer on the 2.4 GHz and 5 GHz radio interfaces.

Running the spectrum analyzer on radio interfaces

❗ Note that running the spectrum analyzer on the radio interface (Radio 2.4 GHz or Radio 5 GHz) will put it into scanning mode, which will disable all Wi-Fi clients connected to that radio interface.



Scan will take no more than 26 seconds.

Last scan was 03/11/2022 07:24:26

Channels List: 1 6 11

Channel	Load
1	95%
6	96%
11	71%

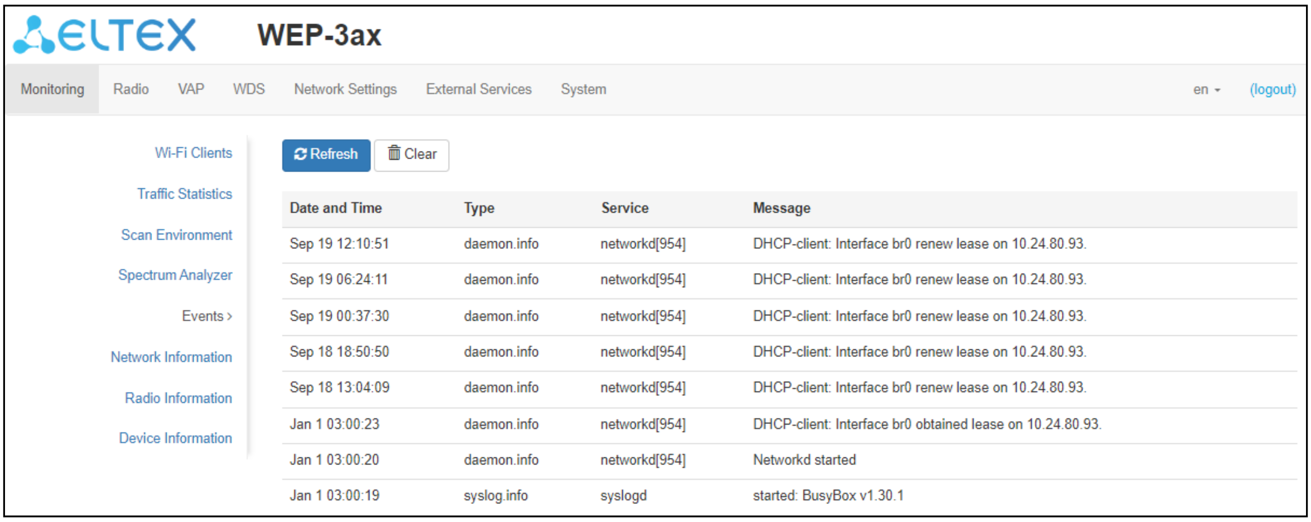
Click "Scan" to start the spectrum analyzer. The information window to the right of the button displays the time in seconds that has elapsed since the start of scanning. The time of the spectrum analyzer on the Radio 2.4 GHz radio interface does not exceed 26 seconds, on the Radio 5 GHz does not exceed 34 seconds.

- *Last scan was...* – last scan date and time;
- *Channels list* – list of channels to be scanned;
- *Channel* – number of the channel on which the scan was performed;
- *Load* – information about radio channel load, expressed as a percentage.

✓ The spectrum analyzer on the radio interface operates only on channels that are reflected in the "Channels List" parameter. For example, if the Radio 2.4 GHz channel list contains channels '1 6 11', the spectrum analysis will only be performed for channels 1, 6 and 11. To add/remove channels from this list, go to the tab corresponding to this radio interface on the "Radio" page and make changes in the "Use Limit Channels" parameter.
In order to analyze all the channels of the band on which the radio interface operates, go to the tab corresponding to the radio interface on the "Radio" page and uncheck the option "Use Limit Channels".
After receiving the results of the spectrum analyzer, check the "Use Limit Channels" option again.
For more information about configuring the radio interface via web interface, see the "Radio" menu section.

5.4.5 "Events" submenu

The **"Events"** submenu provides a list of events occurring on the device in real time. The event log contains the following information:



Date and Time	Type	Service	Message
Sep 19 12:10:51	daemon.info	networkd[954]	DHCP-client: Interface br0 renew lease on 10.24.80.93.
Sep 19 06:24:11	daemon.info	networkd[954]	DHCP-client: Interface br0 renew lease on 10.24.80.93.
Sep 19 00:37:30	daemon.info	networkd[954]	DHCP-client: Interface br0 renew lease on 10.24.80.93.
Sep 18 18:50:50	daemon.info	networkd[954]	DHCP-client: Interface br0 renew lease on 10.24.80.93.
Sep 18 13:04:09	daemon.info	networkd[954]	DHCP-client: Interface br0 renew lease on 10.24.80.93.
Jan 1 03:00:23	daemon.info	networkd[954]	DHCP-client: Interface br0 obtained lease on 10.24.80.93.
Jan 1 03:00:20	daemon.info	networkd[954]	Networkd started
Jan 1 03:00:19	syslog.info	syslogd	started: BusyBox v1.30.1

- *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 6 – Description of event severity levels

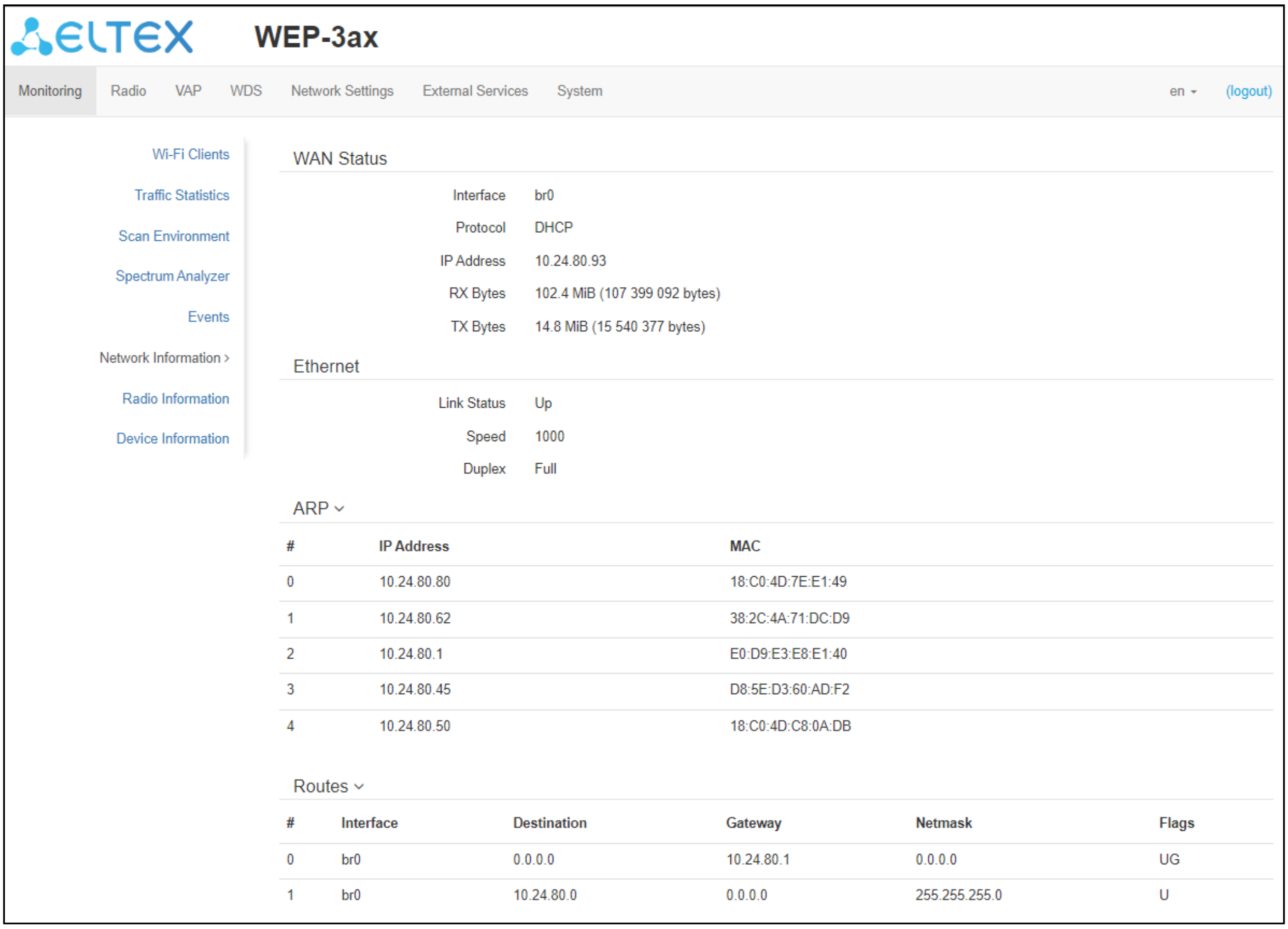
Level	Message severity level	Description
0	Emergency	A critical error has occurred in the system, the system may not work properly.
1	Alert	Immediate intervention is required.
2	Critical	A critical error has occurred in the system.
3	Error	An error has occurred in the system.
4	Warning	Warning, non-emergency 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 “Clear”.

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	10.24.80.93
RX Bytes	102.4 MiB (107 399 092 bytes)
TX Bytes	14.8 MiB (15 540 377 bytes)

Ethernet

Link Status	Up
Speed	1000
Duplex	Full

ARP

#	IP Address	MAC
0	10.24.80.80	18:C0:4D:7E:E1:49
1	10.24.80.62	38:2C:4A:71:DC:D9
2	10.24.80.1	E0:D9:E3:E8:E1:40
3	10.24.80.45	D8:5E:D3:60:AD:F2
4	10.24.80.50	18:C0:4D:C8:0A:DB

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

WAN Status:

- *Interface* – name of the 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.

Ethernet:

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

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

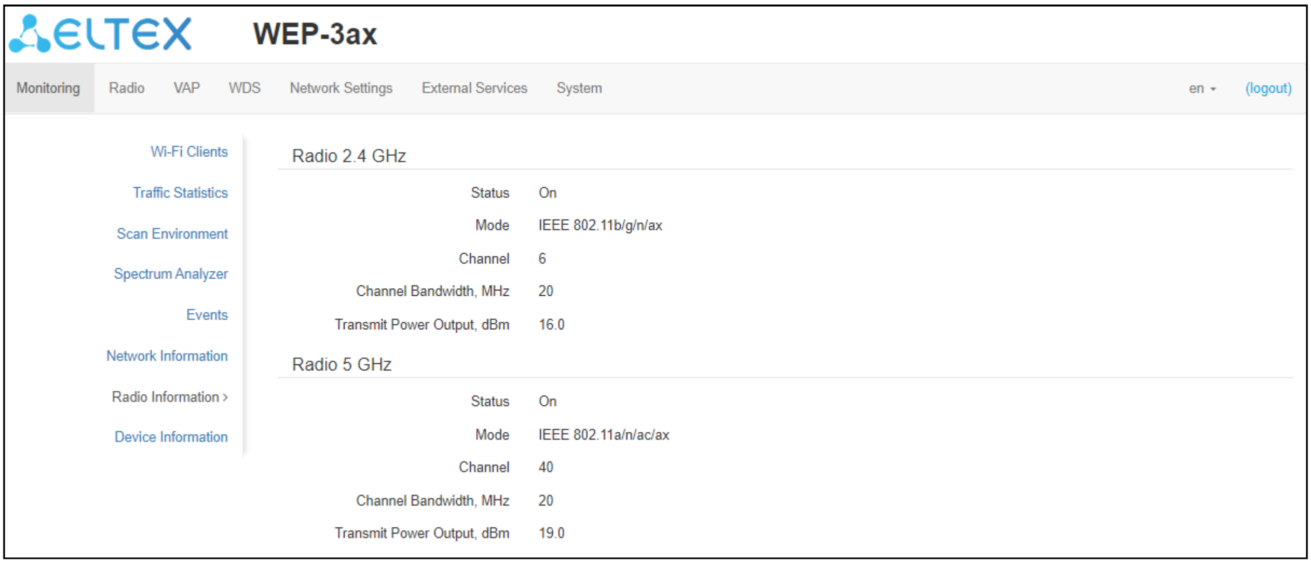
- *IP Address* – device IP address;
- *MAC* – device MAC address.

Routes:

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

5.4.7 "Radio Information" submenu

The **"Radio Information"** submenu displays the current status of WEP-3ax radio interfaces.



Radio 2.4 GHz

Status	On
Mode	IEEE 802.11b/g/n/ax
Channel	6
Channel Bandwidth, MHz	20
Transmit Power Output, dBm	16.0

Radio 5 GHz

Status	On
Mode	IEEE 802.11a/n/ac/ax
Channel	40
Channel Bandwidth, MHz	20
Transmit Power Output, dBm	19.0

Radio interfaces of an access point may be in two states: "On" and "Off". The status of each of the radio interfaces is reflected in the "Status" parameter.
Radio status depends on whether a given radio interface has virtual access points (VAP) enabled. If there is at least one active VAP on the radio interface, Radio will be in the "On" status, otherwise it will be in "Off" status.

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

"Off":

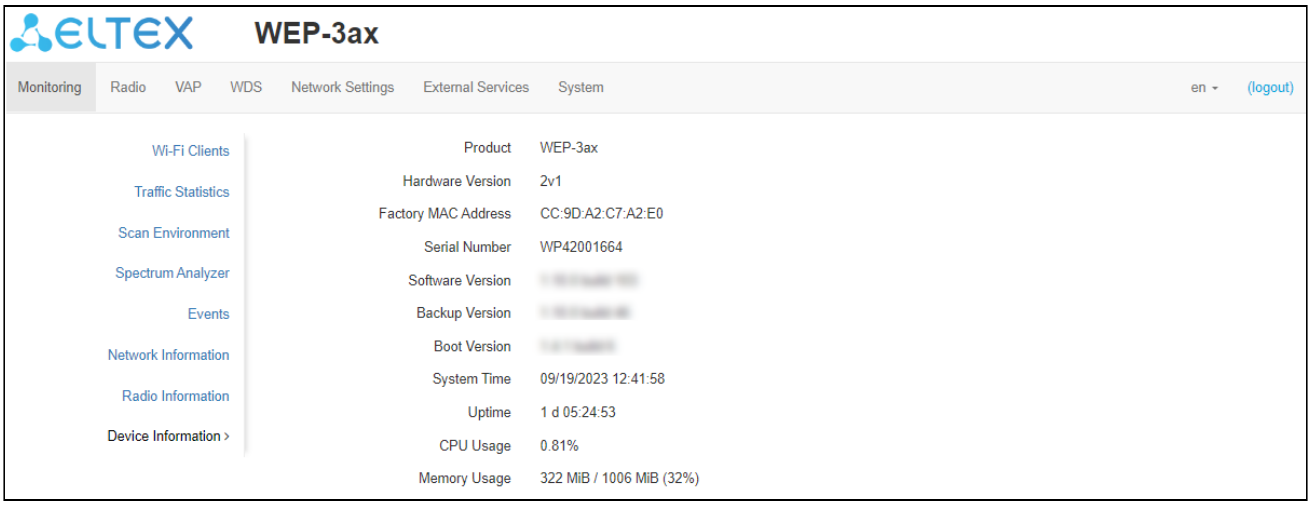
- *Status* – radio interface status.

"On":

- *Status* – radio interface status;
- *Mode* – radio interface operation mode according to IEEE 802.11 standards;
- *Channel* – number of the wireless channel on which the radio interface operates;
- *Channel Bandwidth* – the bandwidth of the channel where the radio interface operates, MHz;
- *Transmit Power Output* – actual power of the transmitter, dBm.

5.4.8 "Device Information" submenu

The "**Device Information**" submenu displays main WEP-3ax parameters.



Product	WEP-3ax
Hardware Version	2v1
Factory MAC Address	CC:9D:A2:C7:A2:E0
Serial Number	WP42001664
Software Version	[redacted]
Backup Version	[redacted]
Boot Version	[redacted]
System Time	09/19/2023 12:41:58
Uptime	1 d 05:24:53
CPU Usage	0.81%
Memory Usage	322 MiB / 1006 MiB (32%)

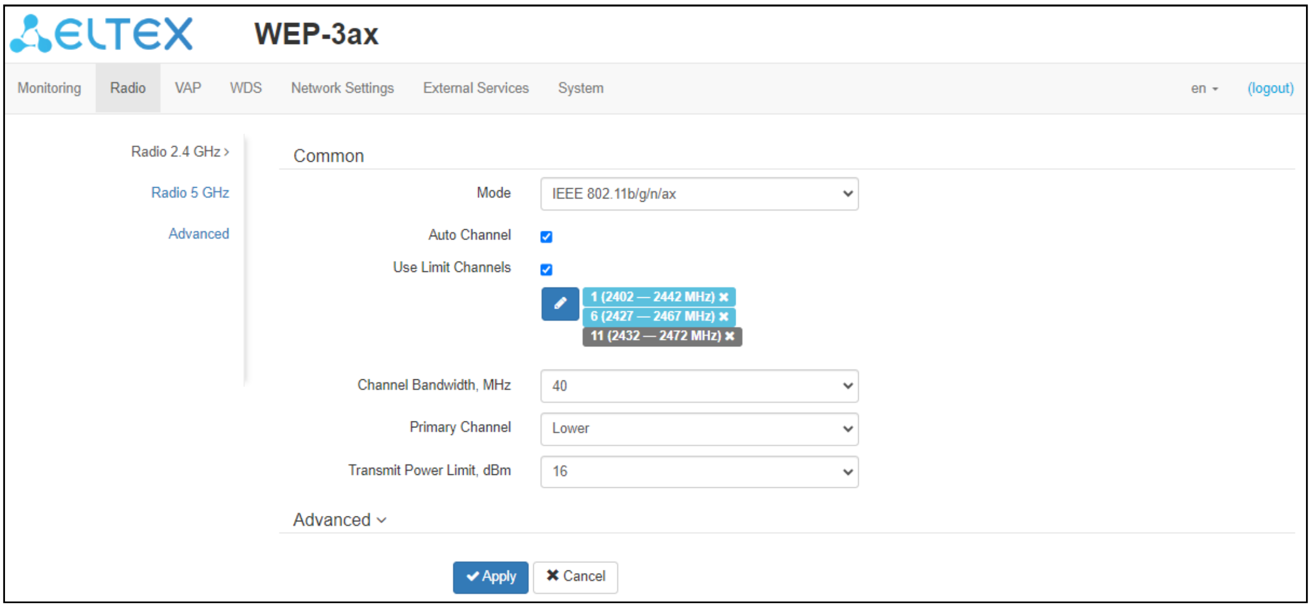
- *Product* – device model name;
- *Hardware Version* – device hardware version;
- *Factory MAC Address* – device WAN interface MAC address, set by the manufacturer;
- *Serial Number* – device serial number, set by the manufacturer;
- *Software Version* – device firmware version;
- *Backup Version* – previously installed firmware version;
- *Boot Version* – device firmware boot version;
- *System Time* – current time and date, set in the system;
- *Uptime* – time since the last start or restart of the device;
- *CPU Usage* – average percentage of CPU load for the last 5 seconds;
- *Memory Usage* – percentage of the device memory 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

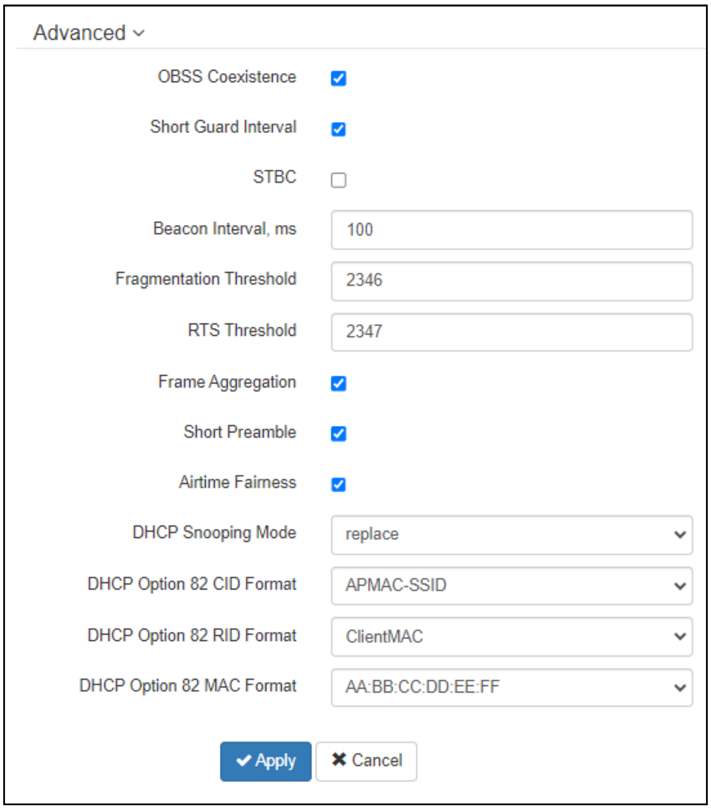
- *Mode* – interface operation mode according to the following standards:
  - IEEE 802.11ax;
  - IEEE 802.11n/ax;
  - IEEE 802.11b/g;
  - IEEE 802.11b/g/n;
  - IEEE 802.11b/g/n/ax.
- *Auto Channel* – when checked, the device will automatically select the least loaded radio channel for the Wi-Fi interface. Removing the flag opens the access to install the static operation channel;
- *Channel* – select channel for data transmission;
- *Use Limit Channels* – when checked, the access point will use a user-defined list of channels to work in automatic channel selection mode. If the "Use Limit Channels" flag is not checked or there are no channels in the list, the access point will select the operation channel from all available channels in the given band. The 2.4 GHz band channels: 1–13;
- *Channel Bandwidth, MHz* – the bandwidth of the channel where the radio interface operates. Can take a value of 20 or 40 MHz;
- *Primary Channel* – the parameter can only be changed if the bandwidth of a statically specified channel is equal to 40 MHz. The 40 MHz channel can be considered as consisting of two 20 MHz channels, which border in the frequency range. These two 20 MHz channels are called primary and secondary channels. The primary channel is used by clients who only support 20 MHz channel bandwidth:
  - *Upper* – the primary channel will be the upper 20 MHz channel in the 40 MHz band;
  - *Lower* – the primary channel will be the lower 20 MHz channel in the 40 MHz band.
- *Transmit Power Limit, dBm* – transmitting Wi-Fi signal power adjustment, dBm. May take values between 6 and 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 should 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 to change the "Channel Bandwidth" parameter to 40 MHz and do not remove the "grey" channels from the list, then when you click "Apply" 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, the advanced radio interface parameters of the device can be configured.



