Wireless access point

WOP-20L

User manual

Firmware version 1.7.1

IP address: 192.168.1.10

Username: admin

Password: password

Contents

1 Introduction 5

1.1 Annotation 5

1.2 Symbols 5

2 Device description 6

2.1 Purpose 6

2.2 Device specification 6

2.3 Technical parameters 8

2.4 Design 9

2.5 Restore the factory configuration 11

2.6 Delivery package 11

3 Rules and recommendations for device installation 12

3.1 Safety rules 12

3.2 Installation recommendations 12

3.3 Frequency bandwidths and channels in the 5 GHz band for Wi-Fi 13

3.4 Calculating the number of required access points 13

3.5 Channel selection for neighbouring access points 13

3.6 Installation 15

3.6.1 Device installation on a mast/pole 15

3.6.2 Device installation on a wall 16

3.7 Connection 18

3.7.1 Instructions for sealing antenna connectors 19

4 Device management via the web interface 22

4.1 Getting started 22

4.2 Applying configuration and discarding changes 23

4.3 Web interface basic elements 24

4.4 The “Monitoring” menu 25

4.4.1 The “Wi-Fi Clients” submenu 25

4.4.2 The “WDS” submenu 26

4.4.3 The “Traffic Statistics” submenu 28

4.4.4 The “Scan Environment” submenu 30

4.4.5 The “Events” submenu 31

4.4.6 The “Network information” submenu 32

4.4.7 The “Radio Information” submenu 34

4.4.8 The “Device Information” submenu 35

4.5 The “Radio” menu 36
4.5.1 The “Radio 2.4 GHz” submenu 36
4.5.2 The “Radio 5 GHz” submenu 40
4.5.3 The “Advanced” submenu 44
4.6 The “VAP” menu 44
4.6.1 The “Summary” submenu 44
4.6.2 The “VAP” submenu 45
4.7 The “WDS” menu 49
4.7.1 The "WDS" submenu 49
4.8 The “Network Settings” menu 50
4.8.1 The “System Configuration” submenu 50
4.8.2 The “Access” submenu 51
4.9 The “External Services” menu 52
4.9.1 The “Captive Portal” submenu 52
4.10 The “System” menu 53
4.10.1 The “Device Firmware Upgrade” submenu 53
4.10.2 The “Configuration” submenu 54
4.10.3 The “Reboot” submenu 55
4.10.4 The “Password” submenu 55
4.10.5 The “Log” submenu 56
4.10.6 The “Date and Time” submenu 57
5 Managing the device using the command line 59
5.1 Connection to the device 59
5.2 Network parameters configuration 60
5.2.1 Network parameters configuration via set-management-vlan-mode utility 61
5.2.2 IPv6 network parameters configuration 62
5.3 Virtual Wi-Fi access points (VAP) configuration 64
5.3.1 Configuration of VAP without encryption 64
5.3.2 Configuration of VAP with WPA-Personal security mode 65
5.3.3 Configuration of VAP with Enterprise authorization 66
5.3.4 Configuration of VAP with Captive Portal 67
5.3.5 Advanced VAP settings 68
5.4 Radio configuration 74
5.4.1 Advanced Radio settings 75
5.5 DHCP option 82 Configuration 77

5.6 WDS Configuration 78
5.7 System settings 79
5.7.1 Device firmware update 79
5.7.2 Device configuration management 79
5.7.3 Device reboot 80
5.7.4 Authentication mode configuration 80
5.7.5 Setting the date and time 81
5.7.6 Advanced system settings 81
5.8 APB service configuration 82
5.9 Monitoring 83
5.9.1 Wi-Fi clients 83
5.9.2 WDS 85
5.9.3 Device information 86
5.9.4 Network information 87
5.9.5 Wireless interfaces 88
5.9.6 Event logging 88
5.9.7 Environment scan 89
5.9.8 Spectrum analyzer 90
6 The list of changes 91

1 Introduction

1.1 Annotation

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

WOP-20L device is a Wi-Fi access point. The device enclosed into hermetic case which allows using the access point outdoor in different climatic conditions – at temperatures from -45 to +65 °C

This manual specifies intended purpose, main technical parameters, design, safe operation rules and installation and configuration recommendations for WOP-20L.

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

WOP-20L wireless access point is designed to provide the user access to high-speed and secure network.

The main purpose of the device is to create a Layer 2 wireless network at the junction with a wired network. WOP-20L connects to a wired network over 10/100/1000M Ethernet interface and using radio interfaces creates wireless high-speed access for devices that support Wi-Fi technology in the 2.4 GHz and 5 GHz bands.

The device contains 2 radio interfaces for organizing two physical wireless networks.

WOP-20L supports modern requirements for the the quality of services and allows transmitting the most important traffic in higher priority queues than normal. Prioritization is provided by the following QoS technologies: CoS (special tags in the VLAN packet field) and ToS (tags in the IP packet field). Support for creating ACL rules and traffic shaping on each VAP allows one to fully manage access, quality of service and restrictions both for all subscribers and for everyone in particular.

The device is an indispensable solution for organizing a wireless network in various climatic conditions, in a wide range of operating temperatures and high humidity (parks, factories, stadiums, etc.), and is also an ideal platform for organizing communication in suburban settlements and remote locations.

2.2 Device specification

Interfaces:

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

Functions:

WLAN capabilities:

- support for IEEE 802.11a/b/g/n/ac;
- support for IEEE 802.11r/k/v roaming standards;
- data aggregation, including A-MPDU (Tx/Rx) and A-MSDU (Rx);
- WMM-based priorities and packet planning;
- wireless bridging (WDS);
- dynamic frequency selection (DFS);
- support for hidden SSID;
- 14 virtual access points;
- external access points detection;
- spectrum analyzer;
- auto channel selection.

Network functions:

- auto-negotiation of speed, duplex mode and switching between MDI and MDI-X modes;
- IPv6;
- support for VLAN;
- DHCP client;
- ACL;
- NTP;
- Syslog;
- GRE;
- transmission of subscriber traffic out of tunnels.

QoS functions:

- priority and profile-based packet scheduling;
- bandwidth limitation for each VAP;
- bandwidth limitation for each client;
- WMM parameters changing.

Security:

- centralized authorization via RADIUS server (802.1X WPA/WPA2 Enterprise);
- WPA/WPA2 data encryption;
- support for Captive Portal.

Figure 1 shows WOP-20L application diagram.

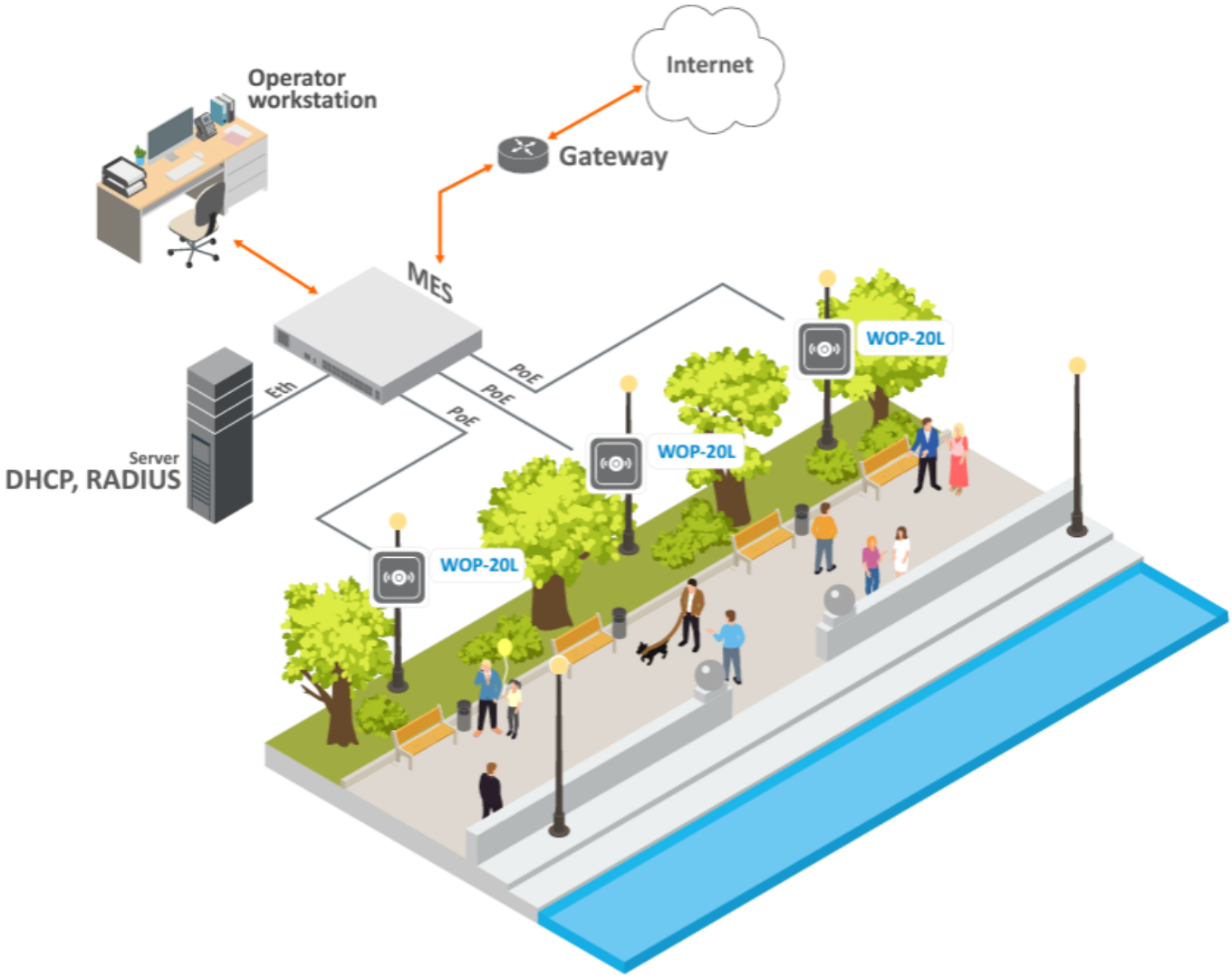


Figure 1 — WOP-20L application diagram

2.3 Technical parameters

Table 1 — Main specifications

WAN interface parameters	
Number of ports	1
Electrical connector	RJ-45
Data rate	10/100/1000 Mbps, auto-negotiation
Standards	BASE-T
Wireless interface parameters	
Standards	802.11a/b/g/n/ac
Frequency range	2400–2483.5 MHz; 5150–5350 MHz, 5470–5850 MHz
Modulation	BPSK, QPSK, 16QAM, 64QAM, 256QAM
Operating channels	802.11b/g/n: 1–13 (2402–2482 MHz) 802.11a/n/ac: • 36–64 (5170–5330 MHz) • 100–144 (5490–5730 MHz) • 149–165 (5735–5835 MHz)
Data rate	802.11a: up to 54 Mbps 802.11b: up to 11 Mbps 802.11g: up to 54 Mbps 802.11n: up to 300 Mbps 802.11ac: up to 867 Mbps
Maximum output power of the transmitter	2.4 GHz: 18 dBm 5 GHz: 20 dBm
Receiver sensitivity	2.4 GHz: up to -91 dBm 5 GHz: up to -93 dBm
Security	Centralized authorization via RADIUS server (802.1X WPA/WPA2 Enterprise) WPA/WPA2 data encryption Support for Captive Portal
The choice of antenna model depends on the use of the access point	
Supporting 2×2 MIMO	
Control	
Remote control	Web interface, Telnet, SSH, CLI, SNMP, NETCONF, SoftWLC
Access restriction	By password, authentication via RADIUS server
General parameters	
Flash	128 MB NAND Flash
RAM	256 MB RAM DDR3

Power supply	PoE 48 V/56 V (IEEE 802.3af-2003)
Power consumption	No more than 12 W
Ingress protection	IP55
Operating temperature range	From -45 to +65 °C
Relative humidity at 25 °C	Up to 95 %
Dimensions (W× H × D)	125 × 227 × 49 mm
Weight	0.77 kg
Lifetime	No less than 15 years

2.4 Design

WOP-20L enclosed in a plastic case. The layout of WOP-20L panels is shown in Figures 2 and 3.

Figure 2 — WOP-20L front panel layout

The bottom panel of WOP-20L has a 10/100/1000BASE-T LAN port (RJ-45 connector) for connecting to the internal network and PoE power, and a factory reset button (“F”).

Figure 3 — WOP-20L bottom panel layout

The current status of the device is displayed using the LEDs located on the device front panel. The possible indicator states are described in Table 2.

Table 2 — Light indication of device status

LED		LED status	Description
	Power – power and device status indicator	Solid	The device power supply is enabled, normal operation
		Flashing	The device did not receive an address via DHCP
		Fast flashing for 3 seconds, then solid	Reboot/factory reset
	LAN – Ethernet port indicator	Solid	The link between the WOP-20L Ethernet interface and the connected device is active
		Flashing	The packet data transfer process between the WOP-20L Ethernet interface and the connected device
2.4G	**Wi-Fi 2.4 GHz** – 2.4 GHz wireless network status indicator	Solid	The Wi-Fi network in the 2.4 GHz band is active
5G	**Wi-Fi 5 GHz** – 5 GHz wireless network status indicator	Solid	The Wi-Fi network in the 5 GHz band is active

2.5 Restore the factory configuration

To restore the factory configuration, press and hold the "F" button for 10–15 seconds until the Wi-Fi 2.4 GHz and the Wi-Fi 5 GHz indicators start flashing. The device will automatically reboot.

By default, the DHCP client will be launched. If the address is not obtained via DHCP, then the device will have the factory IP address — *192.168.1.10*, subnet mask — *255.255.255.0*.

2.6 Delivery package

The delivery package includes:

- WOP-20L wireless access point;
- Mounting kit;
- User manual on a CD (optional);
- Technical passport.

3 Rules and recommendations for device installation

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

3.1 Safety rules

1. Do not open the device case. There are no user serviceable parts inside.
2. The unused antenna connectors should be closed with a protective cover, which is included in the device delivery set.
3. Do not install the device during a lightning storm. There may be a risk of being struck by lightning.
4. The voltage, current and frequency requirements specified in this manual should be observed.
5. Measurement eqipment and a computer should be grounded before connecting to the device. Potential difference between cases of equipment and measurement devices should be no more than 1 V.
6. Before turning on the device, make sure that the cables are intact and securely fastened to the connectors.
7. Do not install the device near heat sources or at places where temperature may be below -45 °C or higher 65 °C.
8. When installing the device on high-rise structures, the established standards and requirements for working at height should be observed.
9. The operation of the device should be carried out by engineering and technical personnel who have undergone special training.
10. Only suitable auxiliary equipment should be connected to the device.

3.2 Installation recommendations

1. The recommended installation position: attaching to a mast/pole.
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. When placing the device, in order to provide the best Wi-Fi coverage consider the following rules:
    - Install the device at the center of a wireless network;
    - Minimize the number of barriers (walls, ceilings, furniture, and etc.) between WOP-20L and other wireless network devices;
    - Do not install the device near (about 2 m) electrical and radio devices;
    - It is not recommended to use radiophones and other equipment operating at frequency of 2.4 GHz or 5 GHz, within the range of a Wi-Fi network;
    - Obstacles like glass/metal constructions, brick/concrete walls, water cans and mirrors can significantly reduce Wi-Fi action radius. It is not recommended to place the device inside a false ceiling as metal frame causes multipath signal propagation and signal attenuation.
4. When installing several access points, cell action radius must overlap with action radius of a neighboring cell at the level from -65 to -70 dBm. It is allowed to reduce the signal level to -75 dBm at cell boundaries, if it is not intended to use VoIP, video streaming and other sensitive to losses traffic in wireless network.

3.3 Frequency bandwidths and channels in the 5 GHz band for Wi-Fi

The data transmission in the 5 GHz band is used for IEEE 802.11a/n/ac standards. The WOP-20L device supports frequency channels in the 5 GHz band with a width of 20, 40 and 80 MHz.

The following formula is used to calculate the center frequency of the Wi-Fi channel (f, in MHz):

f=5000+(5*N), where N — the Wi-Fi channel number.