Advanced

OBSS Coexistence	☑
Short Guard Interval	☑
STBC	□
Beacon Interval, ms	100
Fragmentation Threshold	2346
RTS Threshold	2347
Frame Aggregation	☑
Short Preamble	☑
Airtime Fairness	☑
DHCP Snooping Mode	replace
DHCP Option 82 CID Format	APMAC-SSID
DHCP Option 82 RID Format	ClientMAC
DHCP Option 82 MAC Format	AA:BB:CC:DD:EE:FF

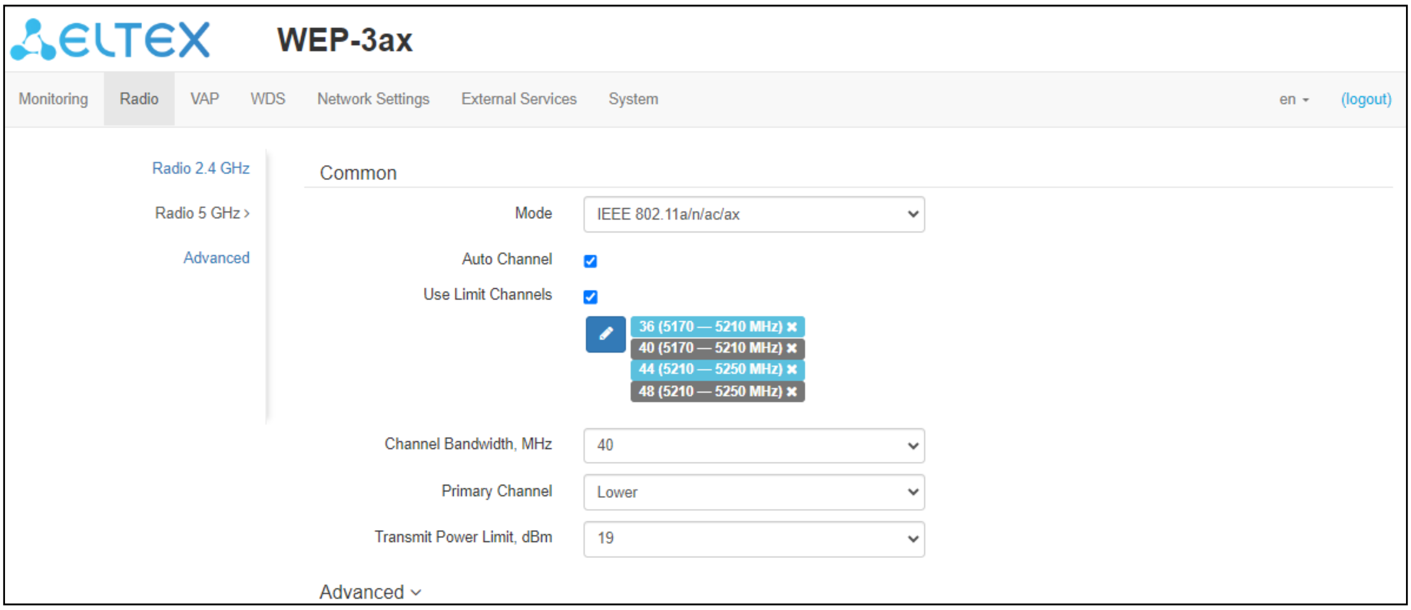
- *OBSS Coexistence* – automatic channel bandwidth reduction when the channel is loaded. When checked, the mode is enabled;
- *Short Guard Interval* – support for Short Guard Interval. Access point transmits data using 400 ns Guard interval (instead of 800 ns) to clients which also support Short Guard 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 one data flow through several antennas;
- *Beacon Interval, ms* – Beacon frame sending 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 can 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;
- *Airtime Fairness* – over-the-air radio accessibility feature. When checked, the function is active – the airtime is distributed evenly among users;
- *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:
        - *DHCP 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.
        - *DHCP 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.
        - *DHCP Option 82 MAC 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 (-).

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.



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: Lower

Transmit Power Limit, dBm: 19

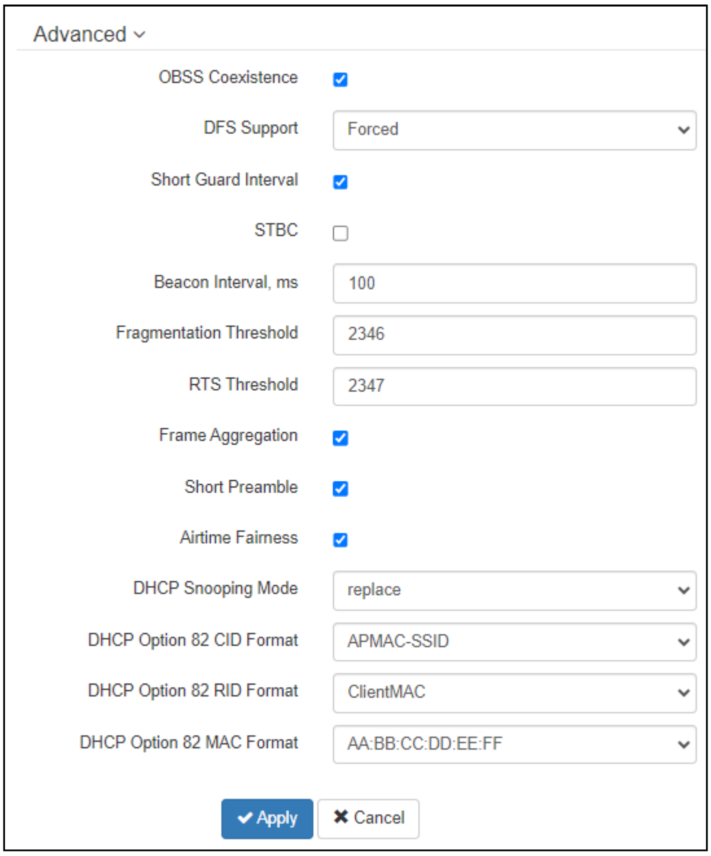
- *Mode* – interface operation mode according to the following standards:
  - IEEE 802.11ax;
  - IEEE 802.11a/n/ac;
  - IEEE 802.11a/n/ac/ax.
- *Auto Channel* – when checked, the device will automatically select the least loaded radio channel for the Wi-Fi interface. Removing the flag opens the access to install the static operation channel;
- *Channel* – select channel for data transmission;
- *Use Limit Channels* – when checked, the access point will use a user-defined list of channels to work in automatic channel selection mode. If the "Use Limit Channels" flag is not checked or there are no channels in the list, the access point will select the operation channel from all available channels in the given band. The 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* – the parameter can only be changed if the bandwidth of a statically specified channel is equal to 40 MHz. The 40 MHz channel can be considered as consisting of two 20 MHz channels, which border in the frequency range. These two 20 MHz channels are called primary and secondary channels. The primary channel is used by clients who only support 20 MHz channel bandwidth:
  - *Upper* – the primary channel will be the upper 20 MHz channel in the 40 MHz band;
  - *Lower* – the primary channel will be the lower 20 MHz channel in the 40 MHz band.
- *Transmit Power Limit, dBm* – transmitting Wi-Fi signal power adjustment, dBm. May take values between 10 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 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" becomes available for editing and the default value is "Lower",
- Channels 40 and 48 in the "Use Limit Channels" list change their 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 "Apply" in the browser an error will appear – "There are errors in data. Changes was not applied". Accordingly, the access point configuration will not be changed. This is due to the fact that channels in the "Use Limit Channels" list that are highlighted in grey do not fit the definition "Primary channel" = Lower.

In the "Advanced" section, the advanced radio interface parameters of the device can be configured.


Advanced

OBSS Coexistence ☑

DFS Support: Forced

Short Guard Interval ☑

STBC ☐

Beacon Interval, ms: 100

Fragmentation Threshold: 2346

RTS Threshold: 2347

Frame Aggregation ☑

Short Preamble ☑

Airtime Fairness ☑

DHCP Snooping Mode: replace

DHCP Option 82 CID Format: APMAC-SSID

DHCP Option 82 RID Format: ClientMAC

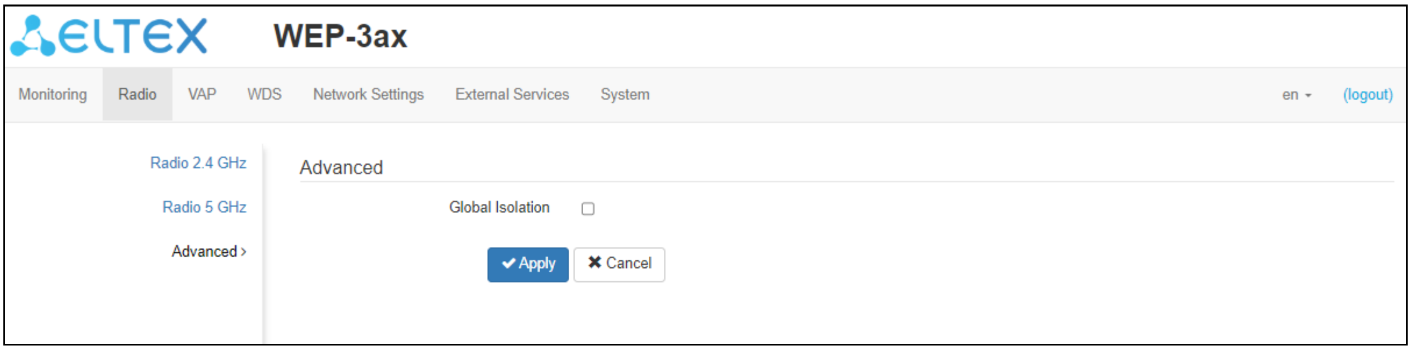
DHCP Option 82 MAC Format: AA:BB:CC:DD:EE:FF

- *OBSS Coexistence* – automatic channel bandwidth reduction when the channel is loaded. When checked, the mode is enabled;
- *DFS Support* – dynamic frequency selection mechanism. The mechanism demands wireless devices to scan environment and avoid using channels which coincide with radiolocation system's channels at 5 GHz:
  - *Disabled* – the mechanism is disabled. DFS channels are not available for selection;
  - *Enabled* – the mechanism is enabled;
  - *Forced* – the mechanism is disabled. DFS channels are available for selection.
- *Short Guard Interval* – support for Short Guard interval. Access point transmits data using 400 ns Guard interval (instead of 800 ns) to clients which also support Short 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 one data flow through several antennas;
- *Beacon Interval, ms* – Beacon frame sending period. The frames are sent to detect access points. The parameter takes values from 20 to 2000 ms, by default – 100 ms;
- *Fragmentation Threshold* – frame fragmentation threshold, bytes. The parameter takes values 256–2346, by default – 2346;
- *RTS Threshold* – after what quantity of bytes the Request to Send will be sent. Decreasing this value can improve access point operation when there are a lot of clients connected. However, this reduces general throughout of wireless network. The parameter takes values from 0 to 65535, by default – 2347;
- *Frame Aggregation* – enable support for AMPDU/AMSDU;
- *Short Preamble* – use of the packet short preamble;
- *Airtime Fairness* – over-the-air radio accessibility feature. When checked, the function is active – the airtime is distributed evenly among users;
- *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:
    - *DHCP 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.
    - *DHCP 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.
    - *DHCP Option 82 MAC 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 (-).

5.5.3 "Advanced" submenu

In the **"Advanced"** submenu, the advanced device radio interface parameters can be configured.



Advanced

Global Isolation □

✔ Apply ✖ Cancel

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

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

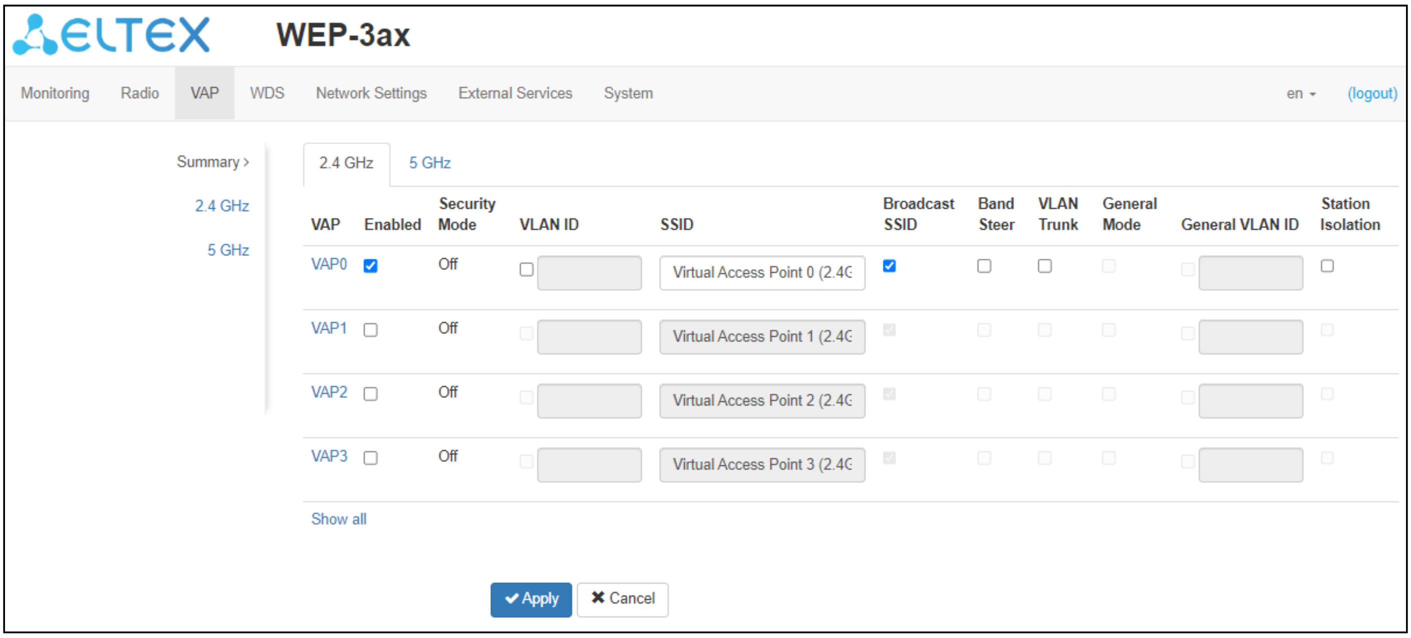
5.6 "VAP" menu

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

5.6.1 "Summary" submenu

The **"Summary"** submenu displays the settings of all VAPs on the Radio 2.4 GHz and the Radio 5 GHz radio interfaces.

Only the first four VAPs of each radio interface are displayed on the page by default. To see a full list of available VAPs, click "Show all". Click "Minimize" to return the display of VAPs number in the list to its original state.

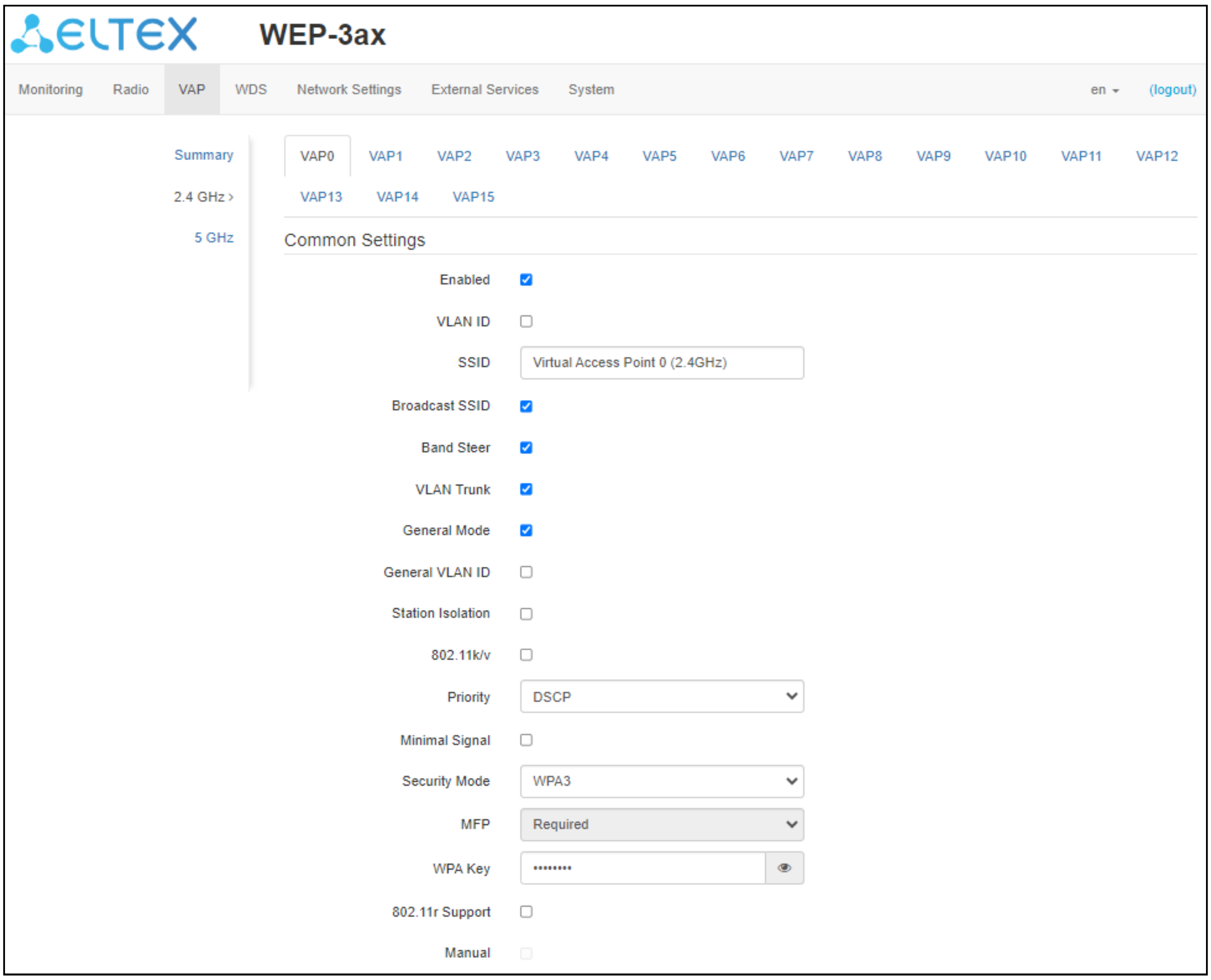


VAP	Enabled	Security Mode	VLAN ID	SSID	Broadcast SSID	Band Steer	VLAN Trunk	General Mode	General VLAN ID	Station Isolation
VAP0	☑	Off	□	Virtual Access Point 0 (2.4G	☑	□	□	□	□	□
VAP1	□	Off	□	Virtual Access Point 1 (2.4G	☑	□	□	□	□	□
VAP2	□	Off	□	Virtual Access Point 2 (2.4G	☑	□	□	□	□	□
VAP3	□	Off	□	Virtual Access Point 3 (2.4G	☑	□	□	□	□	□

- *VAP0..15* – the sequence number of the virtual access point;
- *Enabled* – when checked, the virtual access point is enabled, otherwise it is disabled;
- *Security Mode* – the type of data encryption used on the virtual access point;
- *VLAN ID* – VLAN number from which the tag will be removed when transmitting Wi-Fi traffic to clients connected to this VAP. When traffic flows in the opposite direction, untagged traffic from clients will be tagged with VLAN ID (when VLAN Trunk mode is disabled);
- *SSID* – virtual wireless network name;
- *Broadcast SSID* – when checked, SSID broadcasting is on, otherwise it is disabled;
- *Band Steer* – when checked, the client's priority connection to the 5 GHz network is active. For this function to work, it is required to create a VAP with the same SSID on each radio interface, and activate the "Band Steer" option on them;
- *VLAN Trunk* – when checked, tagged traffic is transmitted to the subscriber;
- *General Mode* – when checked, 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 be transmitted to the client without a tag. When traffic passes in the opposite direction, untagged traffic will be tagged with General VLAN ID;
- *Station Isolation* – when checked, traffic isolation between clients in the same VAP is enabled.

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

5.6.2 "VAP" submenu



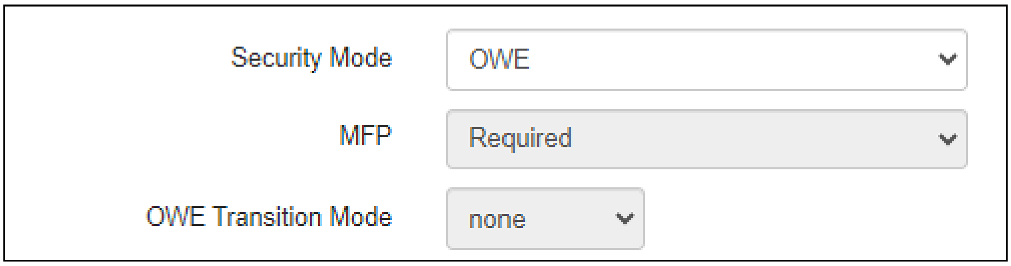
Common Settings

Enabled	☑
VLAN ID	□
SSID	Virtual Access Point 0 (2.4GHz)
Broadcast SSID	☑
Band Steer	☑
VLAN Trunk	☑
General Mode	☑
General VLAN ID	□
Station Isolation	□
802.11k/v	□
Priority	DSCP
Minimal Signal	□
Security Mode	WPA3
MFP	Required
WPA Key	••••••••
802.11r Support	□
Manual	□

<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* – when checked, the client's priority connection to the 5 GHz network is active. For this function to work, you need to create a VAP with the same SSID on each radio interface, and activate the "Band Steer" option on them;
- *VLAN Trunk* – when checked, tagged traffic is transmitted to the subscriber;
- *General Mode* – when checked, 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 be transmitted 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 802.11k/v support on the virtual access point;
- *Priority* – select prioritization means. Defines the field on the basis of which the traffic transmitted to the radio interface will be distributed in WMM queues:
  - *DSCP* – will analyze the priority from the DSCP field of the IP packet header;
  - *802.1p* – will analyze the priority from the CoS (Class of Service) field of the tagged packets.

- *Minimal Signal* – when checked, the function of disabling the client Wi-Fi equipment at low signal level (Minimal Signal) is enabled. The following parameters should be configured for the functionality to operate:
  - *Minimal Signal Level* – signal level in dBm below which the client equipment is disconnected from the virtual network;
  - *Roaming Signal Level* – roaming sensitivity level in dBm, below which the client equipment is switched to another access point. The parameter should be lower than the *Minimal Signal:* If *Minimal Signal* = -75 dBm, then the *Roaming Signal Level* should be equal to -70 dBm, for example;
  - *Minimal Signal Timeout* – the period of time after which the decision is made to disconnect the client equipment from the virtual network.
- *Security Mode* – wireless access security mode:
  - *Off* – do not use encryption for data transfer. The access point is available for any subscriber to connect. For open networks, one can additionally configure OWE Transition mode. In the *Security Mode* field, specify the *OWE* encryption type for the interface with which the connection will be established.



Security Mode: OWE

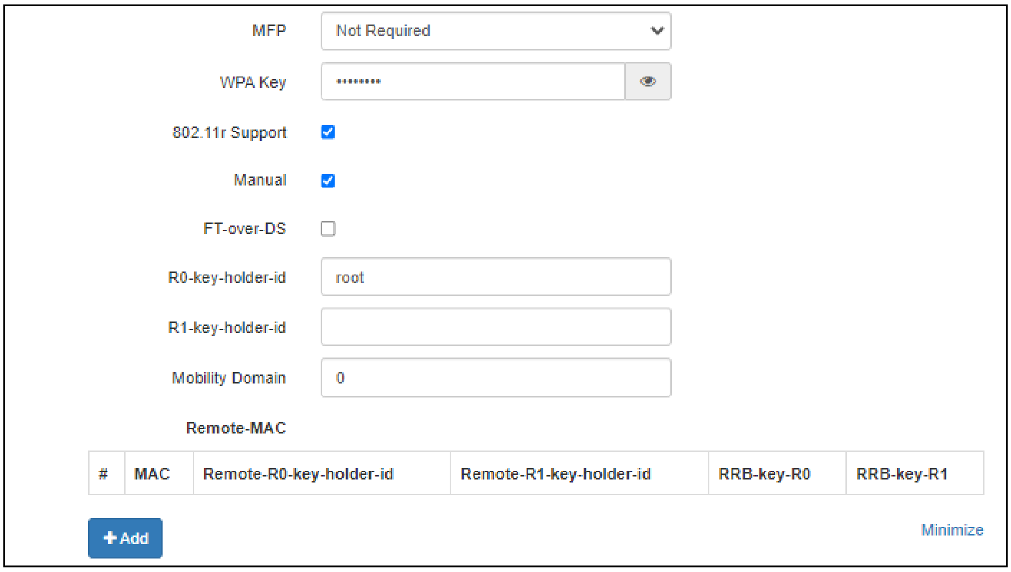
MFP: Required

OWE Transition Mode: none

- *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;

✓ OWE transition mode provides backward compatibility with Wi-Fi clients that do not support OWE authentication. When attempting to connect to an open network with configured OWE transition, a client that supports OWE will connect to the encrypted network configured on the specified interface, while a client without OWE support will connect to the current open network without encryption.

- *WPA, WPA2, WPA/WPA2, WPA2/WPA3, WPA3* – encryption methods, if one of these methods is chosen, the following setting will be available:
  - *WPA Key* – key/password required to connect to the virtual access point. The length of the key is from 8 to 63 characters.
- *WPA-Enterprise, WPA2-Enterprise, WPA3-Enterprise, WPA/WPA2-Enterprise, WPA2/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.

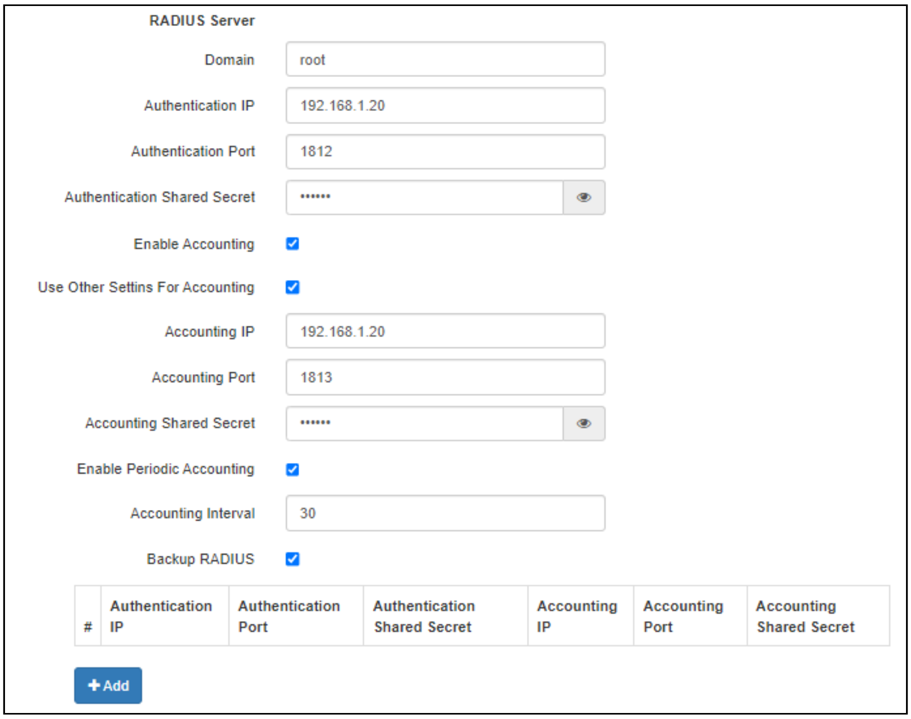


MFP	Not Required
WPA Key	••••••••
802.11r Support	☑
Manual	☑
FT-over-DS	□
R0-key-holder-id	root
R1-key-holder-id	
Mobility Domain	0

Remote-MAC

#	MAC	Remote-R0-key-holder-id	Remote-R1-key-holder-id	RRB-key-R0	RRB-key-R1

- *MFP* – management frame protection (available for WPA2, WPA3, WPA2/WPA3, WPA2-Enterprise, WPA3-Enterprise, WPA2/WPA3-Enterprise security modes. When choosing other security modes, MFP is set to "Disabled" state. When WPA3 security mode is chosen, MFP is set to "Enabled" state):
  - *Not required* – MFP is disabled;
  - *Capable* – MFP works if client supports MFP. Clients without MFP support can be connected to this VAP;
  - *Required* – MFP is enabled, clients without MFP support can not be connected to this VAP.
- *802.11r* – fast roaming works only with clients supporting the IEEE 802.11r standard. The 802.11r roaming is possible only between VAPs with WPA2, WPA3, WPA2/WPA3, WPA2-Enterprise, WPA3-Enterprise, WPA2/WPA3-Enterprise security modes.
  - *802.11r Support* – enable 802.11r support on the VAP;
  - *Manual* – when checked, it is possible to manually set-up roaming parameters;
  - *FT-over-DS* – enable the "Over the DS" mode;
  - *R0-key-holder-id* – a unique key for a given VAP, for example, a serial key number;
  - *R1-key-holder-id* – MAC address of VAP (it can be seen using the ifconfig command);
  - *Mobility Domain* – number of group within which the roaming can be completed. Accepts values from 0 to 65535;
  - *Remote-MAC:*
    - *MAC* – MAC address of the remote accesss point VAP interface. Maiximum number – 256;
    - *Remote-R0-key-holder-id – a* unique key, should match "*R0-key-holder-id* " on the VAP of the remote AP;
    - *Remote-R1-key-holder-id* – MAC address of VAP on the remote AP;
    - *RRB-key-R0* – random key. It should not match "RRB-key-R1", but definitely should match the "RRB key R1" of the remote AP. The key length – 16 characters;
    - *RRB-key-R1* – random key. It should not match "RRB-key-R0", but definitely should match the "RRB key R0" of the remote AP. The key length – 16 characters.



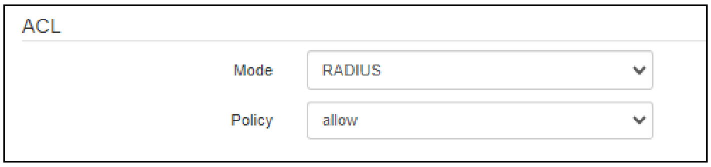
RADIUS Server

Domain	root
Authentication IP	192.168.1.20
Authentication Port	1812
Authentication Shared Secret	••••••
Enable Accounting	☑
Use Other Settins For Accounting	☑
Accounting IP	192.168.1.20
Accounting Port	1813
Accounting Shared Secret	••••••
Enable Periodic Accounting	☑
Accounting Interval	30
Backup RADIUS	☑

#	Authentication IP	Authentication Port	Authentication Shared Secret	Accounting IP	Accounting Port	Accounting Shared Secret

RADIUS Server

- *Domain* – user domain;
- *Authentication IP* – RADIUS server address;
- *Authentication Port* – port of the RADIUS server that used for authentication and authorization;
- *Authentication Shared Secret* – key for the RADIUS server used for authentication and authorization;
- *Enable Accounting* – when checked, "Accounting" messages will be sent to the RADIUS server;
- *Use Other Settings For Accounting:*
    - *Accounting IP* – address of the RADIUS server, used for accounting;
    - *Accounting Port* – port that will be used to collect accounting on the RADIUS server;
    - *Accounting Shared Secret* – password for the RADIUS server used for accounting.
- *Enable Periodic Accounting* – enable periodic sending of "Accounting" messages to the RADIUS server:
    - *Accounting Interval* – interval for sending the "Accounting" messages to the RADIUS server in seconds.
- *Backup RADIUS* – when checked, a table appears where the backup RADIUS servers can be added. If the primary RADIUS server is unavailable, requests will be sent to backup RADIUS servers listed in the table. The parameters in the table correspond to the parameters described above. In total up to 4 backup RADIUS servers can be added.



ACL

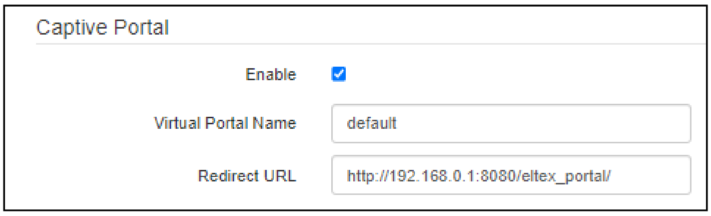
Mode: RADIUS

Policy: allow

ACL

MAC address authentification.

- *Mode*:
  - *Off* – disbale MAC address authentification;
  - *RADIUS* – enable user RADIUS MAC authentication.
- *Policy*:
  - *allow* – for the current SSID the selected list will be white (the access is allowed for devices from the list);
  - *deny* – for the current SSID the selected list will be black (the access is denied for devices from the list).



Captive Portal

Enable: ☑

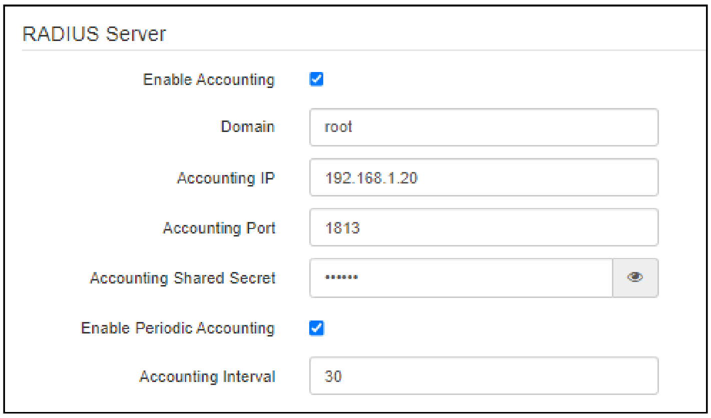
Virtual Portal Name: default

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

Captive Portal

For such security modes as Off, WPA, WPA2, WPA/WPA2, WPA3, WPA2/WPA3 captive portal 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 Server

Enable Accounting: ☑

Domain: root

Accounting IP: 192.168.1.20

Accounting Port: 1813

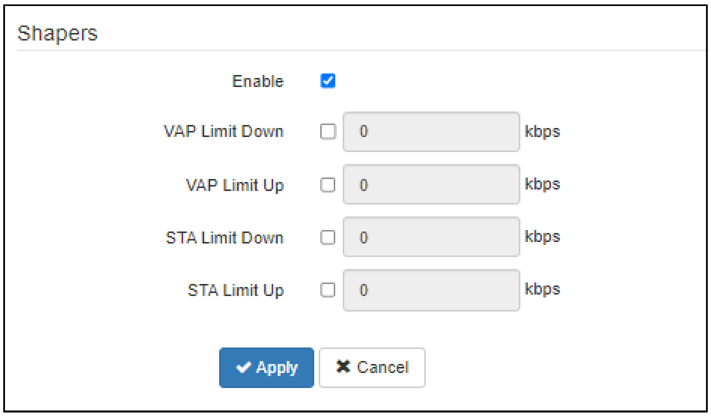
Accounting Shared Secret: ••••••

Enable Periodic Accounting: ☑

Accounting Interval: 30

RADIUS

- *Enable Accounting* – when checked, "Accounting" messages will be sent to the RADIUS server;
- *Domain* – user domain;
- *Accounting IP* – address of the RADIUS server, used for accounting;
- *Accounting Port* – port that will be used to collect accounts on the RADIUS server;
- *Accounting Shared Secret* – password for the RADIUS server used for accounting;
- *Enable Periodic Accounting* – enable periodic sending of "Accounting" messages to the RADIUS server:
  - *Accounting Interval* – interval for sending the "Accounting" messages to the RADIUS server in seconds.



Shapers

Enable ☑

VAP Limit Down □ 0 kbps

VAP Limit Up □ 0 kbps

STA Limit Down □ 0 kbps

STA Limit Up □ 0 kbps

Shapers

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

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

5.7 "WDS" menu

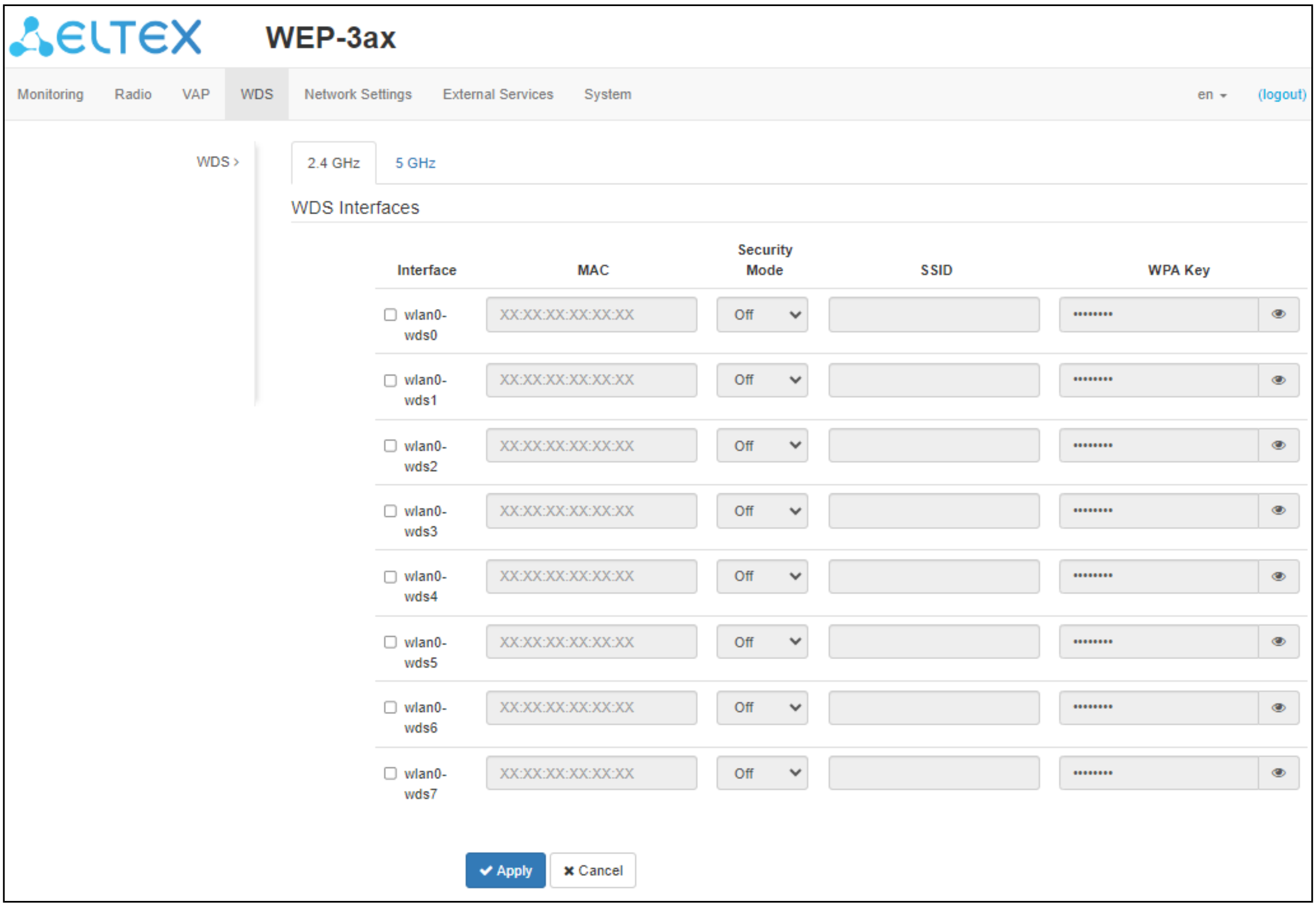
In the **"WDS"** menu, wireless bridges between WEP-3ax are configured.