3.4 Calculating the number of required access points

Table 3 — 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 wire cloth	-14,8	-13,2
Breeze block	-7	-11
Metal lattice (mesh 13×6 mm, metal 2 mm)	-21	-13

3.5 Channel selection for neighbouring access points

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

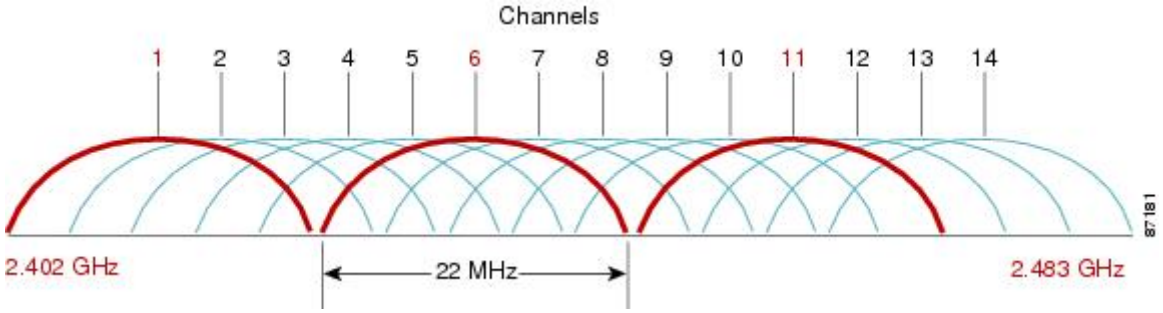


Figure 4 — General diagram of frequency channel overlap in the range of 2.4 GHz

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

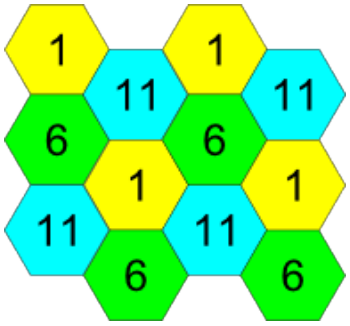


Figure 5 — Scheme of channel allocation among neighboring access points in the frequency range of 2.4 GHz when channel width is 20 MHz

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

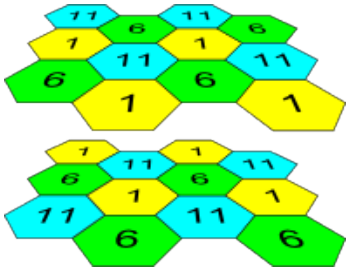


Figure 6 — Scheme of channel allocation between neighboring access points that are located between floors

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

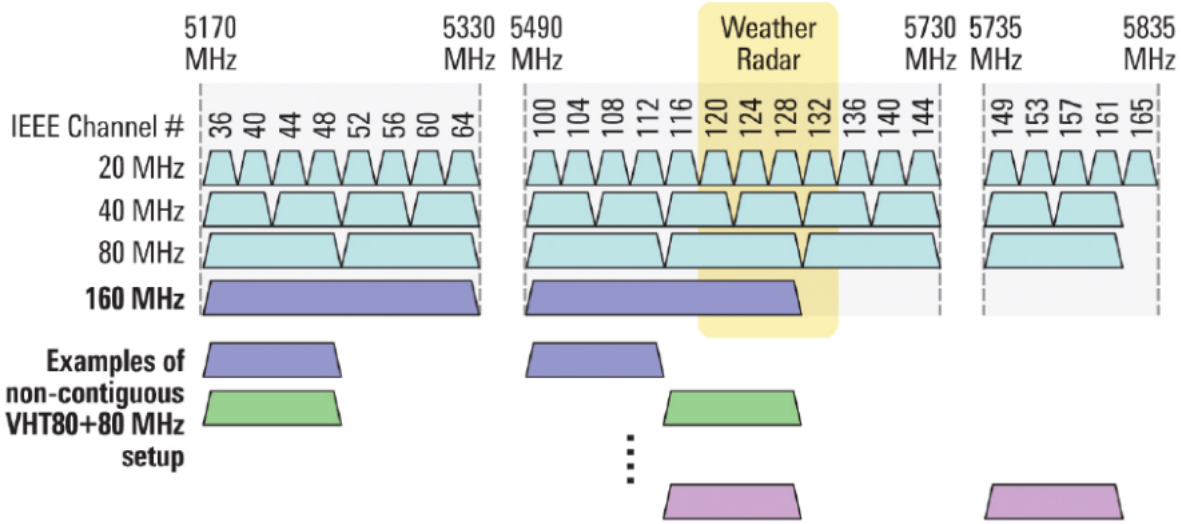


Figure 7 — Channels used in the 5 GHz band when channel width is 20, 40 or 80 MHz

3.6 Installation

There are two mounting options for the WOP-20L access point: mounting the device on a pole and on a wall.

3.6.1 Device installation on a mast/pole

1. Attach the bracket to the device case using the supplied screws as shown in the figure below.

Figure 8 — Attaching the bracket to the device

2. Install the device with the Ethernet port down on the pole as shown in the figure below, and secure it with the clamps supplied with the device. Follow the safety instructions and recommendations in the Safety rules and Installation recommendations sections.

Figure 9 — Attaching the device to the pole

3.6.2 Device installation on a wall

This device installation method is optional — the bracket is sold separately and is not included in the package.

1. Align the four screw holes on the bracket with the same screw holes on the device. Use a screwdriver to attach the bracket to the device as shown in Figure 10.

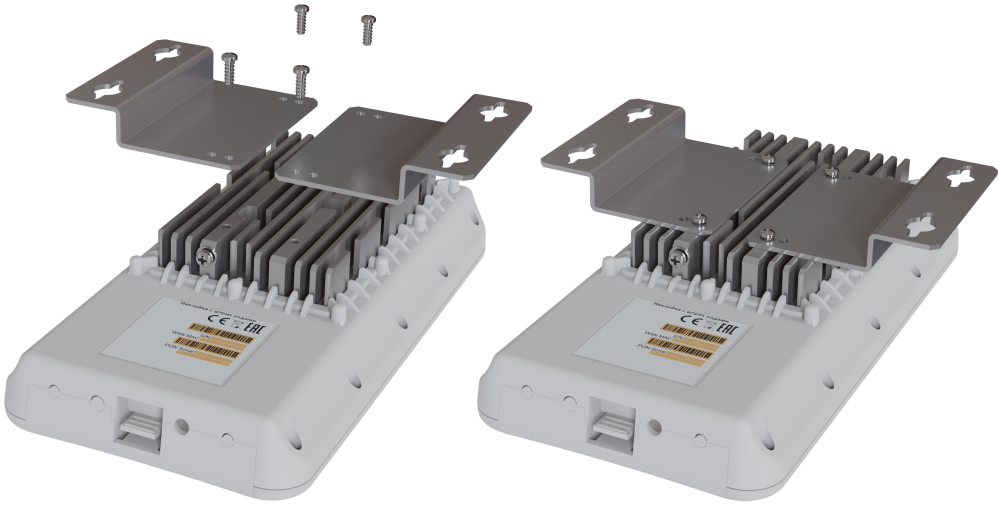


Figure 10 — Attaching the bracket to the device

2. Choose a location for the access point according to the Safety rules and Installation recommendations sections of this manual. Place the base of the bracket against the wall and mark the location of the screw holes (Figure 11). Drill holes and fasten the screws in them. Do not tighten the screws firmly.

Figure 11 — Placing the device on the wall

3. Align the bracket holes with the screws on the wall. Move the bracket up or down until it stops and fasten the screws (Figure 12).

Figure 12 — Fixing the device to the wall

3.7 Connection

Figure 13 — Connecting Ethernet cable to the PoE port

1. Remove the cover protecting the Ethernet port on the bottom of the device, then connect the Ethernet cable to the PoE port (Figure 13).
2. Close the bottom cover.
3. Connect the Ethernet cable from WOP-20L to the injector PoE port or the switch port (IEEE 802.3af-2003).
4. If the PoE injector is used, connect it to a 220V outlet using a power cord.
5. Connect the antenna to the device following the instructions in the Instructions for sealing antenna connectors section:
    a. When using Omni antennas: connect the antennas to the device's SMA connectors;
    b. When using panel/sector antennas: connect the antennas to the device's SMA connectors using cable assemblies. Adjust the position of the antenna so that subscriber units are within the coverage area of the installed antenna.

It is recommended to use lightning protection to avoid damage to the device.

3.7.1 Instructions for sealing antenna connectors

Sealing should be carried out on both sides of the cable.

1. Before connecting the cable to the connector, inspect the cable sheath for damage, and also check if a sealing ring is in the connector nut, the location is shown in Figure 14 (a, b).

Figure 14a

Figure 14b

Figure 15a

Figure 15b

3. Cut the rubber sealing tape to the appropriate length: one SMA connector (Figure 15a) requires 0.15 m of waterproofing tape, one N-type connector (Figure 15b) requires 0.3 m of waterproofing tape, as shown in Figure 16 (a, b).

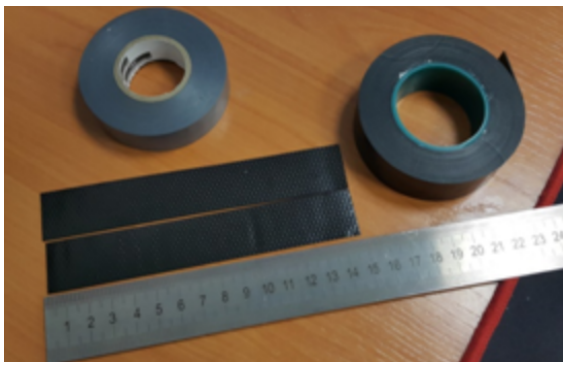


Figure 16a

Figure 16b

4. Remove the protective layer from the rubber tape as shown in Figure 17.

Figure 17

5. Start winding from the side of the cable, having previously stepped back from the crimping part by 10–15 mm. Fix the tip of the tape on the cable sheath at the angle of 15–25 degrees to the cable axis, and, slightly stretching the tape, start wrapping the cable and the connector, moving towards the device case. The tape turns should be laid on top of each other with an overlap, wrinkles on the turns are not allowed. The cable winding is shown in Figure 18 (a, b).

Figure 18a

Figure 18b

6. Having reached the device case (antenna) with the edge of the tape, make a turn around the connector, pressing the edge of the tape to the case as much as possible, then continue winding the tape at a different angle, moving away from the body. When winding, do not forget to stretch the tape and press it tightly against the previously wound turns. At the tip of the tape, the stretch should be reduced and pressed tightly against the turns located on the cable sheath, as shown in Figure 19 (a, b).

Figure 19a

Figure 19b

7. Cut the PVC tape (duct tape) to the appropriate length: one SMA connector requires 0.28 m of the PVC tape, one N-type connector requires 0.6 m of the PVC tape. The PVC tape is required to protect the rubber tape from UV rays. The PVC tape is shown in Figure 20.

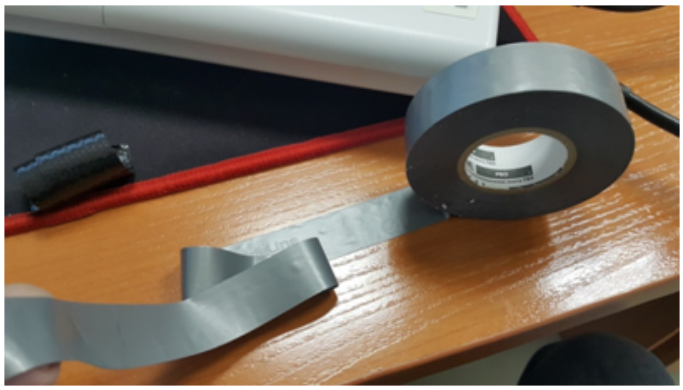


Figure 20

8. Start the winding from the cable sheath, having previously stepped back from the first turn of the rubber tape by 5–10 mm. Fix the tip of the PVC tape on the cable sheath at an angle of 15–25 degrees to the cable axis, and, slightly stretching the tape, start wrapping the cable and connector, moving towards the device case. The turns should be laid on top of each other with an overlap, wrinkles on the turns are not allowed. The cable winding is shown in Figure 21.

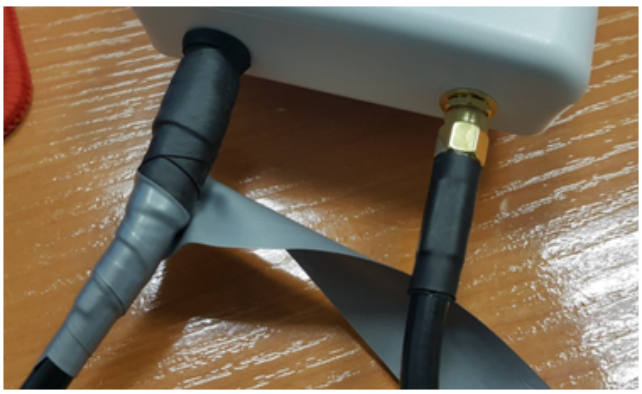


Figure 21

9. Having reached the case with the edge of the tape, make a turn around the connector, pressing the edge of the PVC tape to the device case as much as possible, then continue winding the tape at a different angle, moving away from the case. When winding, tightly apply the turns of the tape, avoiding wrinkles. On the last turns of the PVC tape, the stretch should be reduced to zero and the last turn should be laid without stretching, as shown in Figure 22 (a, b).

Figure 22a

Figure 22b

10. Check the sealed connector for visible rubber tape.

4 Device management via the web interface

4.1 Getting started

In order to start the operation, 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.

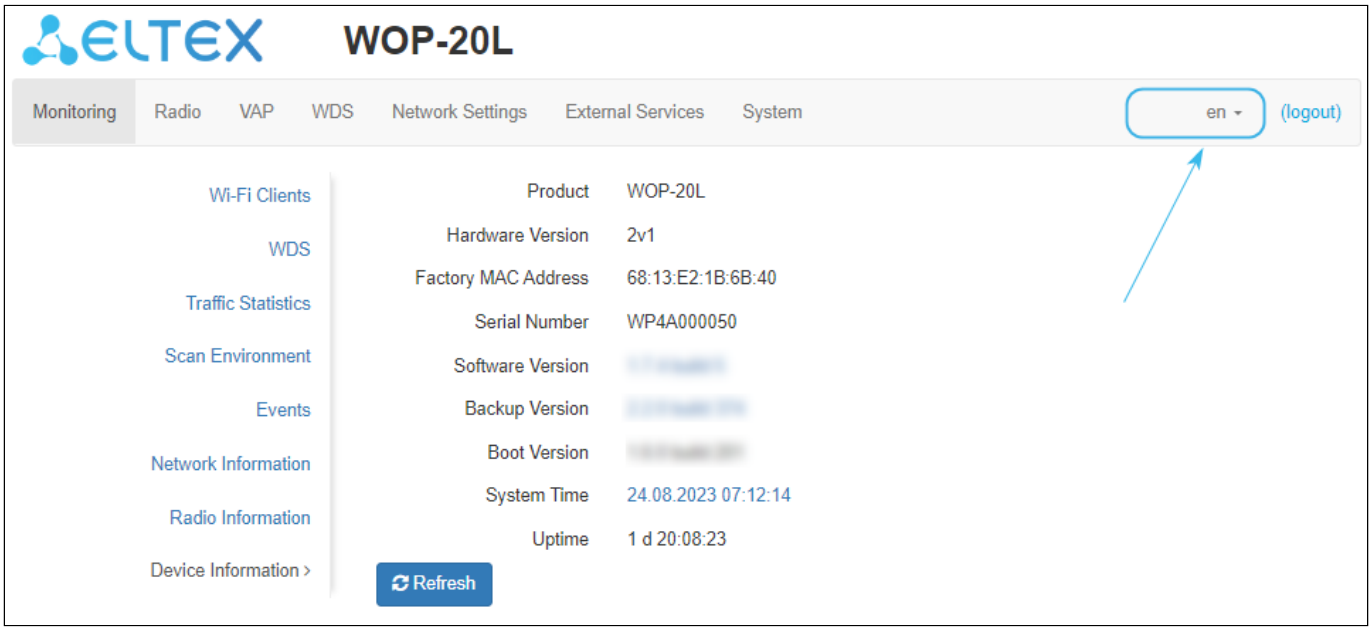
When the device is successfully detected, username and password request page will be shown in the browser window:

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 device status will open in a browser window.

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



4.2 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 WOP-20L web interface has a visual indication of the current status of the setting applying process (Table 4).

Table 4 — Visual indication of the current status of the setting application process

Image	State description
Apply	Clicking "Apply" starts the process of saving the configuration to the device flash memory and applying the new settings. 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 button for discarding changes appears as follows: Cancel.