> When configuring a WDS connection, it is necessary to select the same channel and channel width in the radio interface settings on the the devices that will be connected via WDS. Auto-channel should be disabled and the DFS option should be set to "off" or "forced".
> More detailed information about configuring the radio interface via the command line can be found in the Radio configuration section.

> When configuring a WDS connection on the Radio 2.4 GHz/Radio 5 GHz it is necessary to enable VAP0 on the Radio 2.4 GHz/Radio 5 GHz. The encryption modes on VAP and WDS interfaces should be the same.
> More detailed information about configuring VAPs can be found in the Virtual Wi-Fi access points (VAPs) configuration section.

5.7.1 "WDS" submenu

In the "2.4 GHz" and "5 GHz" tabs of the "WDS" submenu, select the radio interface of the device on which a wireless bridge should be built.



WDS Interfaces

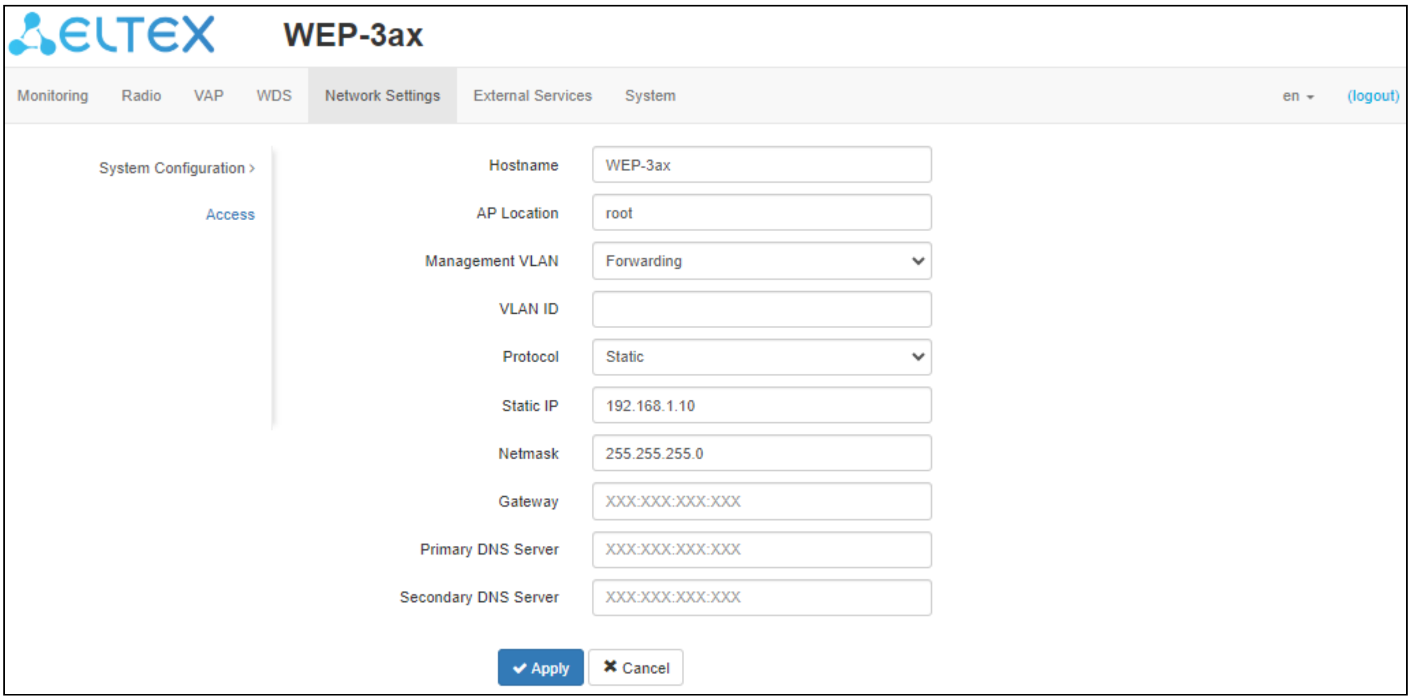
Interface	MAC	Security Mode	SSID	WPA Key
□ wlan0-wds0	XX:XX:XX:XX:XX:XX	Off		••••••••
□ wlan0-wds1	XX:XX:XX:XX:XX:XX	Off		••••••••
□ wlan0-wds2	XX:XX:XX:XX:XX:XX	Off		••••••••
□ wlan0-wds3	XX:XX:XX:XX:XX:XX	Off		••••••••
□ wlan0-wds4	XX:XX:XX:XX:XX:XX	Off		••••••••
□ wlan0-wds5	XX:XX:XX:XX:XX:XX	Off		••••••••
□ wlan0-wds6	XX:XX:XX:XX:XX:XX	Off		••••••••
□ wlan0-wds7	XX:XX:XX:XX:XX:XX	Off		••••••••

- *Interface* – selecting and enabling the WDS interface on which the wireless bridge will be built;
- *MAC address* – MAC address of the radio interface on the remote device to which the wireless bridge is configured. The MAC address of the radio interface can be found in the remote device web interface, Monitoring/Radio information submenu. To configure WDS on the Radio 2.4 GHz, it is required to specify the MAC address of the remote device Radio 2.4 GHz. The configuration of WDS on the Radio 5 GHz is done in the same way — the MAC address of the remote device Radio 5 GHz is specified.
- *Security Mode* – security mode of access to the wireless network:
  - *Off* – disable the encryption for data transmission;
  - *WPA2* – encryption method, when selected the following settings will be available:
    - *SSID* – Wi-Fi network name;
    - *WPA Key* – key/password required for connection to the remote access point. The key length is from 8 to 63 characters.

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

5.8 "Network settings" menu

5.8.1 "System Configuration" submenu



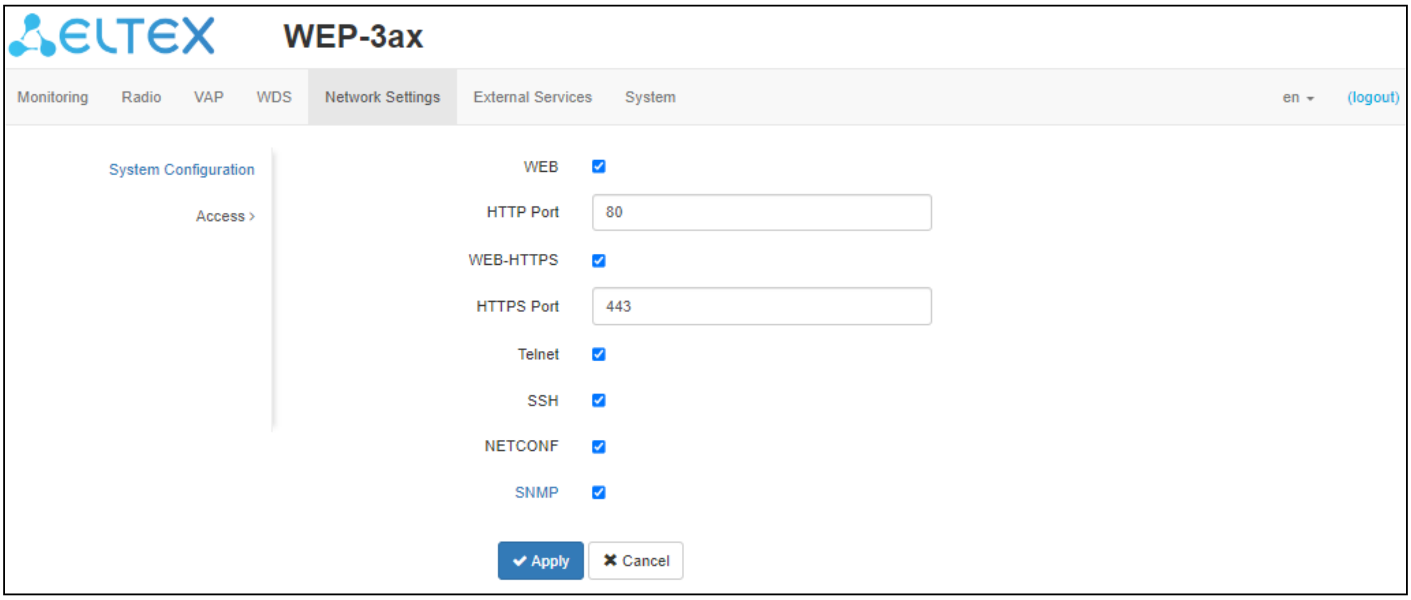
Hostname	WEP-3ax
AP Location	root
Management VLAN	Forwarding
VLAN ID	
Protocol	Static
Static IP	192.168.1.10
Netmask	255.255.255.0
Gateway	XXX:XXX:XXX:XXX
Primary DNS Server	XXX:XXX:XXX:XXX
Secondary DNS Server	XXX:XXX:XXX:XXX

- *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* – 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 where IP address and all the necessary parameters for WAN interface are assigned statically. If "Static" is selected, the following parameters will be available to set:
        - *Static IP* – 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 allocated automatically via DHCP, set them manually.

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

5.8.2 "Access" submenu

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



WEB ☑

HTTP Port: 80

WEB-HTTPS ☑

HTTPS Port: 443

Telnet ☑

SSH ☑

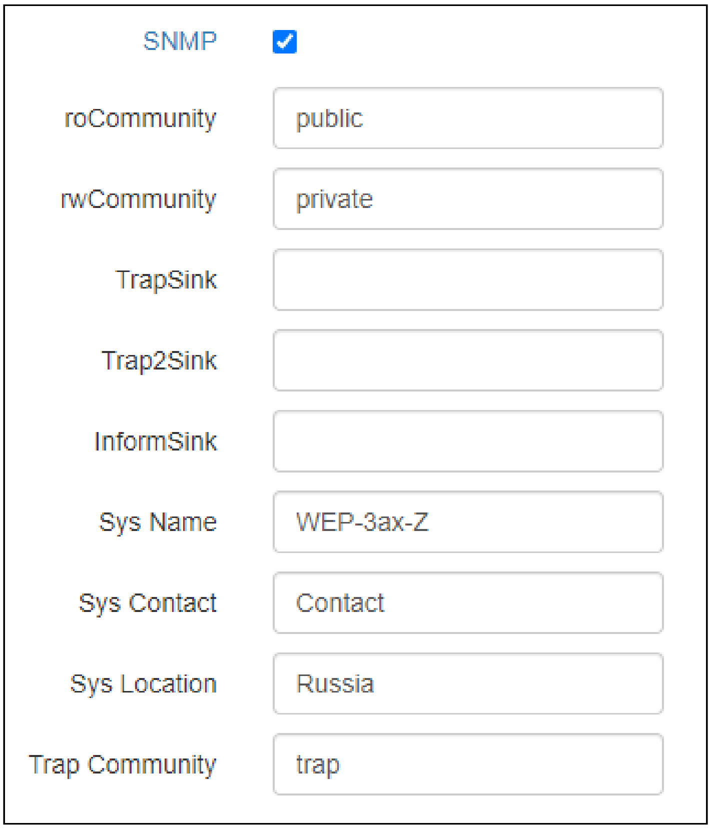
NETCONF ☑

SNMP ☑

- To enable access to the device via the web interface via HTTP protocol, check the box 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, is from 1025 to 65535 inclusive;
- To enable access to the device via the web interface via HTTPS protocol, check the box 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, is 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".



SNMP	☑
roCommunity	public
rwCommunity	private
TrapSink	
Trap2Sink	
InformSink	
Sys Name	WEP-3ax-Z
Sys Contact	Contact
Sys Location	Russia
Trap Community	trap

To change the parameters of the access point SNMP agent, it is necessary to check the "SNMP" box and click the "SNMP", a list of parameters available for editing will appear:

- *roCommunity* – password for parameter reading (common: *public*);
- *rwCommunity* – password for parameter writing (common: *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 which is contained in traps (by default: trap).

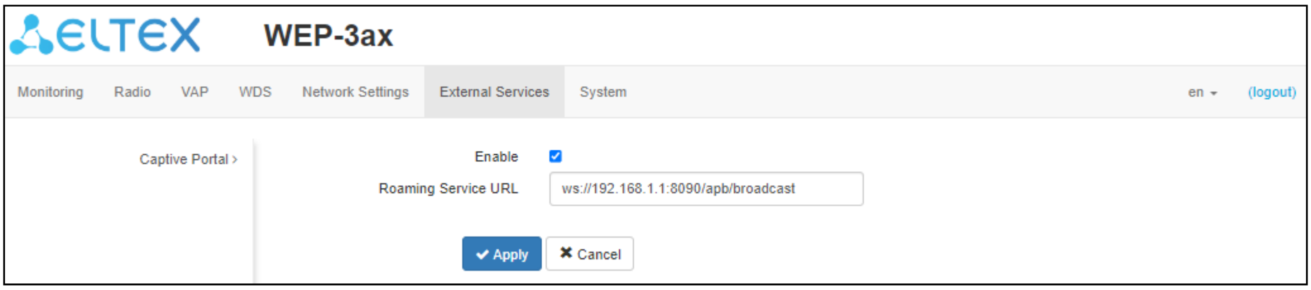
To apply a new configuration and save setting to non-volatile memory, click "Apply". Click "Cancel" to discard the changes.

5.9 "External Services" menu

5.9.1 "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

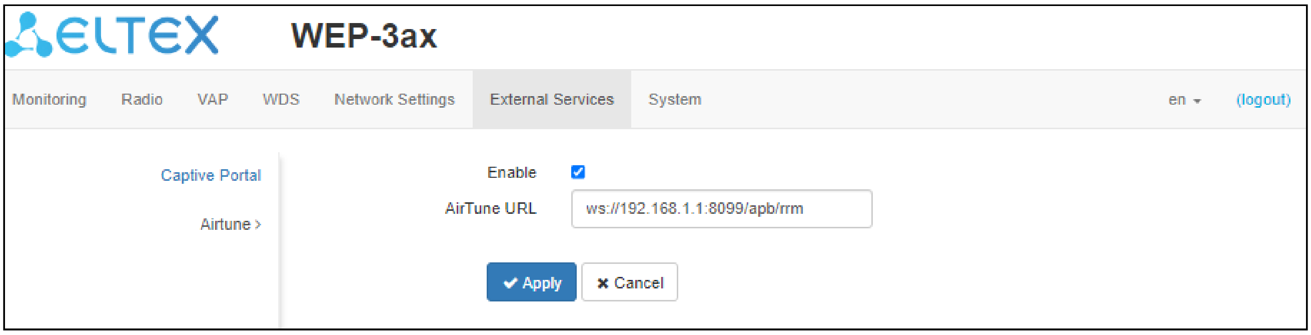
- *Enable* – when checked, the point will connect to the APB service, the address of which is specified in the "Roaming Service URL" field, to provide portal roaming of clients;
- *Roaming Service URL* – APB service address to support roaming in the portal authorization mode. Specified as: "ws://<host>: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

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

5.9.2 "AirTune" submenu

The **"AirTune"** submenu is designed to enable and configure the AirTune service at the access point.

The AirTune service is used to optimize radio resources (Radio Resource Management) and automatically configure seamless 802.11 k/v/r roaming.



Enable ☑

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

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

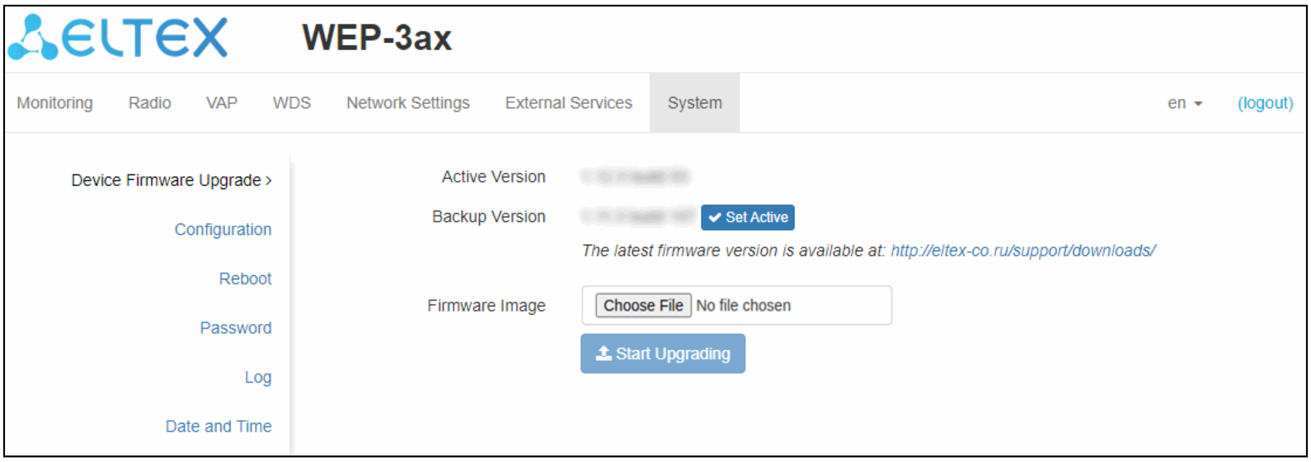
To apply a new configuration and save settings to non-volatile memory, click "Apply". Click "Cancel" to discard the changes.

5.10 "System" menu

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

5.10.1 "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 making a backup version of the firmware active, this will require a reboot of the device. The active firmware version will not be set as a backup.

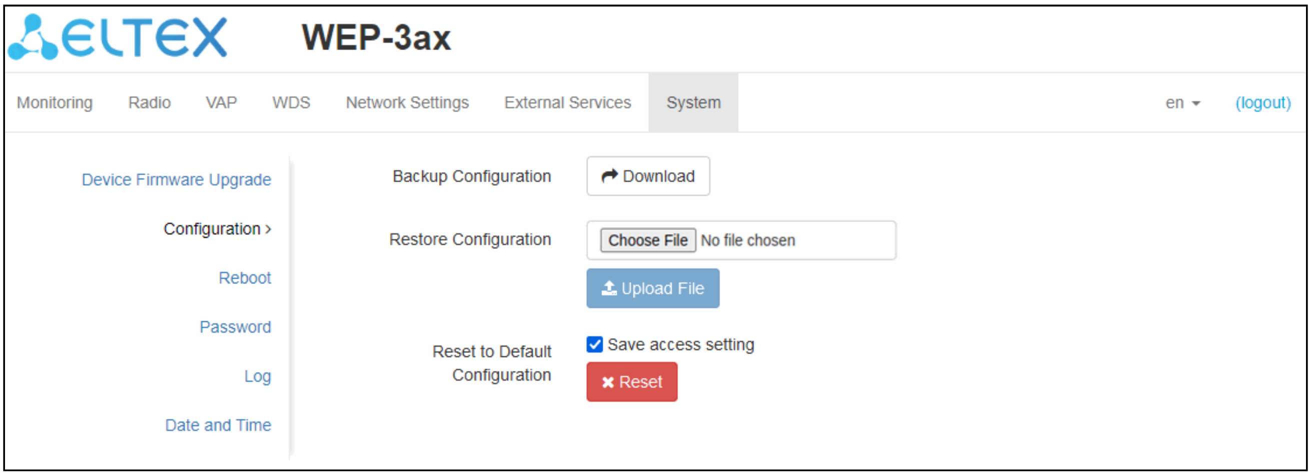
Firmware upgrading

Download the firmware file from *http://eltex-co.com/support/downloads/* and save it on your computer. To do this, 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 "Start Upgrading". The process may take several minutes (its current status will be shown on the page). The device will automatically reboot when the upgrade is completed.

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

5.10.2 "Configuration" submenu

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



☑ Save access setting

Backup Configuration

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

Restore Configuration

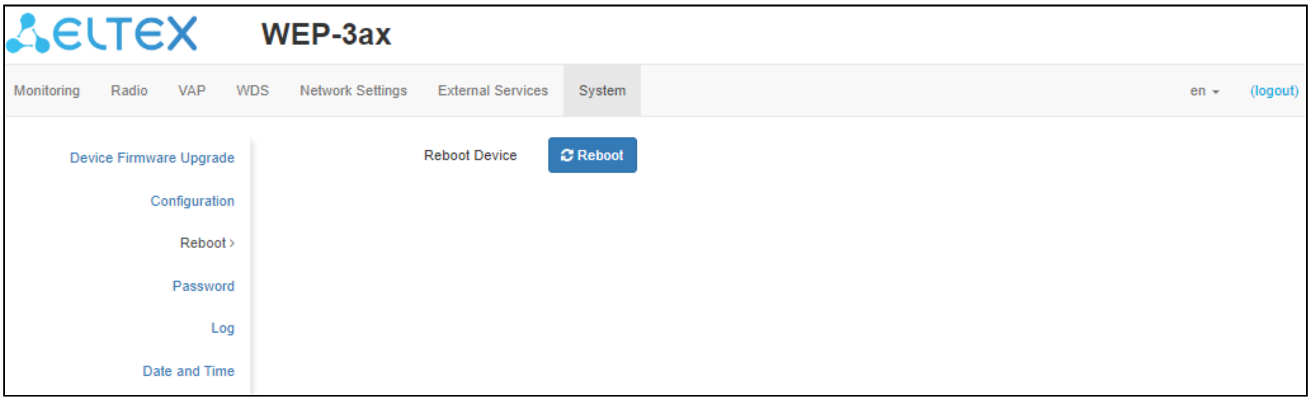
To download the configuration file saved on the local computer, use the *Restore Configuration* item. To update the device configuration, click "Choose File" and specify a file (in .tar.gz format) and click "Upload File". Uploaded configuration will be applied automatically and does not require device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

Reset to Default Configuration

To reset all the settings to default values, click "Reset". If the "Save access setting" box is checked, then those settings that are responsible for access to the device (IP address settings, Telnet/SSH/SNMP/Netconf/web access settings) will be saved.

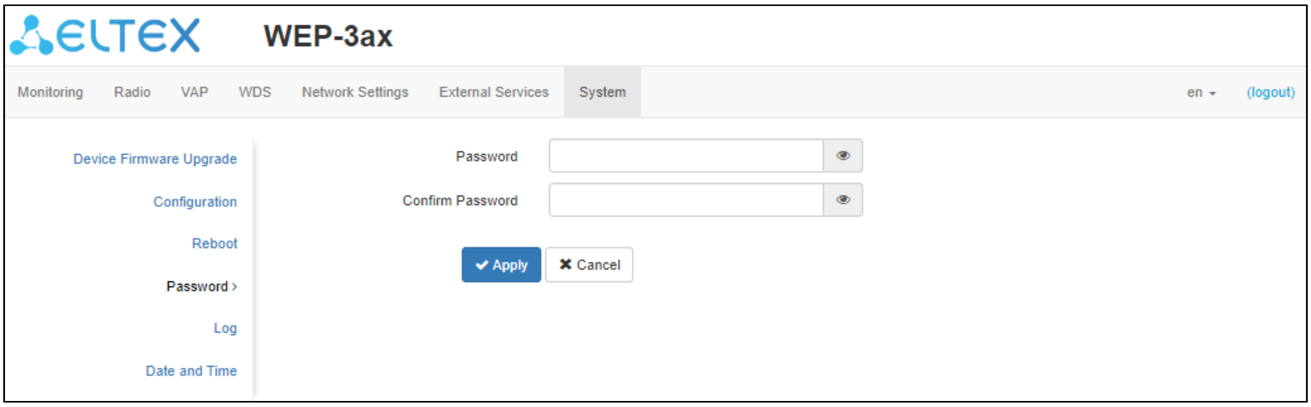
5.10.3 "Reboot" submenu

To reboot the device, click "Reboot". The device reboot process takes about 1 minute.



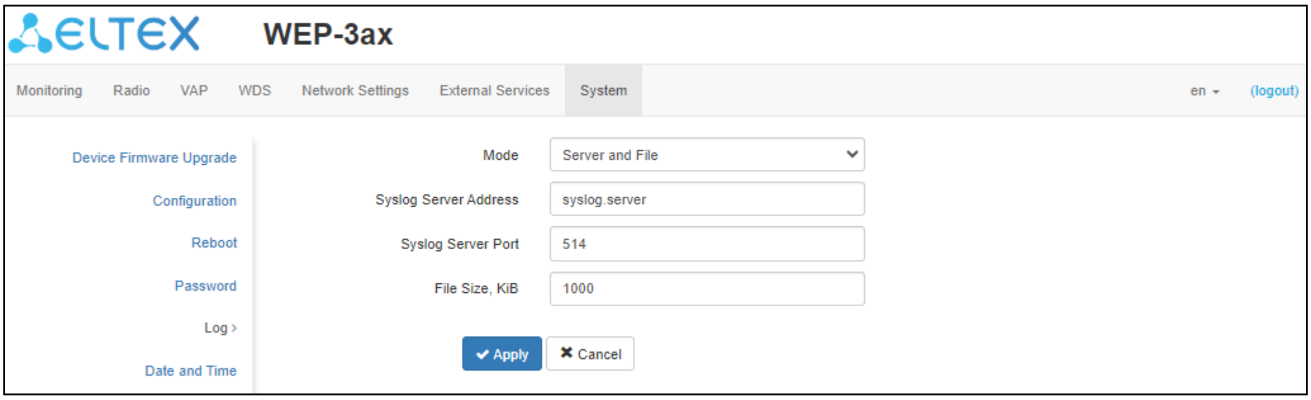
5.10.4 "Password" submenu

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 repeat this password in the "Confirm Password" field and click "Apply" to save the configuration.



5.10.5 "Log" submenu

The **"Log"** submenu is intended to configure the output of various kinds of system debugging messages in order to detect the causes of problems in the device operation.



Mode: Server and File

Syslog Server Address: syslog.server

Syslog Server Port: 514

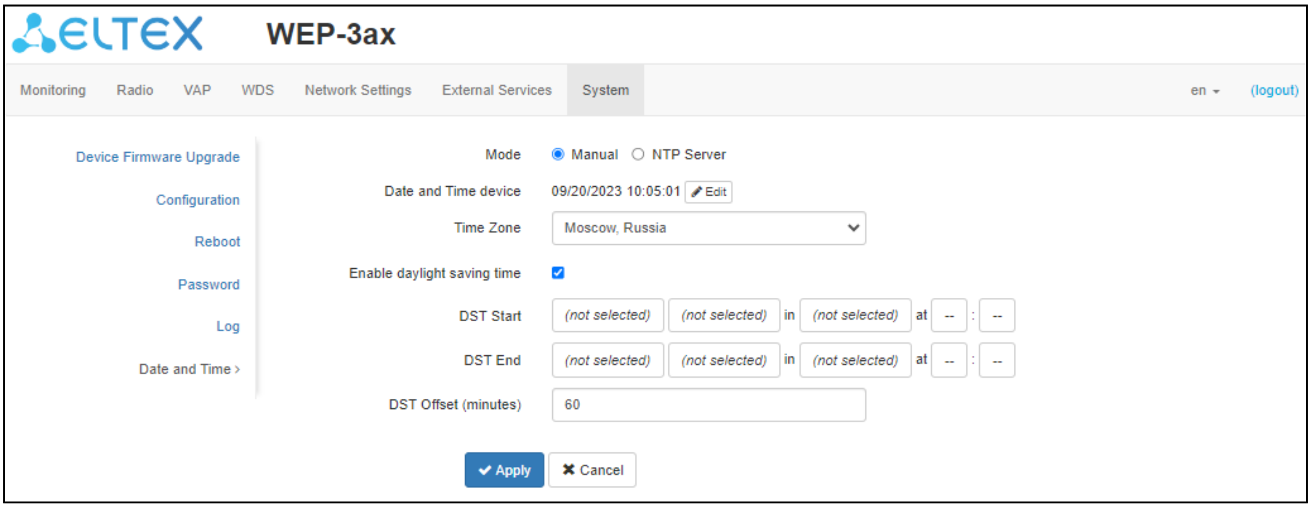
File Size, KiB: 1000

- *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 "Monitoring/Events" tab*;*
  - *Server and File* – log information is sent to a remote Syslog server and stored in a local file.
- *Syslog Server Address* – IP address or domain name of the Syslog server;
- *Syslog Server Port* – port for incoming Syslog server messages (default: 514, valid values: from 1 to 65535);
- *File Size* – maximum size of the log file (valid values: 1–1000 kB).

5.10.6 "Date and Time" submenu

In the **"Date and Time"** submenu, the time can be set up manually or using the time synchronization protocol (NTP).

5.10.6.1 Manual



Mode ● Manual ○ NTP Server

Date and Time device 09/20/2023 10:05:01

Time Zone Moscow, Russia

Enable daylight saving time ☑

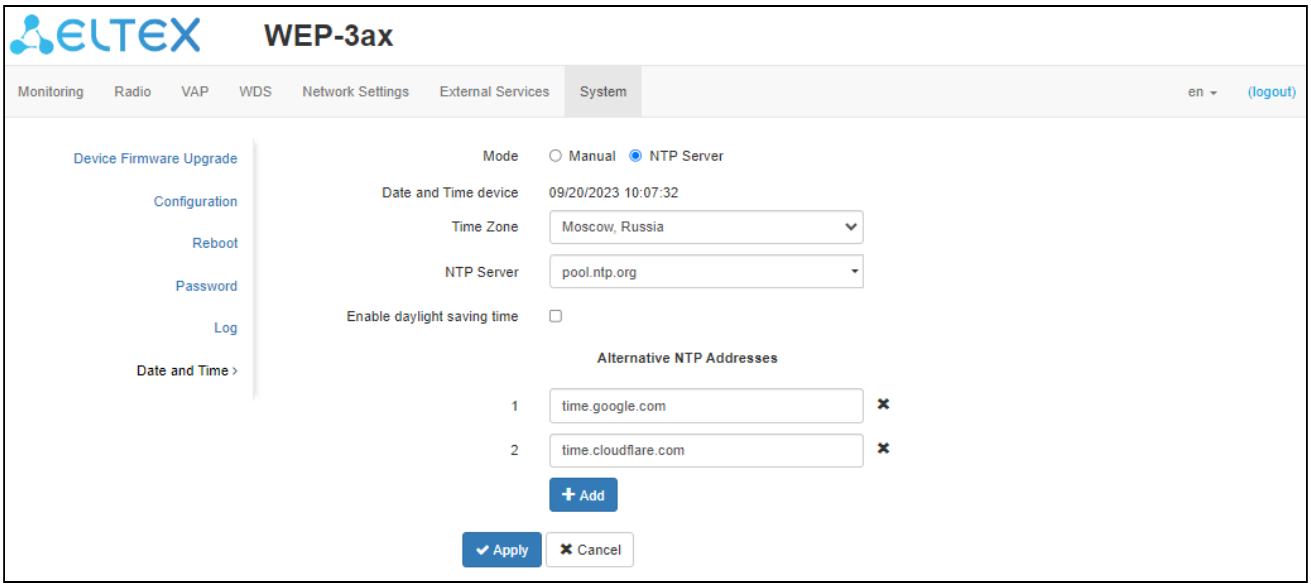
DST Start (not selected) (not selected) in (not selected) at -- : --

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

DST Offset (minutes) 60

- *Date and Time device* – date and time set on the device. Click "Edit" if the correction is necessary;
  - *Date, Time* – set the current date and time or click "Set current date and time" to synchronize with the device;
- *Time Zone* – allows setting the time zone according to the nearest city for your region from the list;
- *Enable daylight saving time* – when checked, 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.

5.10.6.2 NTP Server



Mode ○ Manual ● NTP Server

Date and Time device 09/20/2023 10:07:32

Time Zone Moscow, Russia

NTP Server pool.ntp.org

Enable daylight saving time □

Alternative NTP Addresses

1 time.google.com ✖

2 time.cloudflare.com ✖

- *Date and Time device* – date and time set on the device at the current moment;
- *NTP Server* – time synchronization server IP address/domain name. Specify an address or select from an existing list;
- *Time Zone* – allows setting the time zone according to the nearest city for your region from the list;
- *Alternative NTP Addresses* – in case when the primary time synchronization server is not available, the device will contact additional time synchronization servers. To add an address to the list, click "Add" and enter the IP address or domain name of the server in the displayed window. To remove an address from the list, click ✖ in the corresponding line.

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

6 Device management via the command line

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

6.1 Connection to the device

By default, WEP-3ax is configured to receive the address via DHCP. If this does not happen, it is possible to connect to the device using the factory IP address.

The default IP-address of WEP-3ax: **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 access point static parameters

```
WEP-3ax(root):/# configure
WEP-3ax(config):/# interface
WEP-3ax(config):/interface# br0
WEP-3ax(config):/interface/br0# common
WEP-3ax(config):/interface/br0/common# static-ip X.X.X.X (where X.X.X.X – WEP-3ax IP address)
WEP-3ax(config):/interface/br0/common# netmask X.X.X.X (where X.X.X.X – subnet mask)
WEP-3ax(config):/interface/br0/common# dns-server-1 X.X.X.X (where X.X.X.X – IP address of the dns server #1)
WEP-3ax(config):/interface/br0/common# dns-server-2 X.X.X.X (where X.X.X.X – IP address of the dns server #2)
WEP-3ax(config):/interface/br0/common# protocol static-ip (change operation mode from DHCP to Static-IP)
WEP-3ax(config):/interface/br0/common# save (save configuration)
```

Adding a static route

```
WEP-3ax(config):/interface/br0/common# exit
WEP-3ax(config):/interface/br0# exit
WEP-3ax(config):/interface# exit
WEP-3ax(config):/# route
WEP-3ax(config):/route# add default (where default – route name)
WEP-3ax(config):/route# default
WEP-3ax(config):/route/default# destination X.X.X.X (where X.X.X.X – destination host or network IP address, for the default route – 0.0.0.0)
WEP-3ax(config):/route/default# netmask X.X.X.X (where X.X.X.X – destination network mask, for the default route – 0.0.0.0)
WEP-3ax(config):/route/default# gateway X.X.X.X (where X.X.X.X – gateway IP address)
WEP-3ax(config):/route/default# save (save configuration)
```

Configuring the reception of network parameters via DHCP

```
WEP-3ax(root):/# configure
WEP-3ax(config):/# interface
WEP-3ax(config):/interface# br0
WEP-3ax(config):/interface/br0# common
WEP-3ax(config):/interface/br0/common# protocol dhcp
WEP-3ax(config):/interface/br0/common# save (save configuration)
```

6.2.1 Network parameters configuration using the set-management-vlan-mode utility

Untagged access
Obtain network settings via DHCP: WEP-3ax(root):/# **set-management-vlan-mode off protocol dhcp** Static settings: WEP-3ax(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
Obtain network settings via DHCP: WEP-3ax(root):/# **set-management-vlan-mode terminating vlan-id X protocol dhcp** (where X – VLAN ID used for device access. Possible values: 1–4094) Static settings: WEP-3ax(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 device access. Possible values: 1–4094, X.X.X.X – static IP address; Y.Y.Y.Y – subnet mask; Z.Z.Z.Z – gateway)

Access via management VLAN in Forwarding mode
Obtain network settings via DHCP: WEP-3ax(root):/# **set-management-vlan-mode forwarding vlan-id X protocol dhcp** (where X – VLAN ID used for device access. Possible values: 1–4094) Static settings: WEP-3ax(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 device access. Possible values: 1–4094, X.X.X.X – static IP address; Y.Y.Y.Y – subnet mask; Z.Z.Z.Z – gateway)

Completing and saving configuration
WEP-3ax(root):/# **save** (save configuration)

6.3 Virtual Wi-Fi access points (VAPs) configuration

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

Table 7 – 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	security-mode OWE
WPA-Enterprise	mode WPA_1X
WPA2-Enterprise	mode WPA2_1X
WPA/WPA2-Enterprise	mode WPA_WPA2_1X
WPA3-Enterprise	mode WPA3_1X
WPA2/WPA3-Enterprise	mode WPA2_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

```
WEP-3ax(root):/# configure
WEP-3ax(config):/# interface
WEP-3ax(config):/interface# wlan1-vap0
WEP-3ax(config):/interface/wlan1-vap0# common
WEP-3ax(config):/interface/wlan1-vap0/common# enabled true (enable virtual access point)
WEP-3ax(config):/interface/wlan1-vap0/common# exit
WEP-3ax(config):/interface/wlan1-vap0# vap
WEP-3ax(config):/interface/wlan1-vap0/vap# ssid 'SSID_WEP-3ax_open' (change SSID name)
WEP-3ax(config):/interface/wlan1-vap0/vap# ap-security (go to the security settings block on the VAP)
WEP-3ax(config):/interface/wlan1-vap0/vap/ap-security# mode off (encryption mode off – without
password)
WEP-3ax(config):/interface/wlan1-vap0/vap/ap-security# save (save configuration)
```

6.3.2 Configuration of VAP with OWE encryption

Creating a VAP with OWE encryption

```
WEP-3ax(root):/# configure
WEP-3ax(config):/# interface
WEP-3ax(config):/interface# wlan1-vap0
WEP-3ax(config):/interface/wlan1-va0# vap
WEP-3ax(config):/interface/wlan1-va0/vap# ssid 'SSID_WEP-3ax_owe' (change SSID name)
WEP-3ax(config):/interface/wlan1-va0/vap# ap-security
WEP-3ax(config):/interface/wlan1-va0/vap/ap-security# mode OWE (security-mode OWE — encrypted
connection without entering a password. In this mode, only Wi-Fi 6 clients can connect)
WEP-3ax(config):/interface/wlan1-va0/vap/ap-security# exit
WEP-3ax(config):/interface/wlan1-va0/vap# radius
WEP-3ax(config):/interface/wlan1-va0/vap/radius# acct-enable true (enabling sending of “Accounting”
messages to the RADIUS server. Default: false)
WEP-3ax(config):/interface/wlan1-va0/vap/radius# acct-address X.X.X.X (where X.X.X.X — IP address of
the RADIUS server used for accounting)
WEP-3ax(config):/interface/wlan1-va0/vap/radius# acct-password secret (where secret — password of
the RADIUS server used for accounting)
WEP-3ax(config):/interface/wlan1-va0/vap/radius# acct-periodic true (enabling periodic sending of
“Accounting” messages to the RADIUS server. Default: false)
WEP-3ax(config):/interface/wlan1-va0/vap/radius# acct-interval 600 (interval for sending “Accounting”
messages to the RADIUS server)
WEP-3ax(config):/interface/wlan1-va0/vap/radius# exit
WEP-3ax(config):/interface/wlan1-va0/vap# exit
WEP-3ax(config):/interface/wlan1-va0# common
WEP-3ax(config):/interface/wlan1-va0/common# enabled true (enable virtual access point)
WEP-3ax(config):/interface/wlan1-va0/common# save (save configuration)
```

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-3ax(root):/# configure
WEP-3ax(config):/# interface
WEP-3ax(config):/interface# wlan1-vap0 (set up a hidden VAP with OWE encryption. Wi-Fi 6 clients will implicitly connect to it)
WEP-3ax(config):/interface/wlan1-va0# vap
WEP-3ax(config):/interface/wlan1-va0/vap# ssid 'SSID_WEP-3ax_owe' (change SSID name)
WEP-3ax(config):/interface/wlan1-va0/vap# hidden true (hide VAP)
WEP-3ax(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-3ax(config):/interface/wlan1-va0/vap/ap-security# owe-transition-interface wlan1-vap1 (specify an open VAP to which the connection will occur. The Wi-Fi 6 client will implicitly work with the current VAP with OWE encryption, and other clients will work with the open VAP)
WEP-3ax(config):/interface/wlan1-va0/vap/ap-security# exit
WEP-3ax(config):/interface/wlan1-va0/vap# exit
WEP-3ax(config):/interface/wlan1-va0# common
WEP-3ax(config):/interface/wlan1-va0/common# enabled true (enable virtual access point)
WEP-3ax(config):/interface/wlan1-va0/common#exit
WEP-3ax(config):/interface/wlan1-va0#  exit
WEP-3ax(config):/interface# wlan1-vap1 (set up VAP without encryption)
WEP-3ax(config):/interface/wlan1-vap1# vap
WEP-3ax(config):/interface/wlan1-vap1/vap# ssid 'SSID_WEP-3ax_open' (change SSID name)
WEP-3ax(config):/interface/wlan1-vap1/vap# ap-security (go to the security settings block on the VAP)
WEP-3ax(config):/interface/wlan1-vap1/vap/ap-security# mode off (encryption mode off — without password)
WEP-3ax(config):/interface/wlan1-vap1/vap/ap-security# owe-transition-interface wlan1-vap0 (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-3ax(config):/interface/wlan1-vap1/vap/ap-security# exit
WEP-3ax(config):/interface/wlan1-vap1/vap# exit
WEP-3ax(config):/interface/wlan1-vap1# common
WEP-3ax(config):/interface/wlan1-vap1/common# enabled true (enable virtual access point)
WEP-3ax(config):/interface/wlan1-vap1/common#exit
WEP-3ax(config):/interface/wlan1-vap1# save (save configuration)
```

6.3.4 Configuration of VAP with WPA-Personal security mode

Creating a VAP with WPA-Personal security mode