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

4.3 Web interface basic elements

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

User interface window is divided into five general areas:

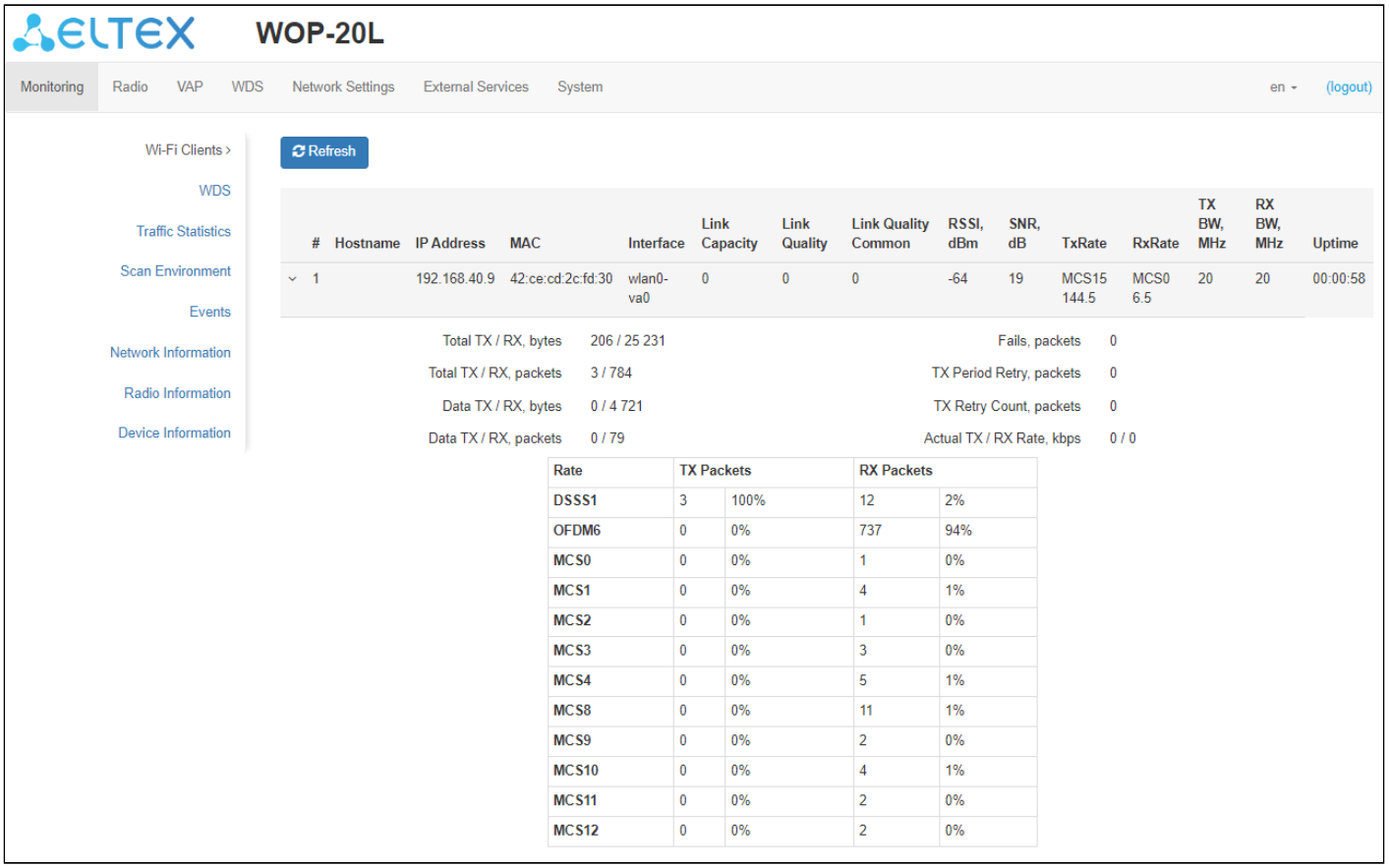
1. Menu tabs categorize the submenu tabs: **Monitoring, Radio, VAP, WDS, Network Settings, External Services, System.**
2. Interface language selection and Logout button designed to end a session in the web interface under a given user.
3. Submenu tabs allow one to control settings field.
4. Device configuration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

4.4 The “Monitoring” menu

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

4.4.1 The “Wi-Fi Clients” submenu

The **“Wi-Fi Clients”** submenu displays information about the status of connected Wi-Fi clients. Information on connected clients is not displayed in real time. In order to update the information on the page, click “Refresh”.



- # — number of the connected device in the list;
- *Hostname* — network name of the device;
- *IP address* — IP address of the connected device;
- *MAC address* — MAC address of the connected device;
- *Interface* — WOP-20L interaction interface 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 3x3 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

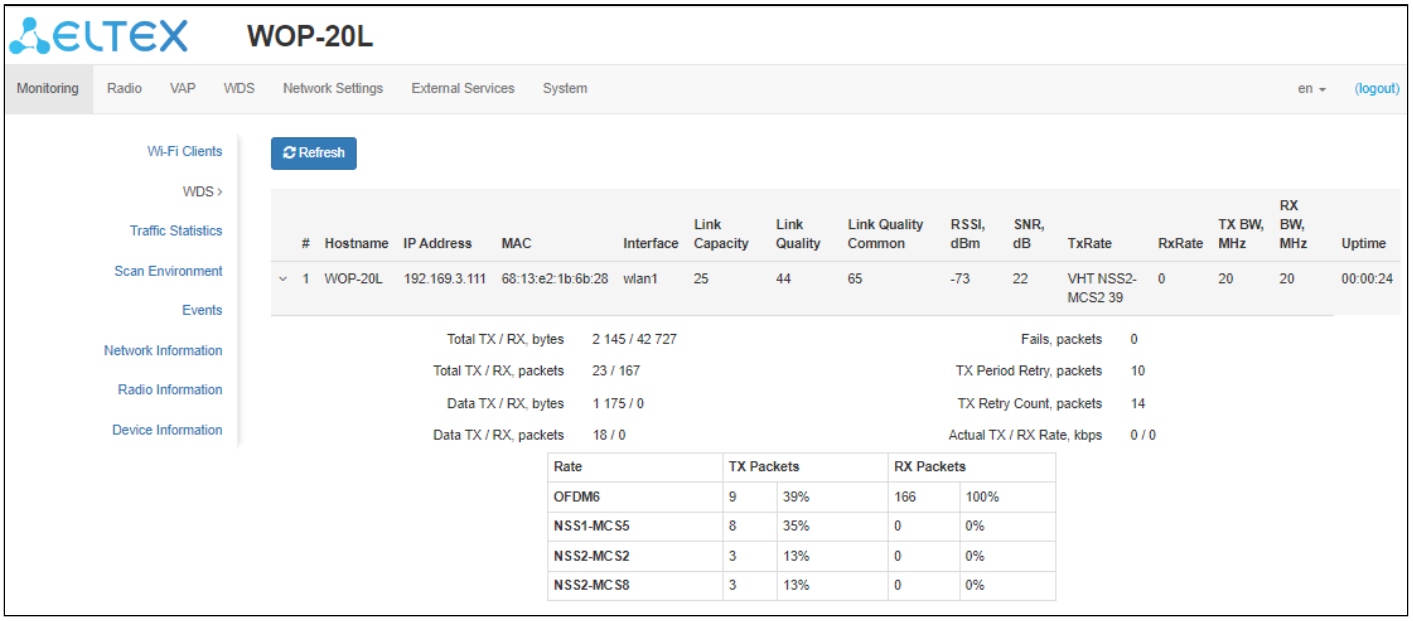
packets were sent on the first attempt), the minimum value is 0% (no packets were successfully sent to the client). The parameter value is calculated for the entire time of the client connection;
- *RSSI* — received signal level, dBm;
- *SNR* — signal/noise ratio, dB;
- *TxRate* — channel data rate of transmission, Mbps;
- *RxRate* — channel data rate of reception, Mbps;
- *Tx BW* — transmission bandwidth, MHz;
- *Rx BW* — reception bandwidth, MHz;
- *Uptime* — Wi-Fi client connection time.

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

- *Total TX/RX, bytes* — number of bytes sent/received on the connected device;
- *Total TX/RX, packets* — number of packets sent/received on the connected device;
- *Data TX/RX, bytes* — number of data bytes sent/received on the connected device;
- *Data TX/RX, packets* — number of data packets sent/received on the connected device;
- *Fails, packets* — number of packets sent with errors on the connected device;
- *TX Period Retry, packets* — number of retries of transmission to the connected device 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.

4.4.2 The “WDS” submenu

The "**WDS**" submenu displays information about the status of WOP-20L access points connected via WDS.



- *#* — number of the connected device in the list;
- *Hostname* — device network name;
- *IP Address* — IP address of the connected device;
- *MAC* — MAC address of the connected device;
- *Interface* — WOP-20L interaction interface 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 3x3 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. Maximum value — 100% (all transmitted packets were sent on the first attempt), minimum value — 0% (no packet to the client was successfully sent). 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* — ratio signal/noise, 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 time.

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

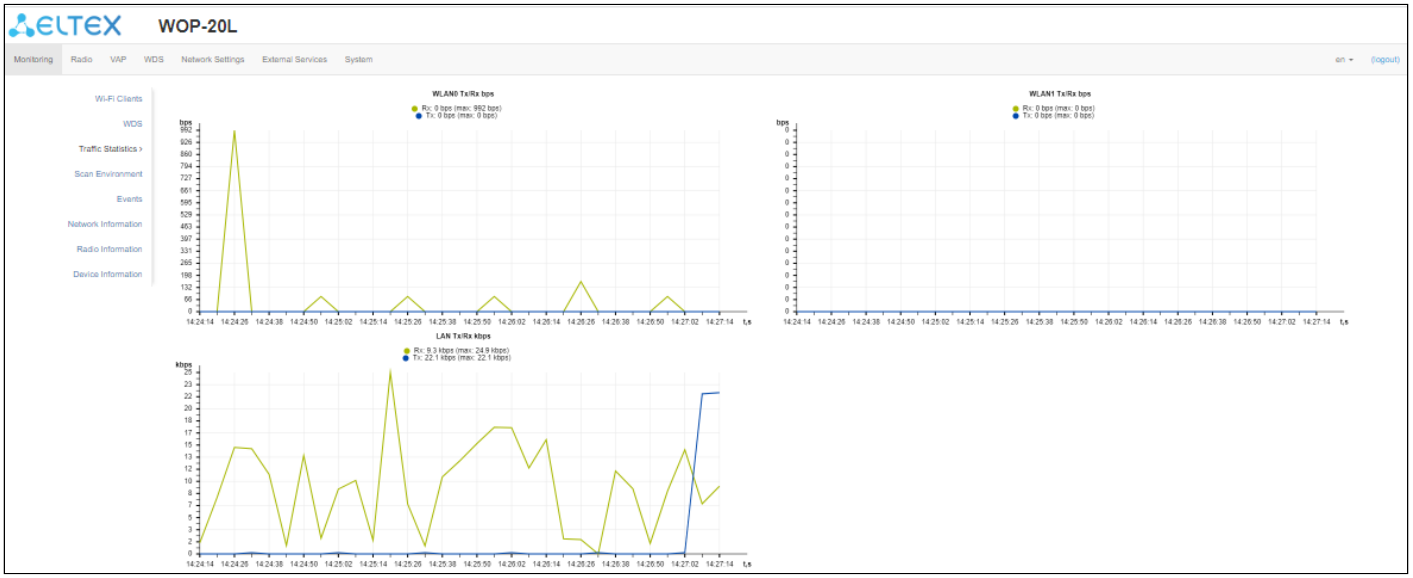
- *Total TX/RX, bytes* — number of bytes sent/received on the connected device;
- *Total TX/RX, packets* — number of packets sent/received on the connected device;
- *Data TX/RX, bytes* — number of data bytes sent/received on the connected device;
- *Data TX/RX, packets* — number of data packets sent/received on the connected device;
- *Fails, packets* — number of packets sent with errors on the connected device;
- *TX Period Retry, packets* — number of retries of transmission to the connected device for the last 10 seconds;
- *TX Retry Count, packets* — the 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.

4.4.3 The “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 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 6 seconds.

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



"Transmit" table description:

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

Transmit

Interface	Total Packets	Total Bytes	Total Drop	Errors
LAN	218928	139979799	0	0
WLAN0	95	13622	2064744	0
WLAN1	0	0	673280	0
wlan0-va0	79	7792	1350	0
wlan0-va1	0	0	0	0
wlan0-va2	0	0	0	0
wlan0-va3	0	0	0	0
wlan0-va4	0	0	0	0
wlan0-va5	0	0	0	0
wlan0-va6	0	0	0	0

"Receive" table description:

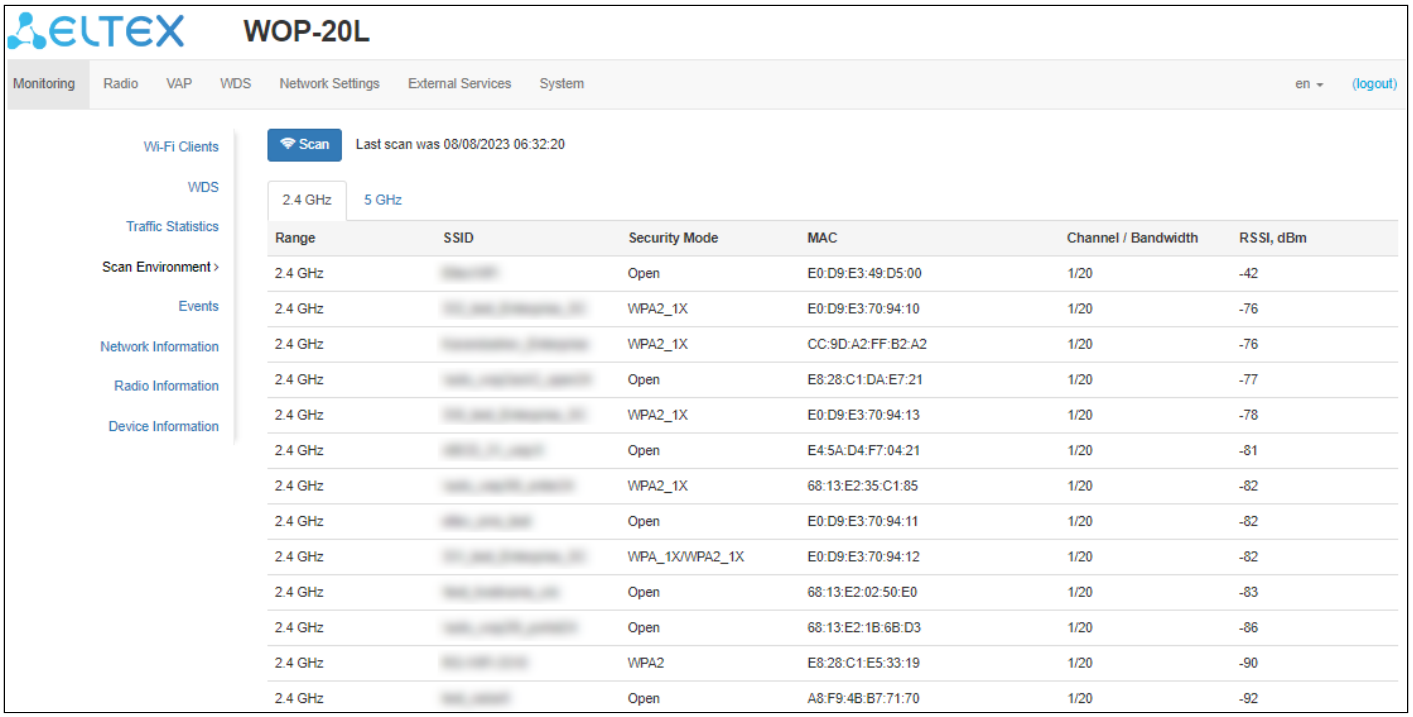
- *Interface* — name of the interface;
- *Total packets* — number of successfully received packets;
- *Total bytes* — number of successfully received bytes;
- *Total drop* — number of rejected packets;
- *Errors* — number of errors.