```
WEP-3ax(root):/# configure
WEP-3ax(config):/# interface
WEP-3ax(config):/interface# wlan1-vap0
WEP-3ax(config):/interface/wlan1-vap0# common
WEP-3ax(config):/interface/wlan1-vap0/common# enabled true (enable virtual access point)
WEP-3ax(config):/interface/wlan1-vap0/common# exit
WEP-3ax(config):/interface/wlan1-vap0# vap
WEP-3ax(config):/interface/wlan1-vap0/vap# ssid 'SSID_WEP-3ax_Wpa2' (change SSID name)
WEP-3ax(config):/interface/wlan1-vap0/vap# ap-security (go to the security settings block on the VAP)
WEP-3ax(config):/interface/wlan1-vap0/vap/ap-security# mode WPA2_WPA3 (encryption mode — WPA2/WPA3)
WEP-3ax(config):/interface/wlan1-vap0/vap/ap-security# key-wpa password123 (where password123 — key/password required to connect to the virtual access point. The length of the key should be between 8 and 63 characters)
WEP-3ax(config):/interface/wlan1-vap0/vap/ap-security# save (save configuration)
```

6.3.5 Configuration of VAP with Enterprise authorization

Creating a VAP with WPA3-Enterprise security mode with a periodic sending of accounting to RADIUS server

```
WEP-3ax(root):/# configure
WEP-3ax(config):/# interface
WEP-3ax(config):/interface# wlan1-vap0
WEP-3ax(config):/interface/wlan1-vap0# common
WEP-3ax(config):/interface/wlan1-vap0/common# enabled true (enable virtual access point)
WEP-3ax(config):/interface/wlan1-vap0/common# exit
WEP-3ax(config):/interface/wlan1-vap0# vap
WEP-3ax(config):/interface/wlan1-vap0/vap# ssid 'SSID_WEP-3ax_enterprise' (change SSID name)
WEP-3ax(config):/interface/wlan1-vap0/vap# ap-security (go to the security settings block on the VAP)
WEP-3ax(config):/interface/wlan1-vap0/vap/ap-security# mode WPA2_WPA3_1X (encryption mode — WPA2/WPA3-Enterprise)
WEP-3ax(config):/interface/wlan1-vap0/vap/ap-security# exit
WEP-3ax(config):/interface/wlan1-vap0/vap# radius
WEP-3ax(config):/interface/wlan1-vap0/vap/radius# domain root (where root — user domain)
WEP-3ax(config):/interface/wlan1-vap0/vap/radius# auth-address X.X.X.X (where X.X.X.X — IP address of RADIUS server)
WEP-3ax(config):/interface/wlan1-vap0/vap/radius# auth-port X (where X — RADIUS server port used for authentication and authorization. Default: 1812)
WEP-3ax(config):/interface/wlan1-vap0/vap/radius# auth-password secret (where secret — RADIUS server password used for authentication and authorization)
WEP-3ax(config):/interface/wlan1-vap0/vap/radius# acct-enable true (enable sending of "Accounting" messages to the RADIUS server. Default: false)
WEP-3ax(config):/interface/wlan1-vap0/vap/radius# acct-address X.X.X.X (where X.X.X.X — IP address of the RADIUS server used for accounting)
WEP-3ax(config):/interface/wlan1-vap0/vap/radius# acct-password secret (where secret — password of the RADIUS server used for accounting)
WEP-3ax(config):/interface/wlan1-vap0/vap/radius# acct-periodic true (enable a periodic sending of "Accounting" messages to the RADIUS server. Default: false)
WEP-3ax(config):/interface/wlan1-vap0/vap/radius# acct-interval 600 (interval of sending "Accounting" messages to the RADIUS server)
WEP-3ax(config):/interface/wlan1-vap0/vap/radius# save (save configuration)
```

6.3.6 Configuration of VAP with Captive Portal

Commands for configuring portal authorization with sending of accounting to the Radius server

```
WEP-3ax(root):/# configure
WEP-3ax(config):/# interface
WEP-3ax(config):/interface# wlan1-vap0
WEP-3ax(config):/interface/wlan1-vap0# common
WEP-3ax(config):/interface/wlan1-vap0/common# enabled true
WEP-3ax(config):/interface/wlan1-vap0/common# exit
WEP-3ax(config):/interface/wlan1-vap0# vap
WEP-3ax(config):/interface/wlan1-vap0/vap# vlan-id X (where X — VLAN-ID on VAP)
WEP-3ax(config):/interface/wlan1-vap0/vap# ap-security (go to the security settings block on the VAP)
WEP-3ax(config):/interface/wlan1-vap0/vap/ap-security# mode off (encryption mode off — without password)
WEP-3ax(config):/interface/wlan1-vap0/vap/ap-security# exit
WEP-3ax(config):/interface/wlan1-vap0/vap# ssid 'Portal_WEP-3ax' (change SSID name)
WEP-3ax(config):/interface/wlan1-vap0/vap# captive-portal
WEP-3ax(config):/interface/wlan1-vap0/vap/captive-portal# scenarios
WEP-3ax(config):/interface/wlan1-vap0/vap/captive-portal/scenarios# scenario-redirect
WEP-3ax(config):/interface/wlan1-vap0/vap/captive-portal/scenarios/scenario-redirect# redirect-url http://<IP>:<PORT>/eltex_portal/ (specify virtual portal URL)
WEP-3ax(config):/interface/wlan1-vap0/vap/captive-portal/scenarios/scenario-redirect# virtual-portal-name default (specify portal name. Default: default)
WEP-3ax(config):/interface/wlan1-vap0/vap/captive-portal/scenarios/scenario-redirect# exit
WEP-3ax(config):/interface/wlan1-vap0/vap/captive-portal/scenarios# exit
WEP-3ax(config):/interface/wlan1-vap0/vap/captive-portal# enabled true
WEP-3ax(config):/interface/wlan1-vap0/vap/captive-portal# exit
WEP-3ax(config):/interface/wlan1-vap0/vap# radius
WEP-3ax(config):/interface/wlan1-vap0/vap/radius# domain root (where root — user domain)
WEP-3ax(config):/interface/wlan1-vap0/vap/radius# acct-enable true (enable the sending of "Accounting" messages to the RADIUS server. Default: false)
WEP-3ax(config):/interface/wlan1-vap0/vap/radius# acct-address X.X.X.X (where X.X.X.X — IP address of the RADIUS server used for accounting)
WEP-3ax(config):/interface/wlan1-vap0/vap/radius# acct-password secret (where secret — password for RADIUS server used for accounting)
WEP-3ax(config):/interface/wlan1-vap0/vap/radius# acct-periodic true (enable a periodic sending of "Accounting" messages to the RADIUS server. Default: false)
WEP-3ax(config):/interface/wlan1-vap0/vap/radius# acct-interval 600 (interval of sending "Accounting" messages to the RADIUS server)
WEP-3ax(config):/interface/wlan1-vap0/vap/radius# save (save configuration)
```

6.3.7 Configuration of VAP with RADIUS MAC authorization

Commands for configuring RADIUS MAC authorization

```
WEP-3ax(root):/# configure
WEP-3ax(config):/# interface
WEP-3ax(config):/interface# wlan1-vap0
WEP-3ax(config):/interface/wlan1-vap0# vap
WEP-3ax(config):/interface/wlan1-vap0/vap# acl
WEP-3ax(config):/interface/wlan1-vap0/vap/acl# mode radius (select an authorization mode via RADIUS server. Default: off)
WEP-3ax(config):/interface/wlan1-vap0/vap/acl# policy allow (allow: access is allowed to those approved by the RADIUS server; deny: access is denied to those approved by the RADIUS server. Default: allow)
WEP-3ax(config):/interface/wlan1-vap0/vap/acl# exit
WEP-3ax(config):/interface/wlan1-vap0/vap# radius
WEP-3ax(config):/interface/wlan1-vap0/vap/radius# domain root (where root — user domain)
WEP-3ax(config):/interface/wlan1-vap0/vap/radius# auth-address X.X.X.X (where X.X.X.X – IP address of RADIUS server)
WEP-3ax(config):/interface/wlan1-vap0/vap/radius# auth-port X (where X — port of RADIUS server, used for authentication and authorization. Default: 1812)
WEP-3ax(config):/interface/wlan1-vap0/vap/radius# auth-password secret (where secret — password for RADIUS server, used for authentication and authorization)
WEP-3ax(config):/interface/wlan1-vap0/vap/radius# acct-enable true (enable sending of "Accounting" messages to the RADIUS server. Default: false)
WEP-3ax(config):/interface/wlan1-vap0/vap/radius# acct-address X.X.X.X (where X.X.X.X — IP address of RADIUS server, used for accounting)
WEP-3ax(config):/interface/wlan1-vap0/vap/radius# acct-password secret (where secret — password for RADIUS server, used for accounting)
WEP-3ax(config):/interface/wlan1-vap0/vap/radius# acct-periodic true (enable a periodic sending of "Accounting" messages to the RADIUS server. Default: false)
WEP-3ax(config):/interface/wlan1-vap0/vap/radius# acct-interval 600 (interval of sending "Accounting" messages to the RADIUS server)
WEP-3ax(config):/interface/wlan1-vap0/vap/radius# save (save configuration)
```

6.3.8 Configuration of backup RADIUS server on VAP

Commands for configuring a backup RADIUS server on VAP

```
WEP-3ax(root):/# configure
WEP-3ax(config):/# interface
WEP-3ax(config):/interface# wlan1-vap0
WEP-3ax(config):/interface/wlan1-vap0# vap
WEP-3ax(config):/interface/wlan1-vap0/vap# radius (configuring primary RADIUS server)
WEP-3ax(config):/interface/wlan1-vap0/vap/radius# backup (configuring a backup RADIUS server)
WEP-3ax(config):/interface/wlan1-vap0/vap/radius/backup# add <Domain name/IP address of backup RADIUS server in the configuration> (creating a configuration section for a backup RADIUS server. Maximum number: 4)
WEP-3ax(config):/interface/wlan1-vap0/vap/radius/backup# X.X.X.X (where X.X.X.X — domain name/IP address of a backup RADIUS server in the configuration)
WEP-3ax(config):/interface/wlan1-vap0/vap/radius/backup/X.X.X.X# auth-address X.X.X.X (where X.X.X.X — IP address of RADIUS server)
WEP-3ax(config):/interface/wlan1-vap0/vap/radius/backup/X.X.X.X# auth-port X (where X — port of RADIUS server, used for authentication and authorization. Default: 1812)
WEP-3ax(config):/interface/wlan1-vap0/vap/radius/backup/X.X.X.X# auth-password secret (where secret — password for RADIUS server, used for authentication and authorization)
WEP-3ax(config):/interface/wlan1-vap0/vap/radius/backup/X.X.X.X# acct-address X.X.X.X (where X.X.X.X — IP address of RADIUS server, used for accounting)
WEP-3ax(config):/interface/wlan1-vap0/vap/radius/backup/X.X.X.X# acct-port X (where X — port of RADIUS server, used for accounting. Default: 1813)
WEP-3ax(config):/interface/wlan1-vap0/vap/radius/backup/X.X.X.X# acct-password secret (where secret — password for RADIUS server, used for accounting)
WEP-3ax(config):/interface/wlan1-vap0/vap/radius/backup/X.X.X.X# save (save configuration)
```

6.3.9 Advanced VAP settings

Assignment of VLAN-ID to VAP

```
WEP-3ax(config):/interface/wlan1-vap0/vap# vlan-id X (where X — VLAN-ID number on VAP)
```

Enabling VLAN trunk on VAP

```
WEP-3ax(config):/interface/wlan1-vap0/vap# vlan-trunk true (enable VLAN Trunk on VAP. To disable, enter false)
```

Enabling General VLAN on VAP

```
WEP-3ax(config):/interface/wlan1-vap0/vap# general-vlan-mode true (enable General VLAN on SSID. To disable, enter false)
WEP-3ax(config):/interface/wlan1-vap0/vap# general-vlan-id X (where X — General VLAN number)
```

Selecting the priority mode

WEP-3ax(config):/interface/wlan1-vap0/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-3ax(config):/interface/wlan1-vap0/vap/ap-security# **mfp required** (enable management frame protection. required — MFP support is required from the client, clients without MFP will not be able to connect. capable — compatible with MFP, clients without MFP support can connect. To disable, enter **off**)

Enabling hidden SSID

WEP-3ax(config):/interface/wlan1-vap0/vap# **hidden true** (enable hidden SSID. To disable, enter **false**)

Enabling Band Steer mode

WEP-3ax(config):/interface/wlan1-vap0/vap# **band-steer-mode true** (enable Band Steer mode. To disable, enter **false**)

Enabling client isolation on VAP

WEP-3ax(config):/interface/wlan1-vap0/vap# **station-isolation true** (enable traffic isolation between clients within a single VAP. To disable, enter **false**)

Enabling Minimal Signal and Roaming Signal

WEP-3ax(config):/interface/wlan1-vap0/vap# **check-signal-enable true** (enable the use of Minimal Signal functionality. To disable, enter **false**)
WEP-3ax(config):/interface/wlan1-vap0/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-3ax(config):/interface/wlan1-vap0/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-3ax(config):/interface/wlan1-vap0/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-3ax(config):/interface/wlan1-vap0/vap# **save** (save configuration)

Shaping configuration

Configuring the shaper in the direction from the clients (each individually) connected to this VAP to the AP:

```
WEP-3ax(config):/interface/wlan1-vap0/vap# shaper-per-sta-rx
WEP-3ax(config):/interface/wlan1-vap0/vap/shaper-per-sta-rx# value X (where X — maximum rate in Kbps)
WEP-3ax(config):/interface/wlan1-vap0/vap/shaper-per-sta-rx# mode kbps (enable shaper. To disable, enter off)
WEP-3ax(config):/interface/wlan1-vap0/vap/shaper-per-sta-rx# exit
WEP-3ax(config):/interface/wlan1-vap0/vap# save (save configuration)
```

Configuring the shaper in the direction from the AP to the clients (each individually) connected to this VAP:

```
WEP-3ax(config):/interface/wlan1-vap0/vap# shaper-per-sta-tx
WEP-3ax(config):/interface/wlan1-vap0/vap/shaper-per-sta-tx# value X (where X — maximum rate in Kbps)
WEP-3ax(config):/interface/wlan1-vap0/vap/shaper-per-sta-tx# mode kbps (enable shaper. To disable, enter off)
WEP-3ax(config):/interface/wlan1-vap0/vap/shaper-per-sta-tx# exit
WEP-3ax(config):/interface/wlan1-vap0/vap# save (save configuration)
```

Configuring the shaper in the direction from the clients (all) connected to this VAP to the AP:

```
WEP-3ax(config):/interface/wlan1-vap0/vap# shaper-per-vap-rx
WEP-3ax(config):/interface/wlan1-vap0/vap/shaper-per-vap-rx# value X (where X — maximum rate in Kbps)
WEP-3ax(config):/interface/wlan1-vap0/vap/shaper-per-vap-rx# mode kbps (enable shaper. To disable, enter off)
WEP-3ax(config):/interface/wlan1-vap0/vap/shaper-per-vap-rx# exit
WEP-3ax(config):/interface/wlan1-vap0/vap# save (save configuration)
```

Configuring the shaper in the direction from the AP to the clients (all) connected to this VAP:

```
WEP-3ax(config):/interface/wlan1-vap0/vap# shaper-per-vap-tx
WEP-3ax(config):/interface/wlan1-vap0/vap/shaper-per-vap-tx# value X (where X — maximum rate in Kbps)
WEP-3ax(config):/interface/wlan1-vap0/vap/shaper-per-vap-tx# mode kbps (enable shaper. To disable, enter off)
WEP-3ax(config):/interface/wlan1-vap0/vap/shaper-per-vap-tx# exit
WEP-3ax(config):/interface/wlan1-vap0/vap# save (save configuration)
```

802.11r configuration

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

802.11r roaming is only possible between VAPs with security modes: WPA2 Personal and WPA2 Enterprise. For instructions on configuring a VAP with different security modes, see section Configuration of VAP with WPA-Personal security mode.

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

Below is an example of how to configure 802.11r on two access points: AP1 and AP2.

802.11r configuration on AP1

```
WEP-3ax(config):/interface/wlan1-vap0/vap/ft-config# enabled false
WEP-3ax(config):/interface/wlan1-vap0/vap/ft-config# r1-key-holder-id E8:28:C1:FC:D6:80 (VAP MAC address. Displayed in the ifconfig command output)
WEP-3ax(config):/interface/wlan1-vap0/vap/ft-config# r0-key-holder-id 12345 (unique key for the given VAP, for example, a serial number)
WEP-3ax(config):/interface/wlan1-vap0/vap/ft-config# mobility-domain 100 (the domain should be the same on the remote VAPs)
WEP-3ax(config):/interface/wlan1-vap0/vap/ft-config# mac
WEP-3ax(config):/interface/wlan1-vap0/vap/ft-config/mac# add E4:5A:D4:E2:C4:B0 (MAC address of VAP interface on the remote access point — AP2. Maximum number: 256)
WEP-3ax(config):/interface/wlan1-vap0/vap/ft-config/mac# E4:5A:D4:E2:C4:B0
WEP-3ax(config):/interface/wlan1-vap0/vap/ft-config/mac/E4:5A:D4:E2:C4:B0# r0-kh-id 23456 (unique key of the remote VAP on AP2 – r0-key-holder-id)
WEP-3ax(config):/interface/wlan1-vap0/vap/ft-config/mac/E4:5A:D4:E2:C4:B0# r1-kh-id E4:5A:D4:E2:C4:B0 (MAC address of the remote VAP on AP2)
WEP-3ax(config):/interface/wlan1-vap0/vap/ft-config/mac/E4:5A:D4:E2:C4:B0# r0-kh-key 0102030405060708 (random key. It should not match r1-kh-key of AP1, but it should match r1-kh-key of the remote AP2)
WEP-3ax(config):/interface/wlan1-vap0/vap/ft-config/mac/E4:5A:D4:E2:C4:B0# r1-kh-key 0001020304050607 (random key. It should match r0-kh-key of AP1, but it should match r0-kh-key of the remote AP2)
WEP-3ax(config):/interface/wlan1-vap0/vap/ft-config/mac/E4:5A:D4:E2:C4:B0# exit
WEP-3ax(config):/interface/wlan1-vap0/vap/ft-config/mac# exit
WEP-3ax(config):/interface/wlan1-vap0/vap/ft-config# enabled true (enable access point operation using the 802.11r protocol)
WEP-3ax(config):/interface/wlan1-vap0/vap/ft-config# save (save configuration)
```

802.11r configuration on AP2

```
WEP-3ax(config):/interface/wlan1-vap0/vap/ft-config# enabled false
WEP-3ax(config):/interface/wlan1-vap0/vap/ft-config# r1-key-holder-id E4:5A:D4:E2:C4:B0 (VAP MAC address. Displayed in the ifconfig command output)
WEP-3ax(config):/interface/wlan1-vap0/vap/ft-config# r0-key-holder-id 23456 (unique key for the given VAP, for example, a serial number)
WEP-3ax(config):/interface/wlan1-vap0/vap/ft-config# mobility-domain 100 (the domain should be the same on the remote VAPs)
WEP-3ax(config):/interface/wlan1-vap0/vap/ft-config# mac
WEP-3ax(config):/interface/wlan1-vap0/vap/ft-config/mac# add E8:28:C1:FC:D6:80 (MAC address of VAP interface on the remote access point – AP1)
WEP-3ax(config):/interface/wlan1-vap0/vap/ft-config/mac# E8:28:C1:FC:D6:80
WEP-3ax(config):/interface/wlan1-vap0/vap/ft-config/mac/E8:28:C1:FC:D6:80# r0-kh-id 12345 (unique key for the remote VAP on the AP1 access point — r0-key-holder-id)
WEP-3ax(config):/interface/wlan1-vap0/vap/ft-config/mac/E8:28:C1:FC:D6:80# r1-kh-id E8:28:C1:FC:D6:80 (MAC address of the remote VAP of AP1)
WEP-3ax(config):/interface/wlan1-vap0/vap/ft-config/mac/E8:28:C1:FC:D6:80# r0-kh-key 0001020304050607 (random key. It should not match r1-kh-key of AP2, but it should match r1-kh-key of the remote AP1)
WEP-3ax(config):/interface/wlan1-vap0/vap/ft-config/mac/E8:28:C1:FC:D6:80# r1-kh-key 0102030405060708 (random key. It should not match r0-kh-key of AP2, but it should match r0-kh-key of the remote AP1)
WEP-3ax(config):/interface/wlan1-vap0/vap/ft-config/mac/E8:28:C1:FC:D6:80# exit
WEP-3ax(config):/interface/wlan1-vap0/vap/ft-config/mac# exit
WEP-3ax(config):/interface/wlan1-vap0/vap/ft-config# enabled true (enable access point operation using the 802.11r protocol)
WEP-3ax(config):/interface/wlan1-vap0/vap/ft-config# save (save configuration)
```

802.11r configuration via AirTune

The feature is supported starting from WEP-3ax firmware version 1.6.0, AirTune version 1.4.0.

For 802.11r auto-configuration on the access point via AirTune enable 802.11r functionality and interaction with the AirTune.
Below is an example of how to configure 802.11r via AirTune.

802.11r configuration via AirTune