Receive

Interface	Total Packets	Total Bytes	Total Drop	Errors
LAN	7188178	921420748	0	0
WLAN0	514	49624	242	4697489
WLAN1	0	0	0	0
wlan0-va0	452	35439	186	0
wlan0-va1	0	0	0	0
wlan0-va2	0	0	0	0
wlan0-va3	0	0	0	0
wlan0-va4	0	0	0	0
wlan0-va5	0	0	0	0

4.4.4 The “Scan Environment” submenu

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



Range	SSID	Security Mode	MAC	Channel / Bandwidth	RSSI, dBm
2.4 GHz		Open	E0:D9:E3:49:D5:00	1/20	-42
2.4 GHz		WPA2_1X	E0:D9:E3:70:94:10	1/20	-76
2.4 GHz		WPA2_1X	CC:9D:A2:FF:B2:A2	1/20	-76
2.4 GHz		Open	E8:28:C1:DA:E7:21	1/20	-77
2.4 GHz		WPA2_1X	E0:D9:E3:70:94:13	1/20	-78
2.4 GHz		Open	E4:5A:D4:F7:04:21	1/20	-81
2.4 GHz		WPA2_1X	68:13:E2:35:C1:85	1/20	-82
2.4 GHz		Open	E0:D9:E3:70:94:11	1/20	-82
2.4 GHz		WPA_1X/WPA2_1X	E0:D9:E3:70:94:12	1/20	-82
2.4 GHz		Open	68:13:E2:02:50:E0	1/20	-83
2.4 GHz		Open	68:13:E2:1B:6B:D3	1/20	-86
2.4 GHz		WPA2	E8:28:C1:E5:33:19	1/20	-90
2.4 GHz		Open	A8:F9:4B:B7:71:70	1/20	-92

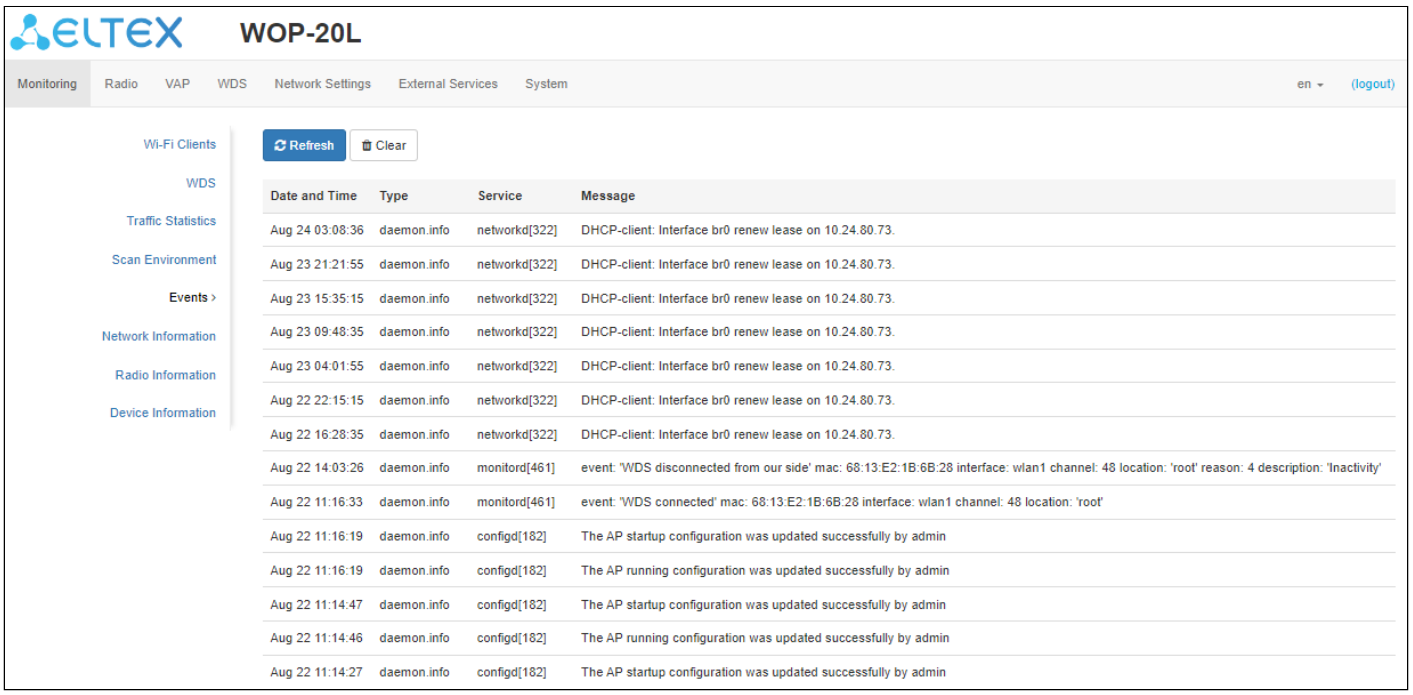
After clicking “Scan”, the process will be launched. After the scan is completed, a list of detected access points and information about them will appear:

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

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

4.4.5 The “Events” submenu

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



- *Date and Time* — 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 5 — Description of event severity levels

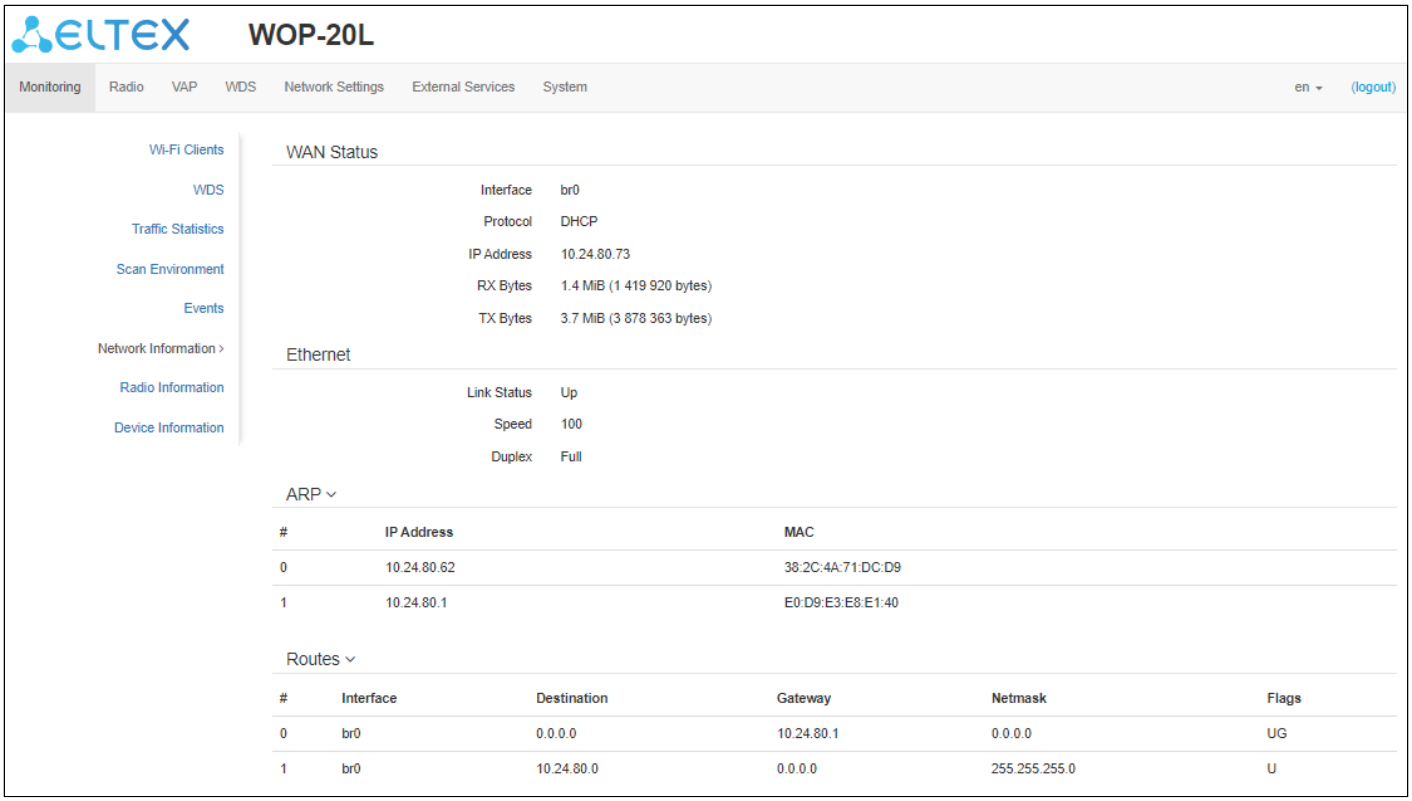
Level	Message severity level	Description
0	Emergency	A critical error has occurred in the system, the system may not work properly.
1	Alert	Immediate intervention is required.
2	Critical	A critical error has occurred in the system.
3	Error	An error has occurred in the system.
4	Warning	Warning, non-emergency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

4.4.6 The “Network information” submenu

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



WAN Status:

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

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:

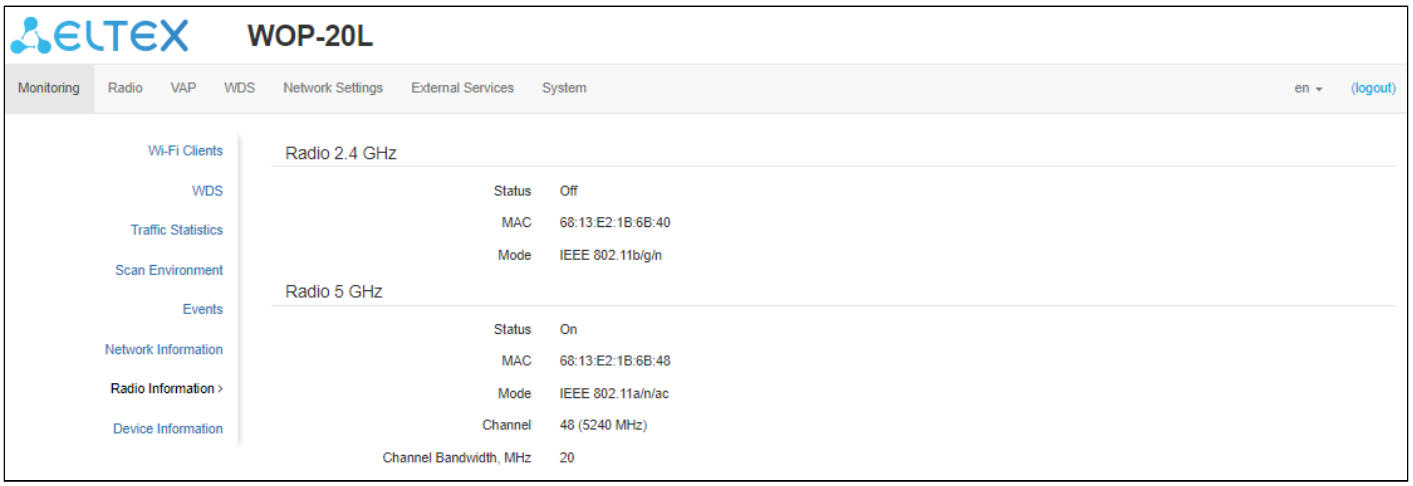
- *Interface* — name of the bridge interface;
- *Destination* — IP address of destination host or subnet that the route is established to;
- *Gateway* — IP address of the gateway through which access to the destination is carried out;
- *Netmask* — subnet mask;
- *Flags* — certain route characteristics.

The following flag values exist:

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

4.4.7 The “Radio Information” submenu

In the **“Radio Information”** submenu, the current status of WOP-20L radio interfaces is displayed.



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

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

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

“Off”:

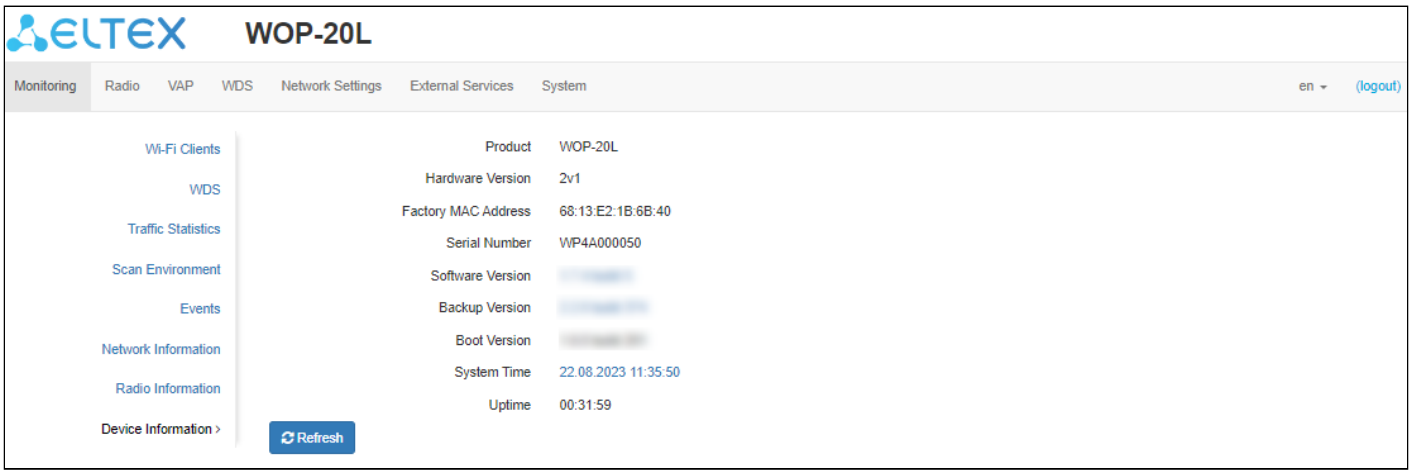
- *Status* — radio interface state;
- *MAC* — radio interface MAC address;
- *Mode* — radio interface operation mode according to IEEE 802.11 standards.

“On”:

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

4.4.8 The “Device Information” submenu

The **“Device Information”** submenu displays WOP-20L main characteristics.



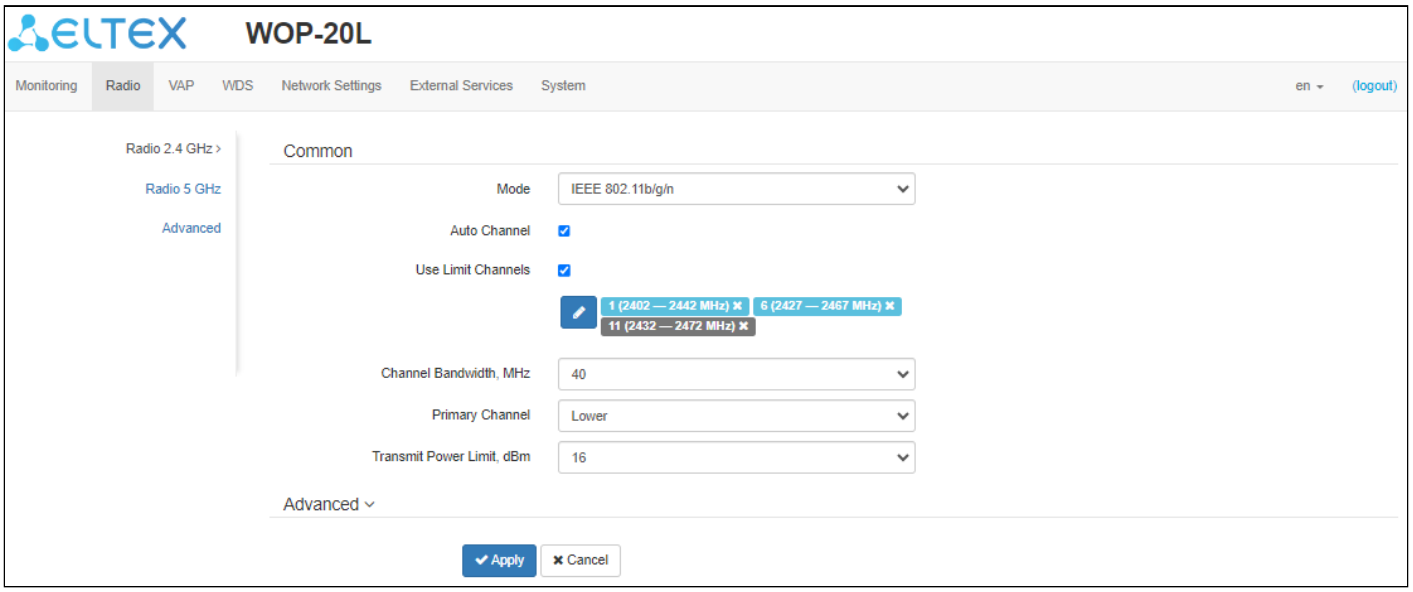
- *Product* — device model name;
- *Hardware Version* — device hardware version;
- *Factory MAC Address* — device WAN interface MAC address, factory set;
- *Serial Number* — device serial number, factory set;
- *Software Version* — device firmware version;
- *Backup Version* — previously installed firmware version;
- *Boot Version* — device firmware boot version;
- *System Time* — current time and date, set in the system;
- *Uptime* — operating time since the last time the device was turned on or rebooted.

4.5 The “Radio” menu

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

4.5.1 The “Radio 2.4 GHz” submenu

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



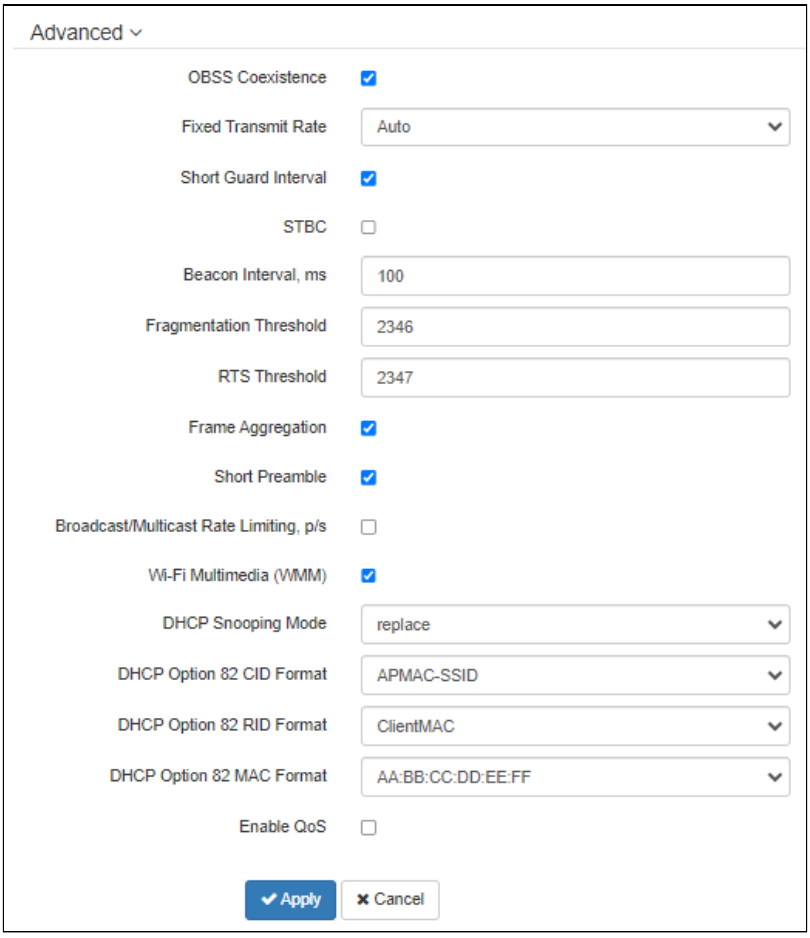
- *Mode* — interface operation mode according to the following standards:
  - IEEE 802.11b/g;
  - IEEE 802.11b/g/n;
  - IEEE 802.11n.
- *Auto Channel* — when checked, the device will automatically select the least congested radio channel for the Wi-Fi interface. Unchecking the flag opens the access to install the static operation channel;
- *Channel* — select channel for data transmission;
- *Use Limit Channels* — when checked, the access point will use a user-defined list of channels to work in automatic channel selection mode. If the “Use Limit channels” flag is not checked or there are no channels in the list, the access point will select the operation channel from all available channels in the given band. The 2.4 GHz band channels: 1–13;
- *Channel Bandwidth, MHz* — channel bandwidth, on which the access point operates. The parameter may take values 20 and 40 MHz;
- *Primary Channel* — 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 supporting 20 MHz channel bandwidth only:
  - *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* — adjustment of the signal strength of the Wi-Fi transmitter in dBm. Accepts value from 8 to 16 dBm.

If the “Use Limit channels” list contains a channel that is not available for selection, it will be marked in grey. In order for the new configuration to be applied to an access point, only available (blue highlighted) channels must be specified in the “Use Limit channels” list.
Example. No settings have been made on the access point yet, Radio 2.4 GHz is set to 20 MHz “Channel Bandwidth” by default, and channels are specified in the “Use Limit channels” list: 1, 6, 11. Suppose the parameter “Channel Bandwidth” should be set to 40 MHz. Upon changing 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 clicking “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.

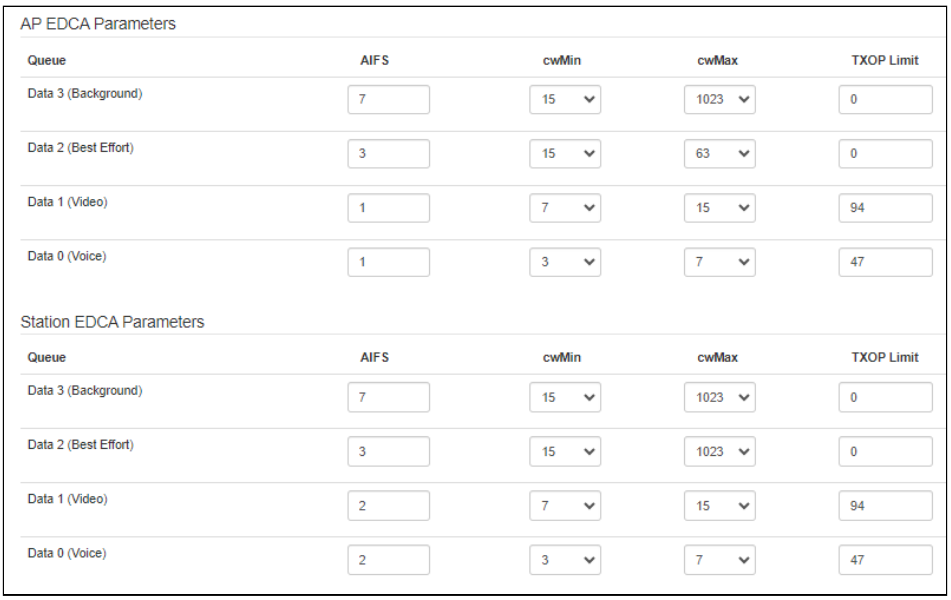
In the “Advanced” section, it is possible to configure advanced radio interface parameters of the device.



- *OBSS Coexistence* — automatic channel bandwidth reduction when the channel is loaded. When the flag is set, the mode is enabled;
- *Fixed Transmit Rate* — fixed wireless data rate, defined by IEEE 802.11b/g/n specifications;
- *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. The field is available only if the selected operating mode for the radio interface includes 802.11n. When checked, the device transmits one data flow through several antennas. When unchecked, the device does not transmit the same data flow through several antennas;

- *Beacon Interval, ms* — beacon frames transmission period. The frames are sent to detect access points on the air. The parameter takes values from 20 to 2000 ms, by default: 100 ms;
- *Fragmentation Threshold* — frame fragmentation threshold, bytes. The parameter takes values 256–2346, by default: 2346;
- *RTS Threshold* — specifies the number of bytes over which the Request to Send will be sent. Decreasing this value may improve the performance of the access point when there are a lot of connected clients. However this reduces general throughput of wireless network. The parameter takes values from 0 to 2347, by default: 2347;
- *Frame aggregation* — enable support for AMPDU/AMSDU;
- *Short Preamble* — use of the packet short preamble;
- *Broadcast/Multicast Rate Limiting, p/s* — when the flag is set, transmission of broadcast / multicast traffic over the wireless network is restricted. Specify the limit for broadcast traffic in the popup window (p/s);
- *Wi-Fi Multimedia (WMM)* — WMM support activation (Wi-Fi Multimedia);
- *DHCP Snooping Mode* — selection of DHCP option 82 processing policy. Available values for selection:
    - *ignore* — option 82 processing is disabled. Default value;
    - *remove* — access point deletes the value of option 82;
    - *replace* — access point substitutes or replaces the value of option 82. When selecting this value to edit, the following parameters are opened:
        - *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 (-).
- *Enable QoS* — when the flag is set, the setting of Quality of Service functions is available.

The following functions are available for quality assurance configuration:

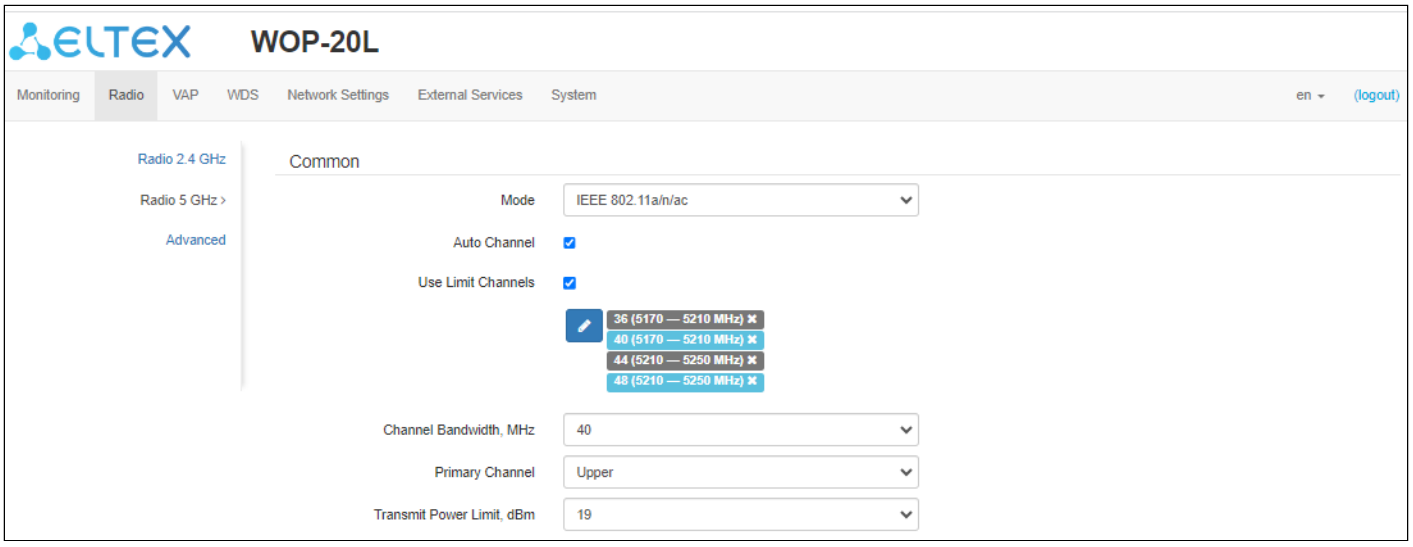


- *AP EDCA parameters* — access point settings table (traffic is transmitted from the access point to the client):
  - *Queue* — predefined queues for various kinds of traffic:
    - *Data 3 (Background)* — low priority queue, high bandwidth (802.1p: cs1, cs2 priorities);
    - *Data 2 (Best Effort)*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

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

4.5.2 The “Radio 5 GHz” submenu

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



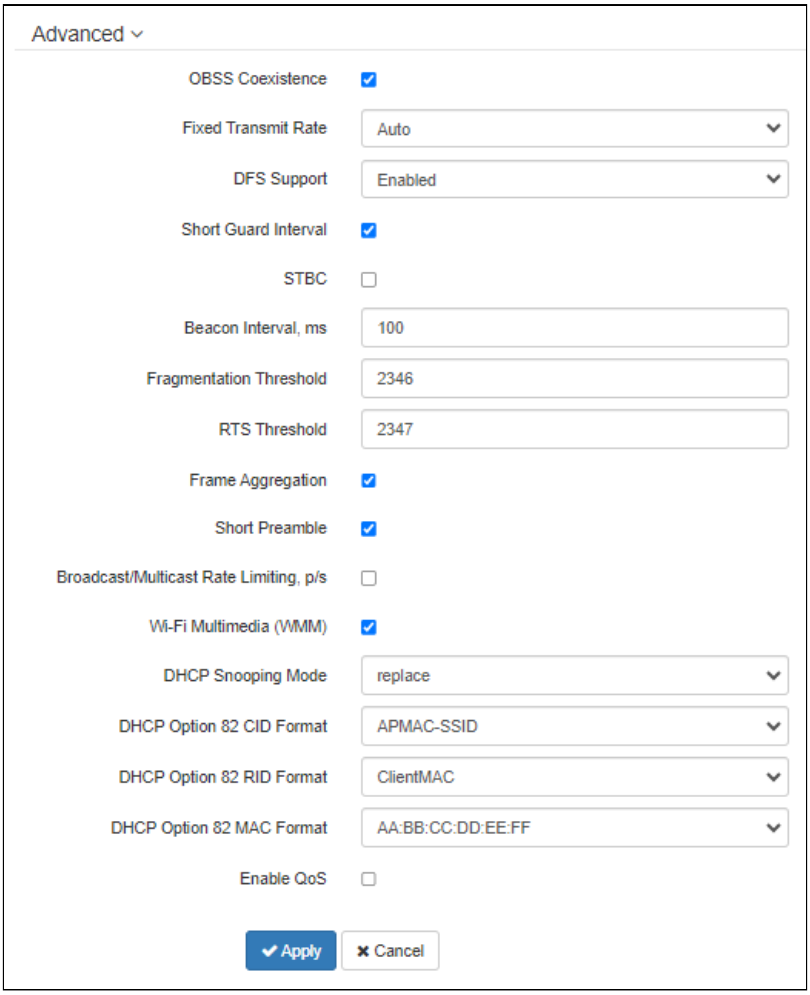
- *Mode* — select interface operation mode according to the following standards:
  - IEEE 802.11a;
  - IEEE 802.11a/n;
  - IEEE 802.11a/n/ac.
- *Auto Channel* — when checked, the device will automatically select the least congested radio channel for the Wi-Fi interface. Removing the flag opens the access to install the static operation channel;
- *Channel* — select channel for data transmission;
- *Use Limit Channels* — when checked, the access point will use a user-defined list of channels to work in automatic channel selection mode. If the “Use Limit channels” flag is not checked or there are no channels in the list, the access point will select the operation channel from all available channels in the given band. 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 11 and 19 dBm.

If the “Use Limit channels” list contains a channel that is not available for selection, it will be marked in grey. In order for the new configuration to be applied to an access point, only available (blue highlighted) channels must be specified in the “Use Limit channels” list.
Example. No settings have been made on the access point yet, Radio 5 GHz is set to 20 MHz “Channel Bandwidth” by default, and channels are specified in the “Use Limit channels” list: 36, 40, 44, 48. Suppose, it is required to set “Channel Bandwidth” to 40 MHz. When you change this parameter from 20 MHz to 40 MHz, the following happens:

- the “Primary Channel” parameter becomes available for editing and the default value is “Upper”;
- channels 36 and 44 in the “Use Limit channels” list changes its color from blue to grey.

If you change the “Channel Bandwidth” parameter to 40 MHz and do not remove the “grey” channels from the list, then when you click “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” = Upper.

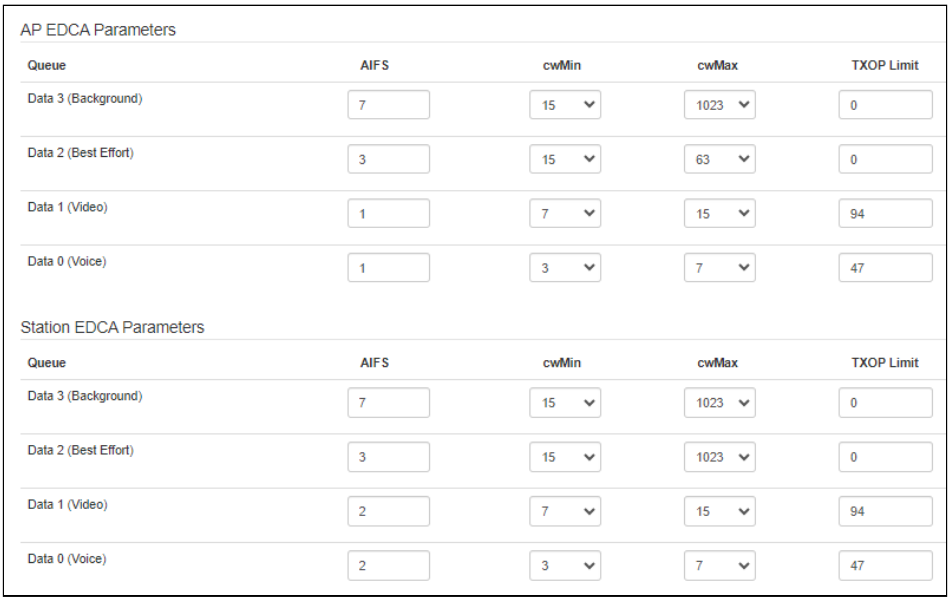
In the “Advanced” section, it is possible to configure advanced radio interface parameters of the device.



- *OBSS Coexistence* — automatic channel bandwidth reduction when the channel is loaded. When the flag is set, the mode is enabled;
- *Fixed Transmit Rate* — fixed wireless data rate, defined by IEEE 802.11a/n/ac specifications;
- *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. The field is available only if the selected operating mode for the radio interface includes 802.11n. When checked, the device transmits one data flow through several antennas. When unchecked, the device does not transmit the same data flow through several antennas;
- *Beacon Interval, ms* — beacon frames transmission period. The frames are sent to detect access points. The parameter takes values from 20 to 2000 ms, by default: 100 ms;
- *Fragmentation Threshold* — frame fragmentation threshold, bytes. The parameter takes values 256–2346, by default: 2346;
- *RTS Threshold* — specifies the number of bytes over which the Request to Send will be sent. Decreasing this value may improve the performance of the access point when there are a lot of connected clients. However this reduces general throughput of wireless network. The parameter takes values from 0 to 2347, by default: 2347;
- *Frame aggregation* — enables support for AMPDU/AMSDU;
- *Short Preamble* — use of the packet short preamble;
- *Broadcast/Multicast Rate Limiting, p/s* — when the flag is set, transmission of broadcast / multicast traffic over the wireless network is restricted. Specify the limit for broadcast traffic in the popup window (p/s);
- *Wi-Fi Multimedia (WMM)* — WMM support activation (Wi-Fi Multimedia);
- *DHCP Snooping Mode* — selection of DHCP option 82 processing policy. Available values for selection:
    - *ignore* — option 82 processing is disabled. Default value;
    - *remove* — access point deletes the value of option 82;
    - *replace* — access point substitutes or replaces the value of option 82. When selecting this value to edit, the following parameters are opened:
        - *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 (-).
- *Enable QoS* — when the flag is set, the setting of Quality of Service functions is available.