```
WEP-3ax(config):/interface/wlan1-vap0/vap/ft-config# enabled true (enable access point operation using the 802.11r protocol)
WEP-3ax(config):/interface/wlan1-vap0/vap/ft-config# exit
WEP-3ax(config):/interface/wlan1-vap0/vap# exit
WEP-3ax(config):/interface# exit
WEP-3ax(config):/# airtune
WEP-3ax(config):/airtune# airtune_service_url ws://192.168.1.20:8099/apb/rrm (where 192.168.1.20 is an IP address of a server, on which the AirTune is installed)
WEP-3ax(config):/airtune# enabled true (enable interaction with the AirTune service)
WEP-3ax(config):/airtune# save (save configuration)
```

802.11k configuration

802.11k roaming can be organized between any networks (open/encrypted). If the access point is configured to work with the 802.11k protocol, then, when the client connects, the access point sends a list of "friendly" access points to which the client can switch while roaming. The list contains information about the MAC addresses of access points and the channels on which they operate.

Using 802.11k reduces the time it takes the client to find another network when roaming because the client does not have to scan for channels where there are no target access points available for switching.

This type of roaming is only available for client devices that support 802.11k.

Below is an example of how to configure 802.11k on an access point – making a list of "friendly" access points.

802.11k configuration

```
WEP-3ax(config):/interface/wlan1-vap0/vap/w80211kv-config# enabled false
WEP-3ax(config):/interface/wlan1-vap0/vap/w80211kv-config# mac
WEP-3ax(config):/interface/wlan1-vap0/vap/w80211kv-config/mac# add E8:28:C1:FC:D6:90 (where E8:28:C1:FC:D6:90 — MAC address of the "friendly" access point. Maximum number: 256)
WEP-3ax(config):/interface/wlan1-vap0/vap/w80211kv-config/mac# E8:28:C1:FC:D6:90
WEP-3ax(config):/interface/wlan1-vap0/vap/w80211kv-config/mac/E8:28:C1:FC:D6:90# channel 132 (where 132 — channel, on which the access point with E8:28:C1:FC:D6:90 MAC address is operating)
WEP-3ax(config):/interface/wlan1-vap0/vap/w80211kv-config/mac/E8:28:C1:FC:D6:90# exit
WEP-3ax(config):/interface/wlan1-vap0/vap/w80211kv-config/mac# add E8:28:C1:FC:D6:70 (where E8:28:C1:FC:D6:70 — MAC address of the "friendly" access point)
WEP-3ax(config):/interface/wlan1-vap0/vap/w80211kv-config/mac# E8:28:C1:FC:D6:70
WEP-3ax(config):/interface/wlan1-vap0/vap/w80211kv-config/mac/E8:28:C1:FC:D6:70# channel 36 (where 36 — channel, on which the access point with E8:28:C1:FC:D6:70 MAC address is operating)
WEP-3ax(config):/interface/wlan1-vap0/vap/w80211kv-config/mac/E8:28:C1:FC:D6:70# exit
WEP-3ax(config):/interface/wlan1-vap0/vap/w80211kv-config/mac# exit
WEP-3ax(config):/interface/wlan1-vap0/vap/w80211kv-config# enabled true (enable access point operation using the 802.11k protocol)
WEP-3ax(config):/interface/wlan1-vap0/vap/w80211kv-config# save (save configuration)
```

802.11k configuration via AirTune

The feature is supported starting from WEP-3ax firmware version 1.6.0, AirTune version 1.4.0.

For 802.11k auto-configuration on the access point via AirTune, enable 802.11k functionality on SSID and interaction with the AirTune.
Below is an example of how to configure 802.11k/v via AirTune.

802.11k configuration via AirTune

```
WEP-3ax(config):/interface/wlan1-vap1/vap/w80211kv-config# enabled true (enable 802.11k protocol support on the VAP)
WEP-3ax(config):/interface/wlan1-vap1/vap/w80211kv-config# exit
WEP-3ax(config):/interface/wlan1-vap1/vap# exit
WEP-3ax(config):/interface/wlan1-vap1# exit
WEP-3ax(config):/interface# exit
WEP-3ax(config):/# airtune
WEP-3ax(config):/airtune# airtune_service_url ws://192.168.1.20:8099/apb/rrm (where 192.168.1.20 is an IP address of the server, on which the AirTune service is installed)
WEP-3ax(config):/airtune# enabled true (enable interaction with the AirTune service)
WEP-3ax(config):/airtune# save (save configuration)
```

802.11v configuration

802.11v roaming can be organized between any networks (open/encrypted). If an access point is configured to work with 802.11v, then during its operation the device sends a special packet (BSS Transition) by the command of admin/controller (Airtune) to the client side recommending that the client roams. Whether or not the client device will follow the access point's recommendation is impossible to guarantee, because the decision to switch to another access point is ultimately made by the client side. In conjunction with the 802.11k standard, in a message with a recommendation to switch the client is also sent a list of recommended roaming access points, indicating on what channel each point works and what standard (IEEE 802.11n/ac/ax). Then the client analyzes the air and make a decision depending on the signal level, channel load, the configuration of the remote access point.

This type of roaming is only available for client devices that support 802.11v.

802.11v configuration

```
WEP-3ax(config):/interface/wlan1-vap0/vap/w80211kv-config# enabled true (enable the access point to operate using the 802.11k/v protocol)

WEP-3ax(config):/interface/wlan1-vap0/vap/w80211kv-config# save (save configuration)
```

Commands for client roaming via 802.11v protocol via driver

```
wl -i wlan1-vap4 wnm_bsstrans_req 7 150 84:ab:1a:c6:db:17 0 0 (sending a roaming recommendation message to a client with MAC address 84:ab:1a:c6:db:17 connected to wlan1-vap4. If the client does not switch to another access point within 15 seconds after sending this message, the access point will forcibly disconnect the client device from the wireless network)
wl -i wlan1 wnm_bsstrans_req 3 150 84:ab:1a:c6:db:17 5 0 (sending a roaming recommendation message to a client with MAC address 84:ab:1a:c6:db:17, connected to wlan1-vap0. Sending a message without forcing the client device to disconnect from the wireless network)
```

802.11v configuration via AirTune

This functionality is supported from the firmware version: WEP-3ax access point from version 1.12.0, Airtune service from 1.6.0.

To automatically configure 802.11v via the AirTune service on the access point, you should enable the 802.11k/v functionality on the SSID and interaction with AirTune; to do this, make the following settings:

802.11k configuration via AirTune

```
WEP-3ax(config):/interface/wlan1-vap1/vap/w80211kv-config# enabled true (enable 802.11k protocol support on a virtual access point)
WEP-3ax(config):/interface/wlan1-vap1/vap/w80211kv-config# exit
WEP-3ax(config):/interface/wlan1-vap1/vap# exit
WEP-3ax(config):/interface/wlan1-vap1# exit
WEP-3ax(config):/interface# exit
WEP-3ax(config):/# airtune
WEP-3ax(config):/airtune# airtune_service_url ws://192.168.1.20:8099/apb/rrm (where 192.168.1.20 — IP address of the server, on which the AirTune service is installed)
WEP-3ax(config):/airtune# enabled true (enable interaction with the AirTune service)
WEP-3ax(config):/airtune# save (save configuration)
```

Commands for client roaming using 802.11v protocol via CLI

```
deauth-client -i wlan1-vap4 -a c2:8c:5f:3f:ce:6e -t disassoc (sending a message with a forced roaming recommendation to a client with MAC address c2:8c:5f:3f:ce:6e connected to wlan1-vap4. If within 15 seconds after sending this message the client does not move to another access point from the received 802.11k list, this point will forcefully disconnect the client device from the wireless network)
```

6.4 Radio configuration

In Radio, automatic selection of the operating channel is used by default. To set the channel manually or to change the power, use the following commands:

Changing the radio channel, bandwidth and power of the radio interface

```
WEP-3ax(root):/# configure
WEP-3ax(config):/# interface
WEP-3ax(config):/interface# wlan0
WEP-3ax(config):/interface/wlan0# wlan
WEP-3ax(config):/interface/wlan0/wlan# radio
WEP-3ax(config):/interface/wlan0/wlan/radio# channel X (where X — the number of the static channel on which the point will operate)
WEP-3ax(config):/interface/wlan0/wlan/radio# auto-channel false (disable automatic channel selection functionality. To enable, enter true)
WEP-3ax(config):/interface/wlan0/wlan/radio# use-limit-channels false (disable Use Limit Channels. To enable, enter true)
WEP-3ax(config):/interface/wlan0/wlan/radio# bandwidth X (where X — channel bandwidth)
WEP-3ax(config):/interface/wlan0/wlan/radio# tx-power X (where X — power level in dBm. The parameter may take values: for Radio 2.4 GHz (wlan0): 6–16 dBm; for Radio 5 GHz (wlan1): 10–19 dBm)
WEP-3ax(config):/interface/wlan0/wlan/radio# save (save configuration)
```

Lists of available channels

The following channels are available to be selected for Radio 2.4 GHz:

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

The following channels are available to be selected for Radio 5 GHz:

- with 20 MHz channel width: 36, 40, 44, 48, 52, 56, 60, 64, 132, 136, 140, 144, 149, 153, 157, 161, 165.
- with 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.
- with 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

Changing the radio interface operation mode
WEP-3ax(config):/interface/wlan0/wlan/radio# **work-mode X** (where X — radio interface operation mode according to the IEEE 802.11 standard. Possible values: for Radio 2.4 GHz (wlan0): **bgn**, **bgnax**, **ax**; for Radio 5 GHz (wlan1): **anac**, **anacax**, **ax**)

Limit channel list configuration
WEP-3ax(config):/interface/wlan0/wlan/radio# **use-limit-channels true** (enable the use of a limited list of channels in the auto channel selection operation. To disable, enter **false**) WEP-3ax(config):/interface/wlan0/wlan/radio# **limit-channels '1 6 11'** (where *1 6 11* — channels of the band in which the configurable radio interface can operate)

Changing the primary channel
WEP-3ax(config):/interface/wlan0/wlan/radio# **control-sideband lower** (parameter may take the following values: lower, upper. Default: **lower**)

Switching on the use of Short Guard Interval
WEP-3ax(config):/interface/wlan0/wlan/radio# **sgi true** (enable the use of a short guard interval for data transfer – 400 ns instead of 800 ns. To disable, enter **false**)

Enabling STBC
WEP-3ax(config):/interface/wlan0/wlan/radio# **stbc true** (enable the Space-Time Block Coding (STBC) method, aimed at improving the reliability of data transmission. To disable, enter **false**)

Enabling aggregation
WEP-3ax(config):/interface/wlan0/wlan/radio# **aggregation true** (enable aggregation on Radio — support for AMPDU/AMSDU. To disable, enter **false**)

Enabling the short preamble
WEP-3ax(config):/interface/wlan0/wlan/radio# **short-preamble true** (enable the short packet preamble. To disable, enter **false**)

Enabling the Wi-Fi Multimedia (WMM)

WEP-3ax(config):/interface/wlan0/wlan/radio# **wmm true** (enable the support for WMM (Wi-Fi Multimedia). To disable, enter **false**)

DFS mechanism configuration

Only Radio 5 GHz (wlan1) is configured

WEP-3ax(config):/interface/wlan1/wlan/radio# **dfs X** (where X — DFS mechanism operation mode. May take values: **forced** — mechanism is disabled, DFS channels are available for selection; **auto** — mechanism is enabled; **disabled** — mechanism is disabled, DFS channels are unavailable for selection)

Enabling the automatic channel width change mode

WEP-3ax(config):/interface/wlan0/wlan/radio# **obss-coex true** (enable automatic change of channel width from 40 MHz to 20 MHz with congested radio environment. To disable, enter **false**)

Configuring BSS coloring

WEP-3ax(config):/interface/wlan1/wlan/radio/bss-coloring# **enable true** (enable the BSS Coloring mechanism. To disable, enter **false**. Default: **true**)
WEP-3ax(config):/interface/wlan1/wlan/radio/bss-coloring#**bss-color X** (where X — color number. The defined value of BSS Color will be announced in all beacon and probe packets from the access point, if it works with 802.11ax support. The parameter can accept the values: **1–63**. Default: **0** (autoselect))

6.5 DHCP option 82 configuration

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

Operation mode of DHCP snooping:

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

Changing the operation mode of DHCP option 82

```
WEP-3ax(root):/# configure
WEP-3ax(config):/# interface
WEP-3ax(config):/interface# wlan0 (configuration will be done for Radio 2.4 GHz. To configure option 82 on Radio 5 GHz – enter wlan1)
WEP-3ax(config):/interface/wlan0# common
WEP-3ax(config):/interface/wlan0/common# dhcp-snooping
WEP-3ax(config):/interface/wlan0/common/dhcp-snooping# dhcp-snooping-mode replace (set DHCP snooping to replace mode)
```

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

Configuring Option 82 parameters

```
WEP-3ax(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-3ax(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-3ax(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-3ax(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-3ax(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 WDS configuration

When configuring a WDS connection, it is necessary to select the same channel and channel width in the radio interface settings on the the devices that will be connected via WDS. Auto-channel should be disabled and the DFS option should be set to "off" or "forced".
More detailed information about configuring the radio interface via the command line can be found in the Radio Settings section.

When configuring a WDS connection on the Radio 2.4/Radio 5 GHz it is necessary to enable VAP0 on the Radio 2.4/Radio 5 GHz. The encryption modes on VAP and WDS interfaces should be the same. More detailed information about configuring VAPs can be found in the Virtual Wi-Fi access points (VAPs) configuration section.

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

Configuring WDS

```
WEP-3ax(root):/# configure
WEP-3ax(config):/# interface
WEP-3ax(config):/interface# wlan1-wds0 (WDS link selection. Possible values for Radio 2.4 GHz: wlan0–wds0 – wlan0–wds7, for Radio 5 GHz: wlan1–wds0 – wlan1–wds7)
WEP-3ax(config):/interface/wlan1-wds0# wds
WEP-3ax(config):/interface/wlan1-wds0/wds# mac-addr XX:XX:XX:XX:XX:XX (MAC address of the remote access point radio interface, that can be found by entering the monitoring radio-interface command on the remote acess point)
WEP-3ax(config):/interface/wlan1-wds0/wds# ssid WDS (SSID name for creating an encrypted WDS)
WEP-3ax(config):/interface/wlan1-wds0/wds# security-mode WPA2 (encryption mode. Possible values: WPA2, off — without password)
WEP-3ax(config):/interface/wlan1-wds0/wds# key-wpa password (WPA key. The key length is from 8 to 63 characters)
WEP-3ax(config):/interface/wlan1-wds0/wds# exit
WEP-3ax(config):/interface/wlan1-wds0# common
WEP-3ax(config):/interface/wlan1-wds0/common# enabled true (enable WDS. To disable, enter false)
WEP-3ax(config):/interface/wlan1-wds0/common# save (save configuration)
```

The **remote access point** is configured in the same way.

6.7 System settings

6.7.1 Device firmware upgrade

Device firmware upgrade via TFTP

```
WEP-3ax(root):/# firmware upload tftp <IP address of TFTP server> <Firmware file name> (example: firmware upload tftp 192.168.1.100 WEP-3ax-1.12.0_build_105.tar.gz)
WEP-3ax(root):/# firmware upgrade
```

Device firmware upgrade via HTTP

```
WEP-3ax(root):/# firmware upload http <firmware file URL> (example: firmware upload http http://192.168.1.100:8080/files/WEP-3ax-1.12.0_build_105.tar.gz)
WEP-3ax(root):/# firmware upgrade
```

Switching to a backup version of the access point firmware

```
WEP-3ax(root):/# firmware switch
```

6.7.2 Device configuration management

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

```
WEP-3ax(root):/# manage-config reset-to-default
```

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

```
WEP-3ax(root):/# manage-config reset-to-default-without-management
```

Download the device configuration file to TFTP server

```
WEP-3ax(root):/# manage-config download tftp <IP address of TFTP server> (example: manage-config download tftp 192.168.1.100)
```

Upload the configuration file from TFTP server to the device

```
WEP-3ax(root):/# manage-config upload tftp <IP address of TFTP server> <configuration file name> (example: manage-config upload tftp 192.168.1.100 config.json)
WEP-3ax(root):/# manage-config apply (apply configuration on access point)
```

6.7.3 Device reboot

The command for rebooting the device

```
WEP-3ax(root):/# reboot
```

6.7.4 Setting the date and time

Commands to configure NTP server time synchronization

```
WEP-3ax(root):/# configure
WEP-3ax(config):/# date-time
WEP-3ax(config):/date-time# mode ntp (enable NTP mode)
WEP-3ax(config):/date-time# ntp
WEP-3ax(config):/date-time/ntp# server <IP address of NTP server> (specify the primary NTP server address)
WEP-3ax(config):/date-time/ntp# alt-servers (specify alternative NTP servers)
WEP-3ax(config):/date-time/ntp/alt-servers# add <Domain name/IP address of NTP server in configuration> (create a configuration section for an alternative NTP server. Maximum number: 8. To delete, use the del command)
WEP-3ax(config):/date-time/ntp/alt-servers# exit
WEP-3ax(config):/date-time/ntp# exit
WEP-3ax(config):/date-time# common
WEP-3ax(config):/date-time/common# timezone 'Asia/Novosibirsk (Novosibirsk)' (set the time zone)
WEP-3ax(config):/date-time/common# save (save configuration)
```

6.7.5 Advanced system settings

Enabling global isolation

```
WEP-3ax(root):/# configure
WEP-3ax(config):/# system
WEP-3ax(config):/system# global-station-isolation true (enable global isolation of traffic between clients of different VAPs and different radio interfaces. To disable, enter false)
WEP-3ax(config):/system# save (save configuration)
```

Changing hostname

```
WEP-3ax(root):/# configure
WEP-3ax(config):/# system
WEP-3ax(config):/system# hostname WEP-3ax_room2 (where WEP-3ax_room2 is a new hostname. The parameter can contain from 1 to 63 characters: Latin uppercase and lowercase letters, numbers, hyphen "-" (the hyphen can not be the last character in the name). Default: WEP-3ax)
WEP-3ax(config):/system# save (save configuration)
```

Changing geographical domain

```
WEP-3ax(root):/# configure
WEP-3ax(config):/# system
WEP-3ax(config):/system# ap-location ap.test.root (where ap.test.root is the domain of the device tree node of the EMS management system in which the access point is located. Default: root)
WEP-3ax(config):/system# save (save configuration)
```

Changing password

```
WEP-3ax(root):/# configure
WEP-3ax(config):/# authentication
WEP-3ax(config):/authentication# admin-password newpassword (where newpassword is a new password to log in to the access point. Default: password)
WEP-3ax(config):/authentication# save (save configuration)
```

Changing Radius NAS-ID

```
WEP-3ax(root):/# configure
WEP-3ax(config):/# system
WEP-3ax(config):/system # nas-id Lenina_1.Novovsibirsk.root (where Lenina_1.Novovsibirsk.root is an identifier of this access point. The parameter is dedicated to identify the device on the RADIUS server in case RADIUS expects a value other than the MAC address. Default: MAC address of AP)
WEP-3ax(config):/system # save (save configuration)
```

Configuring LLDP

```
WEP-3ax(root):/# configure
WEP-3ax(config):/# lldp
WEP-3ax(config):/lldp# enabled true (enable LLDP functionality. To disable, enter false. Default: true)
WEP-3ax(config):/lldp# tx-interval 60 (change the period of sending LLDP messages. Default: 30)
WEP-3ax(config):/lldp# system-name WEP-3ax_reserv (where WEP-3ax_reserv is a new device name. Default: WEP-3ax)
WEP-3ax(config):/lldp# save (save configuration)
```

6.8 APB service configuration

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

Commands for configuring APB service

```
WEP-3ax(root):/# configure
WEP-3ax(config):/# captive-portal
WEP-3ax(config):/captive-portal# apbd
WEP-3ax(config):/captive-portal/apbd# roam_service_url <APB service address>
(example: roam_service_url ws://192.168.1.100:8090/apb/broadcast)
WEP-3ax(config):/captive-portal/apbd# enabled true (enable APB service. To disable, enter false)
WEP-3ax(config):/captive-portal/apbd# save (save configuration)
```

6.9 Configuration of tcpdump utility

The tcpdump utility is designed to analyze and intercept network traffic. This utility allows to intercept traffic from various access point interfaces for further analysis, to change recording parameters (time limits, file size), as well as to send the finished file via TFTP to the server.