The following functions are available for quality assurance configuration:

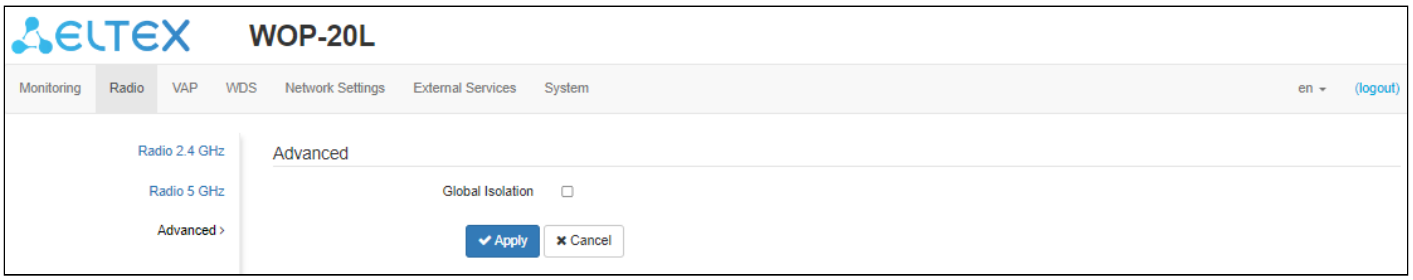


- *AP EDCA parameters* — access point settings table (traffic is transmitted from the access point to the client):
  - *Queue* — predefined queues for various kinds of traffic:
    - *Data 3 (Background)* — low priority queue, high bandwidth (802.1p: cs1, cs2 priorities);
    - *Data 2 (Best Effort)*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

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

4.5.3 The “Advanced” submenu

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



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

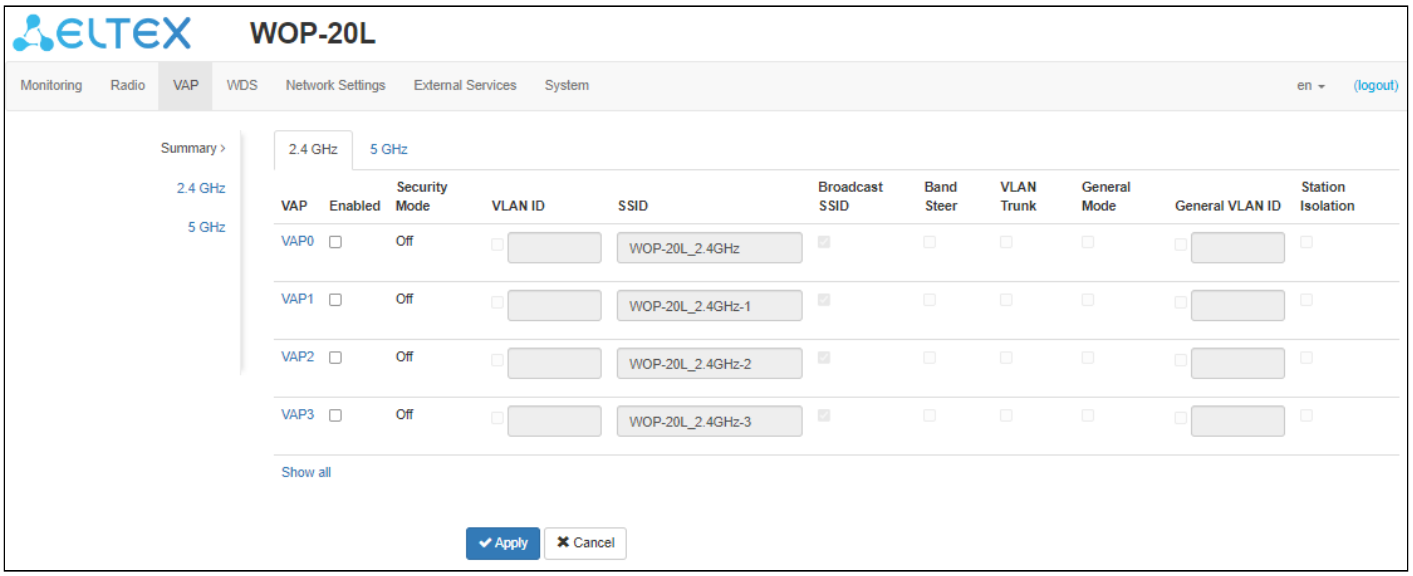
To apply a new configuration and save settings to non-volatile memory, click “Apply”. Click “Cancel” to discard the changes.

4.6 The “VAP” menu

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

4.6.1 The “Summary” submenu

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

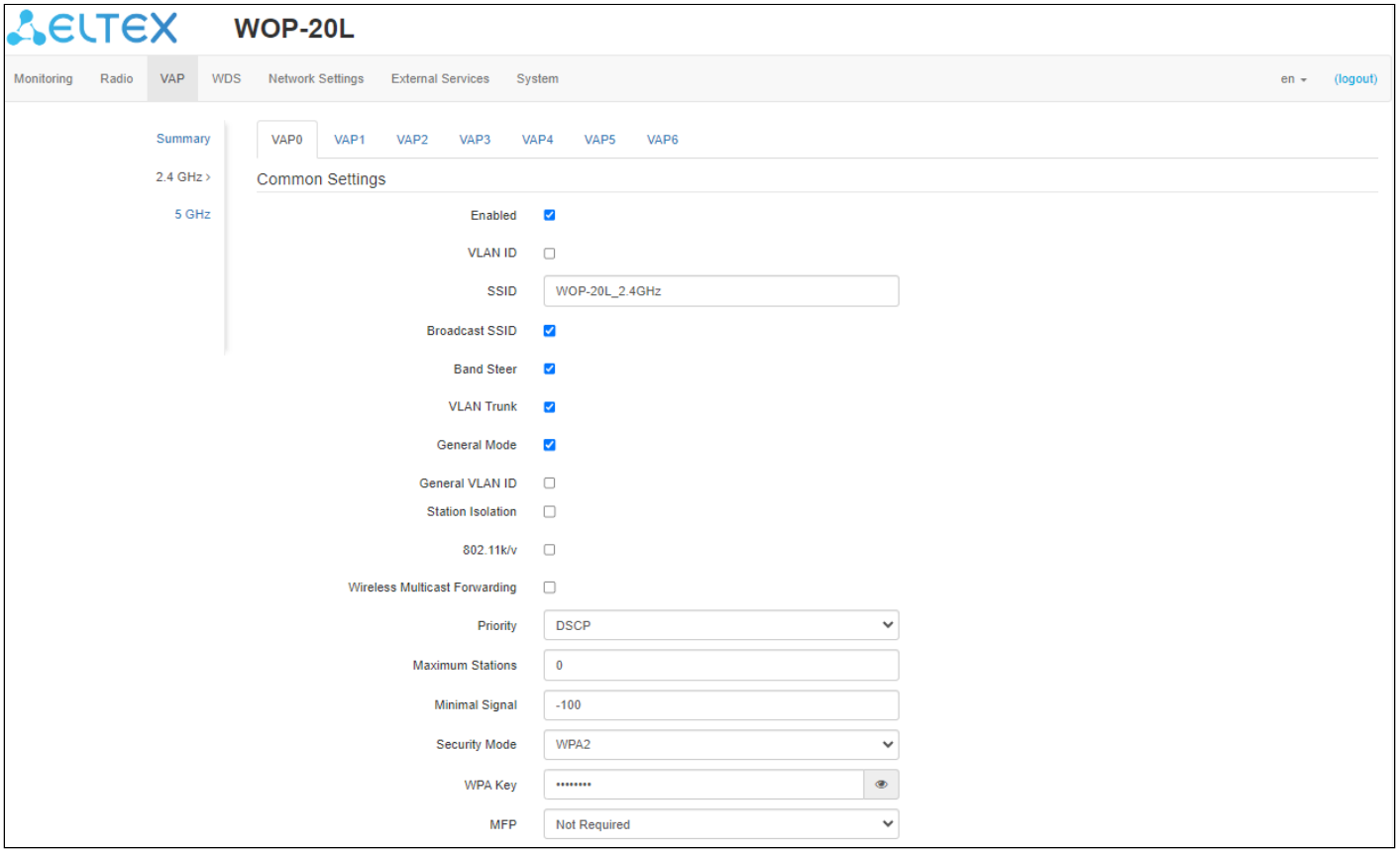


- *VAP0–VAP6* — the sequence number of the virtual access point;
- *Enabled* — when checked, the virtual access point is enabled, otherwise it is disabled;
- *Security Mode* — the type of data encryption used on the virtual access point;
- *VLAN ID* — VLAN number from which the tag will be removed when 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 the flag is set, the priority connection of the client to 5 GHz network is active. In order for this feature to work, it is required to create a VAP with the same SSID on each radio interface and activate the “Band Steer mode” on them;
- *VLAN Trunk* — when the flag is set, tagged traffic is transmitted to the subscriber;
- *General Mode* — when the flag is set, transmission of untagged traffic jointly with tagged traffic is allowed (available when Trunk VLAN mode is enabled);
- *General VLAN ID* — a tag will be removed from the specified VLAN ID and the traffic of this VLAN will pass to the client without a tag. When traffic passes in the opposite direction, untagged traffic will be tagged with General VLAN ID;
- *Station Isolation* — when checked, traffic isolation between clients in the same VAP is enabled.

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

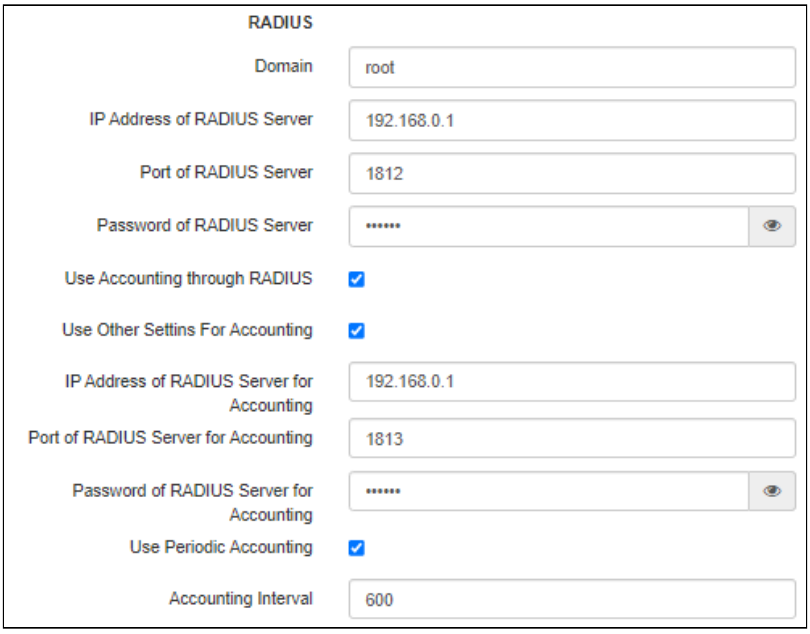
4.6.2 The “VAP” submenu



Common settings

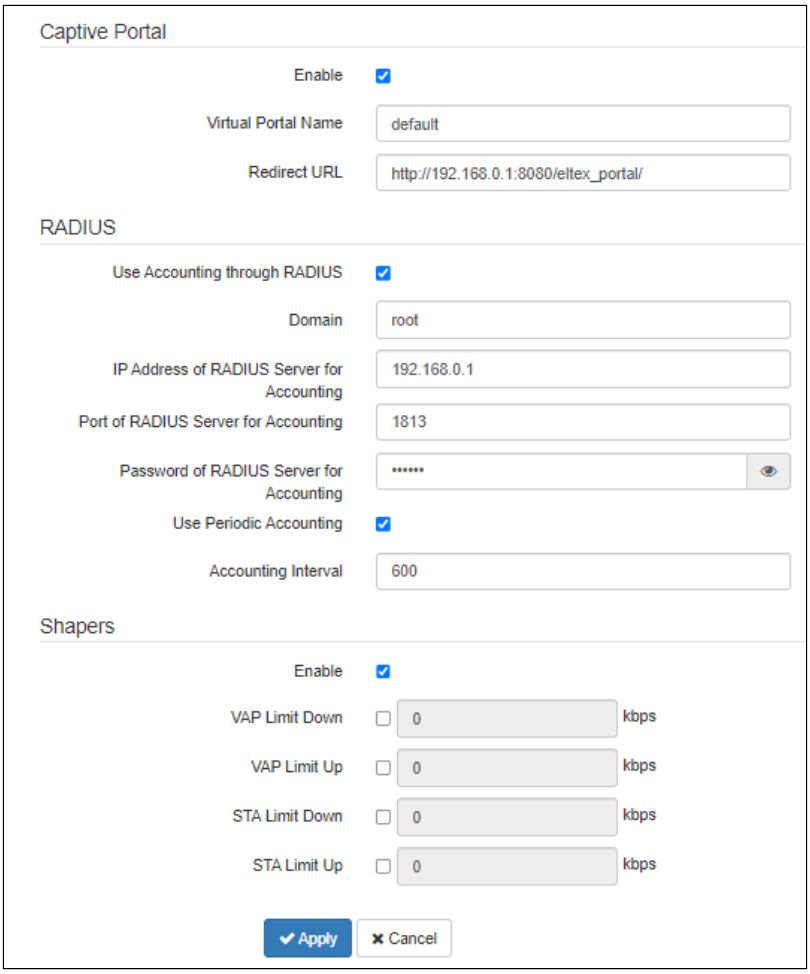
- *Enabled* — when checked, the virtual access point is enabled, otherwise it is disabled;
- *VLAN ID* — VLAN number from which the tag will be removed when transmitting Wi-Fi traffic to clients connected to this VAP. When traffic flows in the opposite direction, untagged traffic from clients will be tagged with VLAN ID (when VLAN Trunk mode is disabled);
- *SSID* — virtual wireless network name;
- *Broadcast SSID* — when checked, SSID broadcasting is on, otherwise it is disabled;
- *Band Steer* — when the flag is set, the priority connection of the client to 5 GHz network is active. In order for this feature to work, it is required to create a VAP with the same SSID on each radio interface and activate the “Band Steer mode” on them;
- *VLAN Trunk* — when the flag is set, tagged traffic is transmitted to the subscriber;
- *General Mode* — when the flag is set, transmission of untagged traffic jointly with tagged traffic is allowed (available when Trunk VLAN mode is enabled);

- *General VLAN ID* — a tag will be removed from the specified VLAN ID and the traffic of this VLAN will pass to the client without a tag. When traffic passes in the opposite direction, untagged traffic will be tagged with General VLAN ID;
- *Station Isolation* — when checked, traffic isolation between clients in the same VAP is enabled;
- *802.11k/v* — enable support for 802.11k/v standards on virtual access point;
- *Wireless Multicast Forwarding* — when the flag is set, traffic towards clients will be converted to Unicast before each client, if it is disabled, it will pass without modifications;
- *Priority* — select prioritization mode. Defines the field on the basis of which the traffic transmitted to the radio interface will be distributed in WMM queues:
    - *DSCP* — will analyze the priority from the DSCP field of the IP packet header;
    - *802.1p* — will analyze the priority from the CoS (Class of Service) field of the tagged packets.
- *Maximum Stations* — the maximum alllowable number of clients connected to the virtual network;
- *Minimal Signal* — signal level in dBm below which the client equipment is disconnected from the virtual network;
- *MFP* — management frame protection (available for WPA2 and WPA2-Enterprise selected security mode, selecting other security modes puts the MFP in the disabled state):
    - *Not required* — management frame protection is disabled;
    - *Capable* — protection works if the client supports MFP. Customers without MFP support can connect to this VAP;
    - *Required* — management frame protection is enabled, clients that do not support MFP cannot connect.
- *Security Mode* — wireless access security mode:
    - *Off* — do not use encryption for data transfer. The access point is available for any subscriber to connect;
    - *WPA, WPA2, WPA/WPA2* — encryption methods, if you select one of the methods, the following setting will be available:
        - *WPA Key* — key/password required to connect to the virtual access point. The length of the key is from 8 to 63 characters.
- *WPA-Enterprise, WPA2-Enterprise, WPA/WPA2-Enterprise* — wireless channel encryption mode, in which the client is authorized on the centralized RADIUS server. To configure this security mode, specify the parameters of the RADIUS server. Also specify a key for the RADIUS server. When selecting one of the these methods, the following setting will be available:



- *Domain* — user domain;
- *IP Address of RADIUS Server* — RADIUS server address;
- *Port of RADIUS Server* — port of the RADIUS server that used for aithentication and authorization;

- *Password of RADIUS Server* — password for the RADIUS server used for authentication and authorization;
- *Use Accounting through RADIUS* — when checked, “Accounting” messages will be sent to the RADIUS server;
- *Use Other Settings For Accounting:*
  - *IP Address of RADIUS Server for Accounting* — address of the RADIUS server, used for accounting;
  - *Password of RADIUS Server for Accounting* — password for the RADIUS server used for accounting.
- *Port of RADIUS Server for Accounting* — port that will be used to collect accounts on the RADIUS server;
- *Use Periodic Accounting* — enable periodic sending of “Accounting” messages to the RADIUS server. The interval for sending messages can be set in the “Accounting Interval” field.



Captive Portal

When selecting one of the following security modes: Off, WPA, WPA2, WPA/WPA2, a portal authorization setting is available on the VAP.

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

RADIUS

- *Use Accounting through RADIUS* — when checked, “Accounting” messages will be sent to the RADIUS server;
- *Domain* — user domain;

- *IP Address of RADIUS Server for Accounting* — address of the RADIUS server, used for accounting;
- *Port of RADIUS Server for Accounting* — port that will be used to collect accounts on the RADIUS server;
- *Password of RADIUS Server for Accounting* — password for the RADIUS server used for accounting;
- *Use Periodic Accounting* — enable periodic sending of “Accounting” messages to the RADIUS server. The interval for sending messages can be set in the “Accounting Interval” field.

Shapers

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

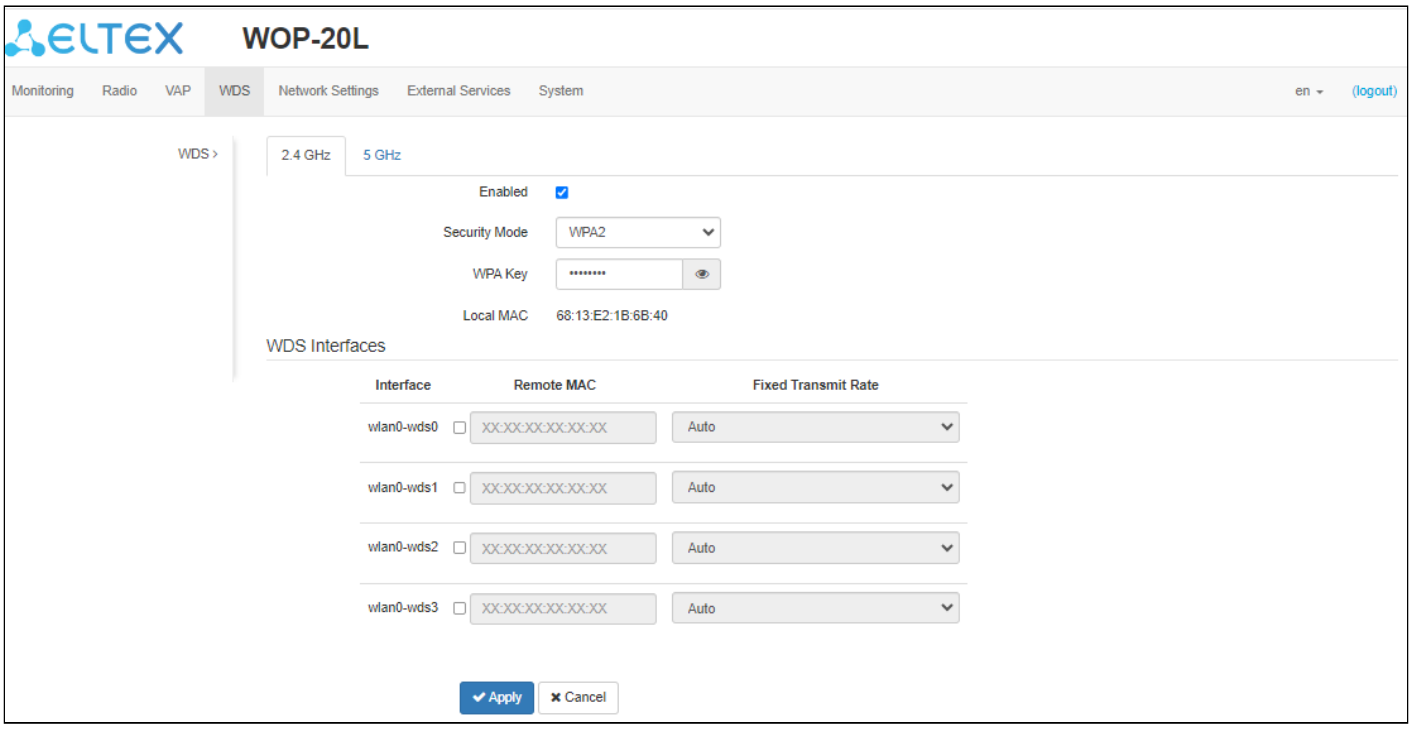
To apply a new configuration and save settings to non-volatile memory, click “Apply”. Click “Cancel” to discard the changes.

4.7 The “WDS” menu

In the "**WDS**" menu, the wireless bridges between WOP-20L 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.

4.7.1 The "WDS" submenu



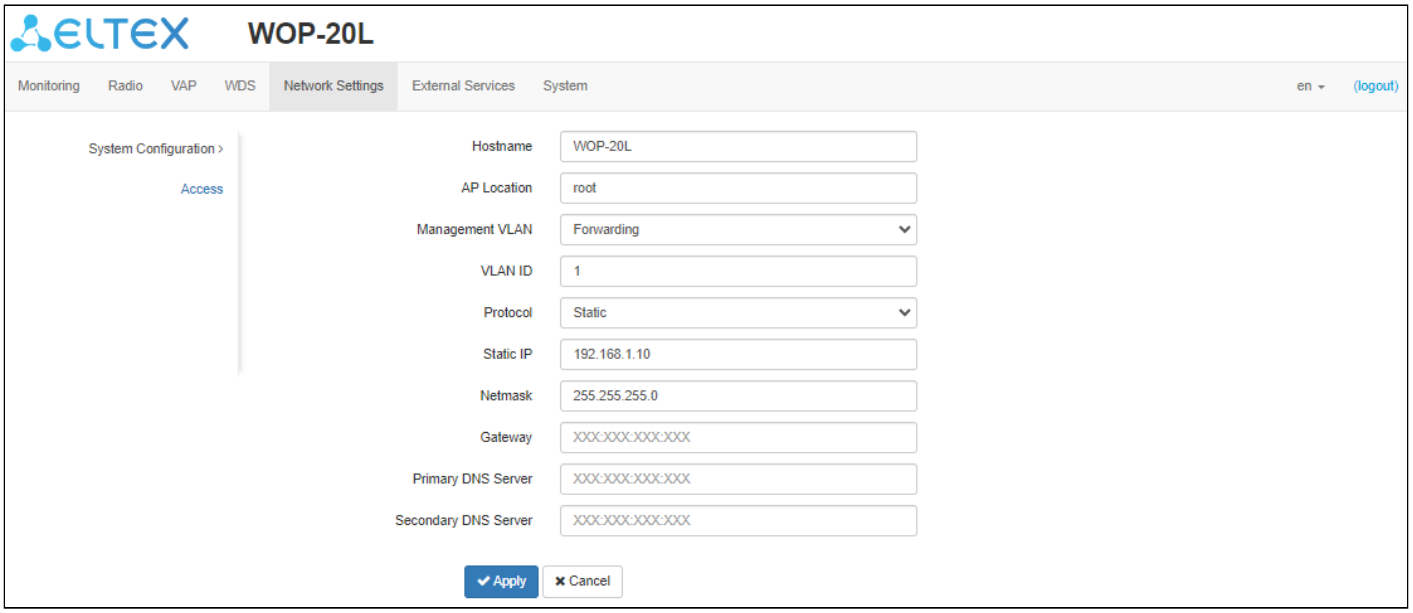
In the "2.4 GHz" and "5 GHz" tabs, select the radio interface of the device on which a wireless bridge should be built.

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

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

4.8 The “Network Settings” menu

4.8.1 The “System Configuration” submenu



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

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

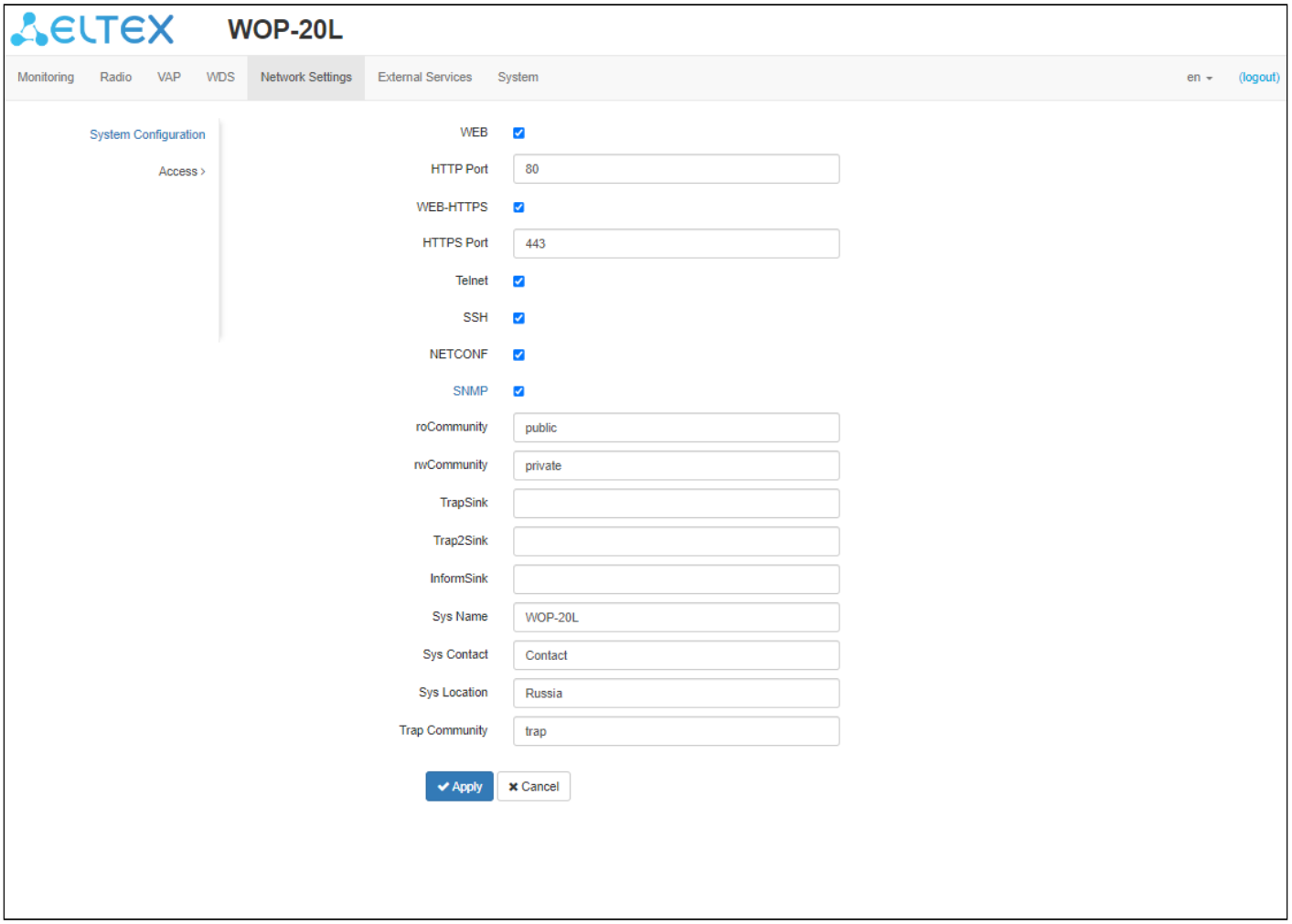
4.8.2 The “Access” submenu

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

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

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

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



The WOP-20L software allows changing the device configuration, monitoring the status of the access point and its sensors, as well as managing the device using the SNMP protocol.

To change the SNMP settings, check the box next to “SNMP”, the following SNMP agent options become available:

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

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

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

where eltexLtd — 1.3.6.1.4.1.35265 is Eltex Enterprise ID.

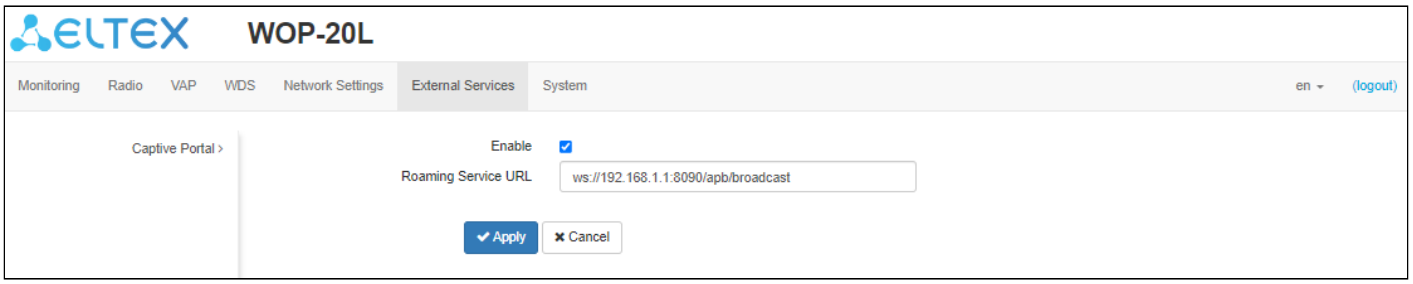
To apply a new configuration and save settings to non-volatile memory, click “Apply”. Click “Cancel” to discard the changes.

4.9 The “External Services” menu

4.9.1 The “Captive Portal” submenu

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

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



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

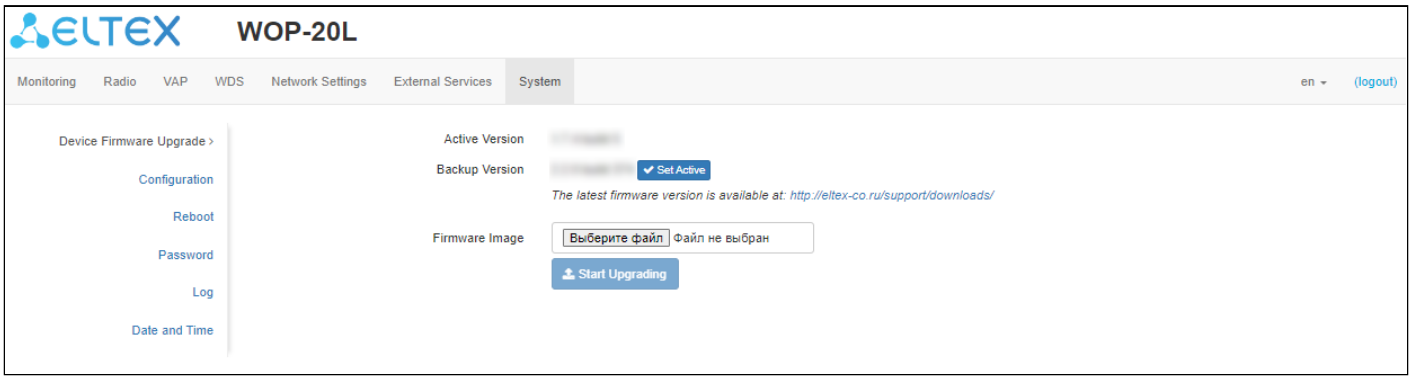
To apply a new configuration and save settings to non-volatile memory, click “Apply”. Click “Cancel” to discard the changes.