6.9.1 Commands for using tcpdump utility

To take a dump from the Ethernet interface of the access point, use the **eth1** interface.
To take a dump from radio interfaces:
radiotap0 – the interface corresponds to 2.4 GHz band (wlan0);
radiotap1 – the interface corresponds to 5 GHz band (wlan1).

Configuring tcpdump utility

```
WEP-3ax(root):/# configure
WEP-3ax(config):/# tcpdump
WEP-3ax(config):/tcpdump# interface radiotap0 (specify interface, for example, radiotap0)
WEP-3ax(config):/tcpdump# time-limit 600 (limit for dumping by time in seconds, for example, 600s=10min)
WEP-3ax(config):/tcpdump# file-size-limit 10 (imit for dumping by file size in MB)
WEP-3ax(config):/tcpdump# mac-filter e0:d9:e3:4e:60:a1 (filtering by MAC address. The parameter is not obligatory)
WEP-3ax(config):/tcpdump# tftp-server-ip: 192.168.1.1 (address of TFTP server, where it is planned to upload a file)
WEP-3ax(config):/tcpdump# tftp-file-name: AP1_dump.pcap (name of uploading file)
WEP-3ax(config):/tcpdump# save (save configuration)
```

Using tcpdump utility

```
WEP-3ax(config):/tcpdump# exit
WEP-3ax(config):/# monitoring tcpdump-start (command to enbale a file recording)
WEP-3ax(config):/# monitoring tcpdump-status (view the current operating status of the utility)
WEP-3ax(config):/# monitoring tcpdump-stop (command to stop recording a file)
WEP-3ax(config):/# monitoring tcpdump-tftp-send (command to send a file to the server via TFTP
protocol)
```

6.10 Configuration of Radar mode

The functionality is intended to collect information about client devices within the coverage area of the access point and transmit data to the collector server.

6.10.1 Configuring a radar with sending data via the HTTP protocol

Command for configuring Radar functionality (HTTP/HTTPS)

```
WEP-3ax(root):/# configure
WEP-3ax(config):/#radar
WEP-3ax(config):/radar# enabled true (enable radar functionality. Default: false)
WEP-3ax(config):/radar# url http://host:port/service (specify a URL link to the service that will receive
data from the access point in JSON format. Data transmission is possible via HTTP/HTTPS)
WEP-3ax(config):/radar# scan-interface all (interface on which scanning will work. Possible
values: wlan0 — 2.4 GHz interface, wlan1 — 5 GHz interface, all — 2.4 GHz and 5 GHz simultaneously)
WEP-3ax(config):/radar# send-interval 1 (interval for sending data to the collector. Default: 5 seconds)
WEP-3ax(config):/radar# mac-source "probe data" (select the type of data collected over the air, possible
values probe — probe request only, assoc — Assoc only, data — data only, all — all packet types)
WEP-3ax(config):/radar# scan-channel-timeout 1000 (time allocated for scanning one channel. Default:
200 ms)
WEP-3ax(config):/radar# scan-limit-channels-2g "1 6 11" (channel for scanning in the 2.4 GHz band.
Empty value — all available channels are scanned)
WEP-3ax(config):/radar# scan-limit-channels-5g "36 40 44 48" (channel for scanning in the 5 GHz band.
Empty value — all available channels are scanned)
WEP-3ax(config):/radar# save (save configuration)
```

6.10.2 Configuring a radar with sending data via the MQTT protocol

Commands for configuring Radar functionality (MQTT)

```
WEP-3ax(root):/# configure
WEP-3ax(config):/#radar
WEP-3ax(config):/radar# url mqtt://host:port/service (specify a URL link to the service that will receive data from the access point via the MQTT protocol. Example: mqtt://rtls.eltex.nsk.ru:1883/)
WEP-3ax(config):/radar# mqtt-username eltex (username: required for authorization on the collector service)
WEP-3ax(config):/radar# mqtt-password Password (password: required for authorization on the collector service
WEP-3ax(config):/radar# mqtt-topic input_mqtt_topic (indicate the URL identifier of entities in the exchange between the AP and the collector via the MQTT protocol)
WEP-3ax(config):/radar# scan-mode passive (radar operating mode, where active — the access point scans the air only and does not provide service to clients; passive — the access point provides service to clients, does not scan the air, transmits data to connected clients)
WEP-3ax(config):/radar# scan-interface all (interface on which scanning will work. Possible values: wlan0 — 2.4 GHz interface, wlan1 — 5 GHz interface, all — 2.4 GHz and 5 GHz simultaneously)
WEP-3ax(config):/radar# send-interval 1 (interval for sending data to the collector. Default: 5 seconds)
WEP-3ax(config):/radar# mac-source "probe data" (select the type of data collected over the air. Possible values: probe — probe request only, assoc — Assoc only, data — data only, all — all packet types)
WEP-3ax(config):/radar# scan-channel-timeout 1000 (time allocated for scanning one channel. Default: 200 ms)
WEP-3ax(config):/radar# scan-limit-channels-2g "1 6 11" (channel for scanning in the 2.4 GHz band. Empty value — all available channels are scanned)
WEP-3ax(config):/radar# scan-limit-channels-5g "36 40 44 48" (channel for scanning in the 5 GHz band. Empty value — all available channels are scanned)
WEP-3ax(config):/radar# scan-min-signal -80 (signal level threshold. If the access point sees a client with a level lower than the specified one, the client's MAC address is not sent to the collector and the client is not considered discovered. Default: 0, functionality is disabled)
WEP-3ax(config):/radar# enabled true (enable radar functionality. To disable, enter false)
WEP-3ax(config):/radar# save (save configuration)
```

6.11 Configuration of IGMP

In the **igmp-config** section the user can configure the following parameters: **enabled, query-interval, querycount, query-resp-interval**. Default: **enabled true**.

Commands for configuring IGMP parameters

```
WEP-3ax(root):/# configure
WEP-3ax(config):/# igmp-config
WEP-3ax(config):/igmp-config# enabled true (enable multicast traffic. To disable, enter false)
WEP-3ax(config):/igmp-config# query-interval X (where X — interval for sending IGMP General Query messages in seconds. Accepted values: from 30 to 18000 seconds. Default: 125)
WEP-3ax(config):/igmp-config# query-count X (where X — value of the expected number of packets lost on the channel (QRV filed in the IGMP request). Possible values: from 1 to 7. Default: 7)
WEP-3ax(config):/igmp-config# query-resp-interval X (where X — maximum response time to an IGMP request. Possible values: from 50 to 200 tenths of a second. Default: 100)
WEP-3ax(config):/igmp-config# save (save configuration)
```

6.12 Monitoring

6.12.1 Wi-Fi Clients

WEP-3ax(root):/# **monitoring associated-clients**

```
 index                     | 0
 hw-addr                   | ac:c4:13:1c:aa:aa
 hw-addr                   | 62:33:e6:73:bf:ec
 authenticated             | yes
 associated                | yes
 authorized                | yes
 ip-addr                   | 192.168.40.248
 hostname                  | Pixel-6
 identity                  | ivanov.ivan
 domain                    | enterprise.service.root
 rssi-1                    | -64
 rssi-2                    | -66
 rssi-3                    | 0
 rssi-4                    | 0
 noise-1                   | -94
 noise-2                   | -95
 noise-3                   | 0
 noise-4                   | 0
 snr-1                     | 30
 snr-2                     | 29
 snr-3                     | 0
 snr-4                     | 0
 tx-rate                   | HE NSS2-MCS11 2xLTF GI 0.8us 286.8
 rx-rate                   | HE NSS2-MCS9 2xLTF GI 0.8us 229.4
 actual-tx-rate            | 5
 actual-rx-rate            | 4
 tx-fails                  | 1
 tx-retry-count            | 0
 rx-retry-count            | 328
 tx-bw                     | 20
 rx-bw                     | 20
 tx-period-retry           | 0
 link-capacity             | 100%
 link-quality              | 100%
 link-quality-common       | 100%
 uptime                    | 00:13:46
 interface                 | wlan1-vap2
 ssid                      | Eltex-Test
 using-802.11r             | yes
 using-802.11k             | no
 using-802.11v             | no
 wireless-mode             | ax
 name                      | wlan1-vap2:sta-0

  Rate                  Transmitted            Received
----------------------------------------------------------------------
 Total Packets:       | 50807                | 2527                 |
 TX success:          | 100                  |                      |
 Total Bytes:         | 20608509             | 491365               |
 Data Packets:        | 50803                | 2522                 |
 Data Bytes:          | 20608377             | 490906               |
 Mgmt Packets:        | 4                    | 5                    |
 Mgmt Bytes:          | 132                  | 459                  |
 Dropped Packets:     | 0                    | 772                  |
 Dropped Bytes:       | 0                    | 18495                |
 Lost Packets:        | 1                    |                      |
---------------------------------------------------------------------

 Rate                  Transmitted            Received
---------------------------------------------------------------------
 ofdm6                | 0              |   0%|            829 |  35%|
 he-nss1-mcs0         | 0              |   0%|              1 |   0%|
 he-nss1-mcs8         | 0              |   0%|              7 |   0%|
 he-nss1-mcs11        | 0              |   0%|              2 |   0%|
 he-nss2-mcs0         | 0              |   0%|              1 |   0%|
 he-nss2-mcs1         | 0              |   0%|              1 |   0%|
 he-nss2-mcs2         | 0              |   0%|              4 |   0%|
 he-nss2-mcs3         | 0              |   0%|             12 |   0%|
 he-nss2-mcs4         | 0              |   0%|            161 |   6%|
 he-nss2-mcs5         | 0              |   0%|             92 |   3%|
 he-nss2-mcs6         | 19             |   0%|            182 |   7%|
 he-nss2-mcs7         | 165            |   1%|            196 |   8%|
 he-nss2-mcs8         | 228            |   2%|            213 |   9%|
 he-nss2-mcs9         | 553            |   4%|            227 |   9%|
 he-nss2-mcs10        | 92             |   0%|            254 |  10%|
 he-nss2-mcs11        | 10335          |  90%|            176 |   7%|
---------------------------------------------------------------------
```

6.12.2 Device information

WEP-3ax(root):/# **monitoring information**

```
 system-time                  | 08:24:03 04.04.2024
 uptime                       | 00:00:31
 hostname                     | WEP-3ax
 software-version             | 1.12.0 build 93
 uboot-version                | 1.12.0 build 93
 secondary-software-version   | 1.12.0 build 93
 boot-version                 | 1.12.0 build 93
 memory-usage                 | 30
 memory-free                  | 702
 memory-used                  | 304
 memory-total                 | 1006
 cpu-load                     | 2.3
 cpu-average                  | 0.31
 cpu-thermal                  | 31
 is-default-config            | true
 board-type                   | WEP-3ax
 hw-platform                  | WEP-3ax
 factory-mac                  | 68:13:E2:xx:xx:xx
 factory-serial-number        | WP42007273
 hw-revision                  | 4v1
 last-reboot-reason           | unknown
```

6.12.3 Network information

WEP-3ax(root):/# **monitoring wan-status**

```
Common information:

 interface                   | br0
 mac                         | 68:13:e2:xx:xx:xx
 rx-bytes                    | 823420
 rx-packets                  | 2068
 tx-bytes                    | 2126556
 tx-packets                  | 2114


IPv4 information:

 protocol                    | dhcp
 ip-address                  | 192.168.1.15
 netmask                     | 255.255.255.0
 gateway                     | 192.168.1.1
 DNS-1                       | 192.168.1.253
 DNS-2                       | 172.16.7.40
```

WEP-3ax(root):/# **monitoring ethernet**

```
    link: up
    speed: 1000
    duplex: enabled
    rx-bytes: 82842279
    rx-packets: 1124216
    tx-bytes: 2283061
    tx-packets: 8875
```

WEP-3ax(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-3ax(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-3ax(root):/# **monitoring lldp**

```
Port     Device ID          Port ID          System Name        Capabilities   TTL
------   -----------------  --------------   ----------------   ------------   -----
eth0     e0:d9:e3:eb:66:80  gi1/0/10                                           120
```

6.12.4 Wireless interfaces

WEP-3ax(root):/# **monitoring radio**

```
     wlan0:
      name: wlan0
      rfid: 0
      hwaddr: 68:13:E2:xx:xx:xx
      thermal: 30
      status: on
      channel: 11
      bandwidth: 20
      frequency: 2462
      power: 16.0
      mode: bgnax

   wlan1:
      name: wlan1
      rfid: 1
      hwaddr: 68:13:E2:xx:xx:xx
      thermal: 36
      status: on
      channel: 40
      bandwidth: 20
      frequency: 5200
      power: 19.0
      mode: anacax
```

6.12.5 Event log

WEP-3ax(root):/# **monitoring events**

```
Feb 25 05:00:19 WEP-3ax syslog.info syslogd: started: BusyBox v1.30.1

Feb 25 05:00:20 WEP-3ax daemon.info networkd[907]: Networkd started

Feb 25 05:00:26 WEP-3ax daemon.info networkd[907]: DHCP-client: Interface br0 obtained
lease on 192.168.1.15.

Feb 25 05:14:59 WEP-3ax auth.info login[1738]: root login on 'pts/0'

Feb 25 05:57:22 WEP-3ax daemon.info networkd[907]: DHCP-client: Interface br0 renew lease
on 192.168.1.15.

Feb 25 06:22:55 WEP-3ax daemon.info configd[651]: The AP startup configuration was updated
successfully.
```

To clear the event log enter the **monitoring clear-events** command.

6.12.6 Scan environment

Please note, while scanning the air, the radio interface of the device will be disabled, which will result in the inability to transmit data to Wi-Fi clients during the scan.

WEP-3ax(root):/# **monitoring scan-wifi**

```
SSID              |Mode |Security|MAC               |Channel|RSSI, dBm|Bandwidth, MHz
------------------|-----|--------|------------------|-------|---------|--------------
HOT_SSID          |     |off     |e8:28:c1:da:cf:f2 |1      |-40      |20
EltexWiFi         |     |off     |e8:28:c1:fc:d2:c0 |1      |-63      |20
Eltex-Local       |     |wpa/wpa2|e8:28:c1:fc:d6:40 |1      |-30      |20
test_wpa          |     |wpa/wpa2|a8:f9:4b:b0:22:a3 |1      |-46      |20
EltexWiFi2.4G     |     |wpa/wpa2|e2:d9:e3:98:36:bd |5      |-62      |20
Nikitenko_2.4     |     |off     |aa:f9:4b:2d:04:f3 |11     |-65      |20
Eltex-Local       |     |wpa/wpa2|e8:28:c1:da:cf:01 |11     |-56      |20
BRAS-Guest        |     |off     |e8:28:c1:da:cf:06 |48     |-66      |20
WEP-3ax_OWE       |     |owe     |E0:D9:E3:49:cf:15 |44     |-17      |20
Eltex-Guest       |     |off     |e8:28:c1:da:cf:07 |48     |-68      |20
Eltex-Local       |     |wpa/wpa2|e8:28:c1:da:cf:08 |48     |-68      |20
WEP-2L_open       |     |off     |e8:28:c1:da:cf:09 |48     |-68      |20
EltexWiFi5G       |     |wpa2    |e2:d9:e3:9f:6b:8c |153    |-76      |80
!wep3ax_test5     |     |off     |e8:28:c1:fc:74:30 |157    |-81      |80
test_1            |     |off     |a8:f9:4b:17:02:33 |161    |-71      |20
...
```

6.12.7 Spectrum analyzer

The WEP-3ax has the possibility to run the spectrum analyzer on radio interfaces wlan0 (2.4 GHz) and wlan1 (5 GHz). Below are the commands to start and monitor the spectrum analyzer.

Note that running the spectrum analyzer on the radio interface (Radio 2.4 GHz or Radio 5 GHz) will put it into scanning mode, which will disable all Wi-Fi clients connected to that radio interface.

The spectrum analyzer on the radio interface only works on the channels that are reflected in the "limit-channels" parameter. For example, if the wlan0 channel list contains channels '1 6 11', the spectrum analysis will only be performed for channels 1, 6 and 11.
To analyze all channels of the band on which the radio interface operates, change the value of use-limit-channels in the radio interface settings to false. After receiving the results of the spectrum analyzer, return the value of use-limit-channels back to the original value – true.
For more information about configuring the radio interface via CLI, see Radio configuration section.

Running the spectrum analyzer on a wlan0 radio interface

WEP-3ax(root):/# **monitoring spectrum-wlan0**

```
Interface:    wlan0 last scanned channel:  11
 Channel| CCA
       1|  70%
       6|   0%
      11|  38%
```

Running the spectrum analyzer on a wlan1 radio interface

WEP-3ax(root):/# **monitoring spectrum-wlan1**

```
Interface:    wlan1 last scanned channel:  48
 Channel| CCA
      36|   8%
      40|   7%
      44|   9%
      48|   6%
```

Spectrum analyzer monitoring

WEP-3ax(root):/# **monitoring spectrum-status**

```
 wlan0:
 State - Idle
 Last run time - Thu Jul  1 16:31:46 2021
 Channel| CCA
       1|  70%
       6|   0%
      11|  38%

 wlan1:
 State - Idle
 Last run time - Thu Jul  1 16:32:53 2021
 Channel| CCA
      36|   8%
      40|   7%
      44|   9%
      48|   6%
```

7 The list of changes

Document version	Issue date	Revisions
Version 1.11	19.04.2024	Synchronization with firmware version 1.12.0 Changed: • 2.4 Radiation pattern of built-in antennas • 6.3.9 Advanced VAP settings Added: • 5.9.2 "AirTune" submenu
Version 1.10	15.12.2023	Synchronization with firmware version 1.11.0 Changed: • 5.6.2 "VAP" submenu Added: • 6.3.2 Configuration of VAP with OWE encryption • 6.3.3 Configuration of VAP with OWE and OWE Transition Mode • 6.10 Configuration of Radar mode
Version 1.9	6.10.2023	Synchronization with firmware version 1.10.0 Changed: • 5.4.8 "Device information" submenu • 5.6.2 "VAP" submenu • 6.4.1 Advanced Radio settings • 6.7.5 Advanced system settings • 6.10 Configuration of IGMP
Version 1.8	07.07.2023	Synchronization with firmware version 1.9.0 Added: • 5.7 "WDS" menu • 6.7 Configuration of WDS Changed: • 2.2 Device specification • 6.8 System settings
Version 1.7	14.02.2023	Synchronization with firmware version 1.8.1 Changed: • 5.6.2 "VAP" submenu
Version 1.6	09.12.2022	Synchronization with firmware version 1.8.0 Added: • 6.3.5 Configuration of VAP with RADIUS MAC authorization • 6.3.6 Configuration of backup RADIUS on VAP • 6.9 Configuration of IGMP

Document version	Issue date	Revisions
Version 1.5	15.08.2022	Synchronization with firmware version 1.7.0 Added: • 6.6 Configuring DHCP option 82 • 6.9 Configuring TCPDUMP Changed: • 5.5 "Radio" menu
Version 1.4	25.03.2022	Synchronization with firmware version 1.6.0 Added: • 2.4 Radiation patterns Changed: • 5.4.4 "Spectrum Analyzer" submenu • 6.3.5 Advanced VAP settings
Version 1.3	03.11.2021	Synchronization with firmware version 1.5.0
Version 1.2	31.07.2021	Synchronization with firmware version 1.4.0 Added: • 5.4.4 "Spectrum Analyzer" submenu • 6.2.1 Network parameters configuration using the set-management-vlan-mode utility • 6.5.5 Advanced system settings • 6.7.7 Spectrum Aanalyzer Changed: • 6.3.5 Advanced VAP settings • 6.7.5 Event log
Version 1.1	26.03.2021	Synchronization with firmware version 1.3.0
Version 1.0	30.06.2020	First issue
Firmware version 1.12.0		

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/