4.10 The “System” menu

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

4.10.1 The “Device Firmware Upgrade” submenu

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



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

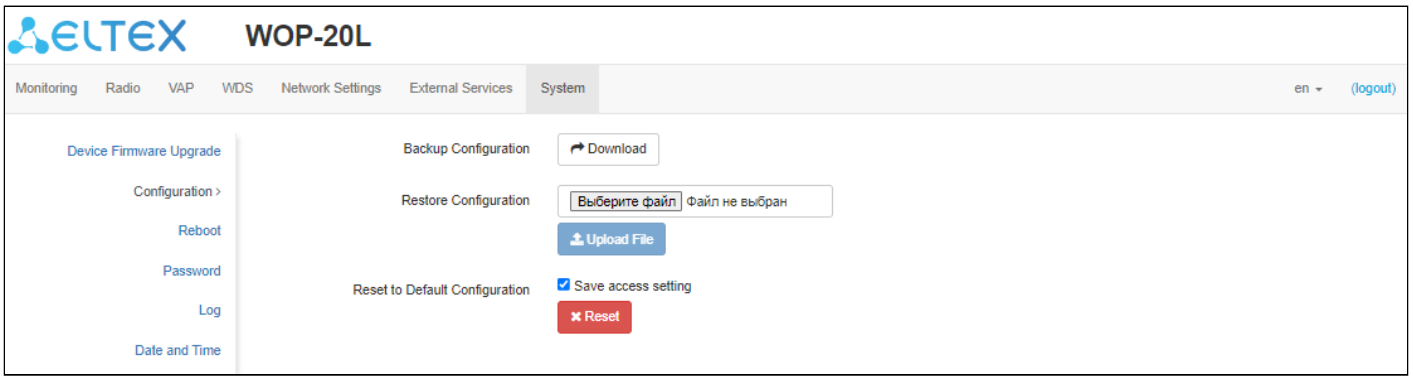
Firmware upgrade

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

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

4.10.2 The “Configuration” submenu

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



Backup Configuration

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

Restore Configuration

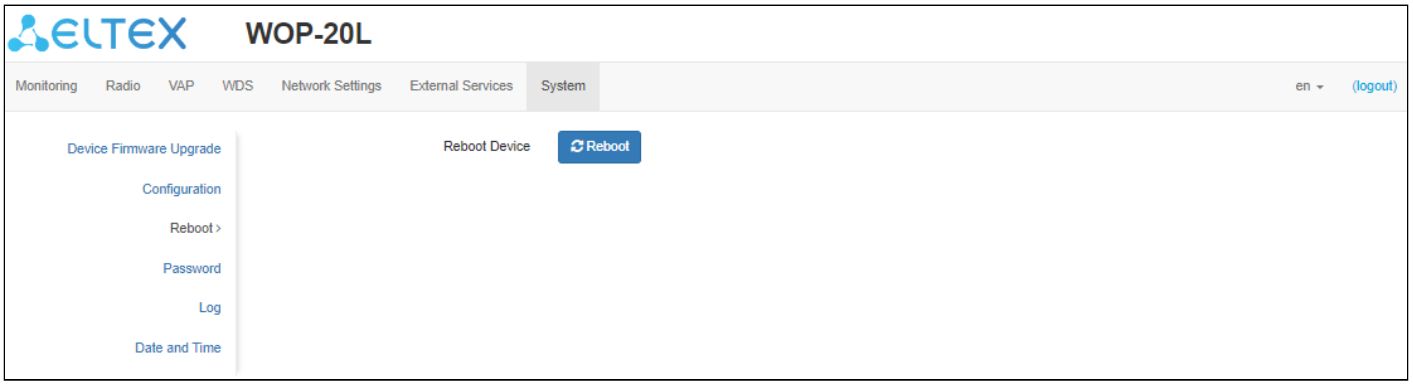
To upload the configuration file saved on the local computer, use the *Restore Configuration* item. To update the device configuration click “Browse”, specify a file (in .tar.gz format) and click “Upload File”. Uploaded configuration will be applied automatically and does not require device reboot.

Reset to Default Configuration

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

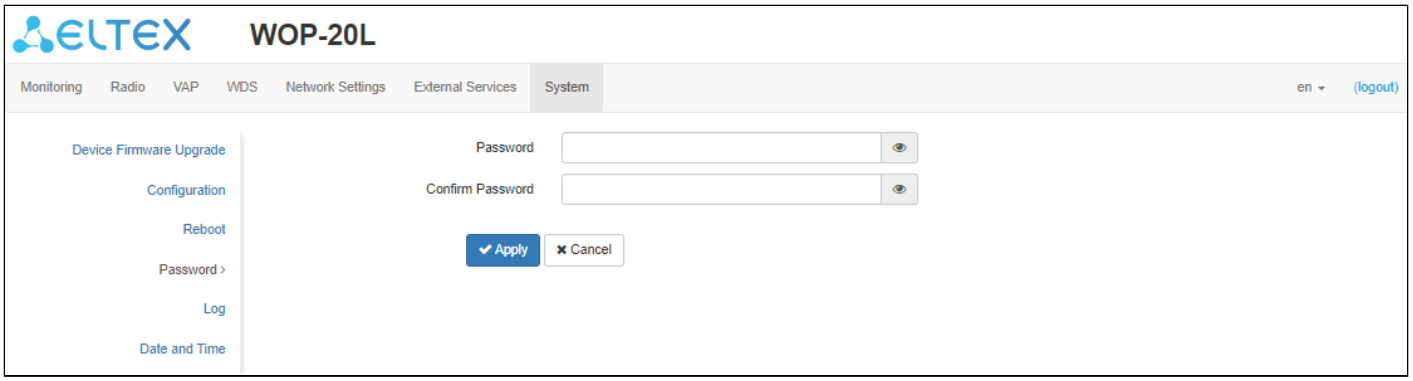
4.10.3 The “Reboot” submenu

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



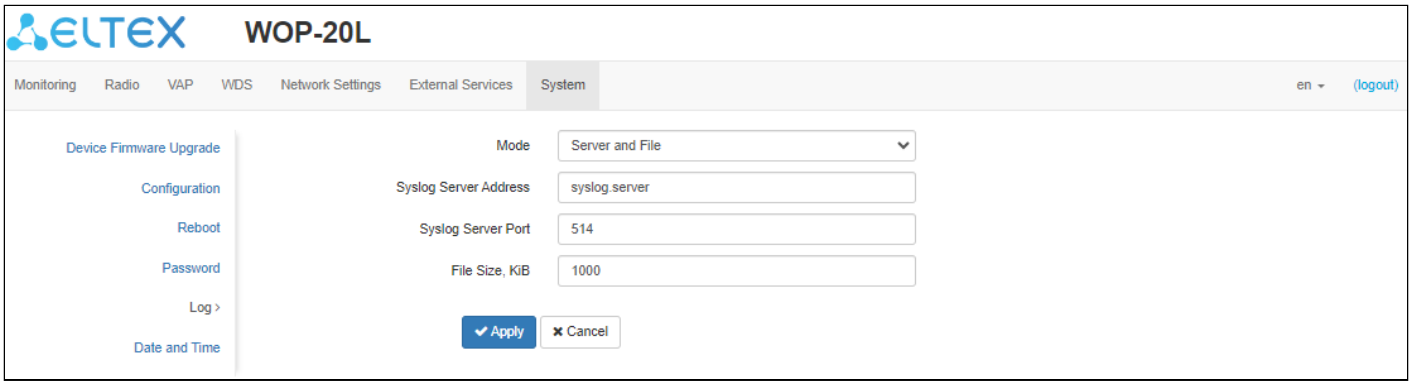
4.10.4 The “Password” submenu

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



4.10.5 The “Log” submenu

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



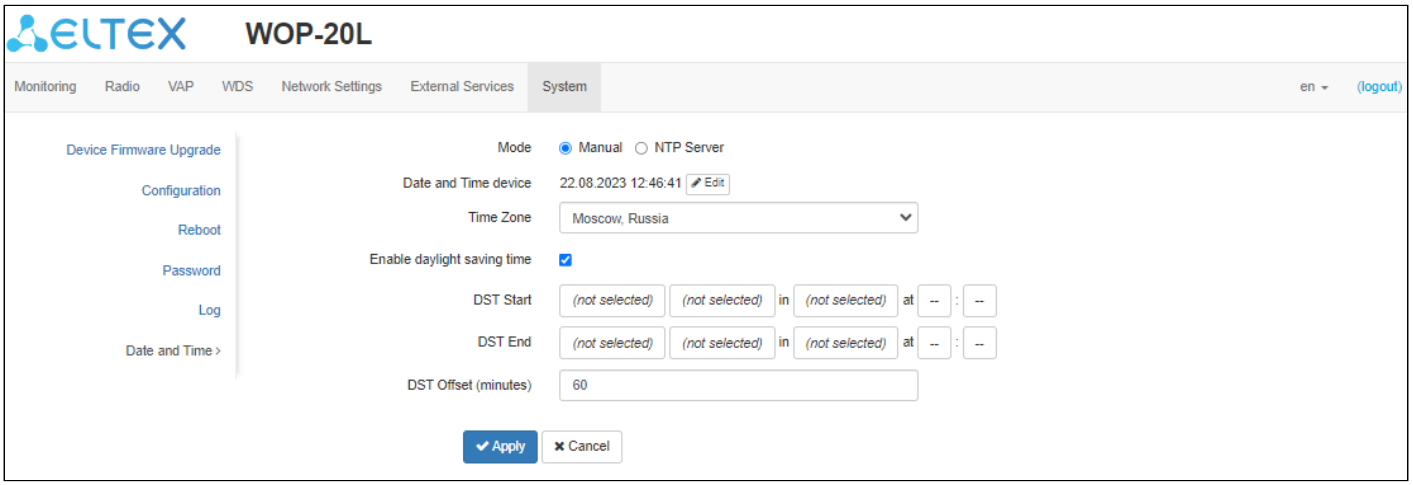
- *Mode* — Syslog agent operation mode:
  - *Local File* — log information is stored in a local file and is available in the device web interface on the Monitoring/Events tab;
  - *Server and File* — log information is sent to a remote Syslog server and stored in a local file.
- *Syslog Server Address*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

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

4.10.6 The “Date and Time” submenu

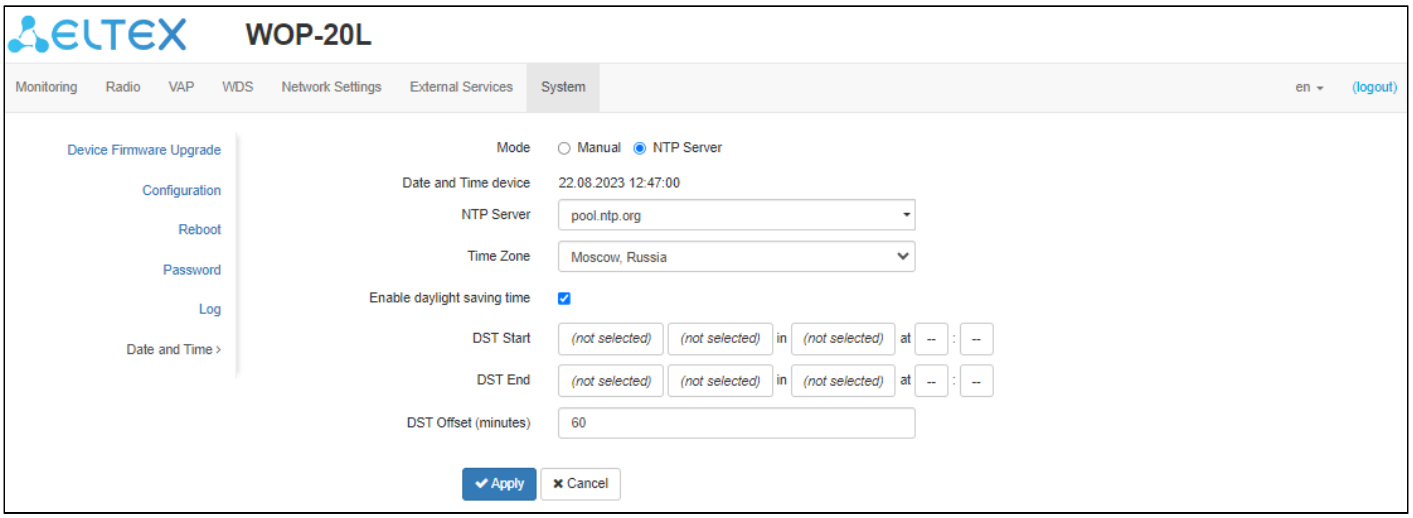
In the **“Date and Time”** submenu, it is possible to set the time manually or using the time synchronization protocol (NTP).

4.10.6.1 Manual



- *Date and Time device* — date and time on the device at the current moment. Click “Edit” to make corrections:
  - *Date, Time* — set the current date and time or click “Set current date and time” to synchronize with the device;
- *Time Zone* — allows to set the timezone according to the nearest city for your region from the list;
- *Enable daylight saving time* — when selected, automatic daylight saving change will be performed automatically within the defined time period:
  - *DST Start* — day and time, when daylight saving time is starting;
  - *DST End* — day and time, when daylight saving time is ending;
  - *DST Offset (minutes)* — time period in minutes, on which time offset is performing. The parameter can take a value from 0 to 720 minutes.

4.10.6.2 NTP server



- *Date and Time device* — date and time set on the device;
- *NTP Server* — IP address/domain name of the time synchronization server. It is possible to specify an address or select from an existing list;
- *Time Zone* — allows to set the time zone according to the nearest city for your region from the list;
- *Enable daylight saving time* — when selected, automatic daylight saving change will be performed automatically within the defined time period:
-
  - *DST Start* — day and time, when daylight saving time is starting;
  - *DST End* — day and time, when daylight saving time is ending;
  - *DST Offset (minutes)* — time period in minutes, on which time offset is performing. The parameter can take a value from 0 to 720 minutes.

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

5 Managing the device using the command line

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

5.1 Connection to the device

By default, WOP-20L 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.

- WOP-20L factory default IP address: **192.168.1.10**, subnet mask: **255.255.255.0**.

Connection to the device is performed via SSH/Telnet:

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

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

5.2 Network parameters configuration

Configuring the static network parameters of the access point

WOP-20L(root):/# **configure**
WOP-20L(config):/# **interface**
WOP-20L(config):/interface# **br0**
WOP-20L(config):/interface/br0# **common**
WOP-20L(config):/interface/br0/common# **static-ip X.X.X.X** (where X.X.X.X — WOP-20L IP address)
WOP-20L(config):/interface/br0/common# **netmask X.X.X.X** (where X.X.X.X — subnet mask)
WOP-20L(config):/interface/br0/common# **dns-server-1 X.X.X.X** (where X.X.X.X — IP address of the DNS server №1)
WOP-20L(config):/interface/br0/common# **dns-server-2 X.X.X.X** (where X.X.X.X — IP address of the DNS server №2)
WOP-20L(config):/interface/br0/common# **protocol static-ip** (change operation mode from DHCP to Static-IP)
WOP-20L(config):/interface/br0/common# **save** (save changes)

Adding a static route

WOP-20L(config):/interface/br0/common# **exit**
WOP-20L(config):/interface/br0# **exit**
WOP-20L(config):/interface# **exit**
WOP-20L(config):/# **route**
WOP-20L(config):/route# **add default** (where default — route name)
WOP-20L(config):/route# **default**
WOP-20L(config):/route/default# **destination X.X.X.X** (where X.X.X.X — IP address of the network or destination node, for default route — 0.0.0.0)
WOP-20L(config):/route/default# **netmask X.X.X.X** (where X.X.X.X — destination network mask, for default route — 0.0.0.0)
WOP-20L(config):/route/default# **gateway X.X.X.X** (where X.X.X.X — gateway IP address)
WOP-20L(config):/route/default# **save** (save changes)

Configuring the reception of network parameters via DHCP

WOP-20L(root):/# **configure**
WOP-20L(config):/# **interface**
WOP-20L(config):/interface# **br0**
WOP-20L(config):/interface/br0# **common**
WOP-20L(config):/interface/br0/common# **protocol dhcp**
WOP-20L(config):/interface/br0/common# **save** (save changes)

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

Untagged access

Obtaining the network parameters via DHCP:

WOP-20L(root):/# **set-management-vlan-mode off protocol dhcp**

Static settings:

WOP-20L(root):/# **set-management-vlan-mode off protocol static-ip ip-addr X.X.X.X netmask Y.Y.Y.Y gateway Z.Z.Z.Z** (where X.X.X.X — static IP address, Y.Y.Y.Y — subnet mask, Z.Z.Z.Z — gateway)

Access via Management VLAN in Terminating mode

Obtaining the network parameters via DHCP:

WOP-20L(root):/# **set-management-vlan-mode terminating vlan-id X protocol dhcp** (where X — VLAN ID, used for access to the device. Acceptable values: 1–4094)

Static settings:

WOP-20L(root):/# **set-management-vlan-mode terminating vlan-id X protocol static-ip ip-addr X.X.X.X netmask Y.Y.Y.Y gateway Z.Z.Z.Z** (where X — VLAN ID, used for access to the device. Acceptable values: 1–4094; X.X.X.X — static IP address; Y.Y.Y.Y — subnet mask; Z.Z.Z.Z — gateway)

Access via Management VLAN in Forwarding mode

Obtaining the network parameters via DHCP:

WOP-20L(root):/# **set-management-vlan-mode forwarding vlan-id X protocol dhcp** (where X — VLAN ID, used for access to the device. Acceptable values: 1–4094)

Static settings:

WOP-20L(root):/# **set-management-vlan-mode forwarding vlan-id X protocol static-ip ip-addr X.X.X.X netmask Y.Y.Y.Y gateway Z.Z.Z.Z** (where X — VLAN ID, used for access to the device. Acceptable values: 1–4094; X.X.X.X — static IP address; Y.Y.Y.Y — subnet mask; Z.Z.Z.Z — gateway)

Completing and saving settings

WOP-20L(root):/# **save** (save changes)

5.2.2 IPv6 network parameters configuration

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

Enabling access to the device via IPv6 protocol

WOP-20L(root):/# **configure**
WOP-20L(config):/# **interface**
WOP-20L(config):/interface# **br0**
WOP-20L(config):/interface/br0# **common**
WOP-20L(config):/interface/br0/common# **ipv6**
WOP-20L(config):/interface/br0/common/ipv6# **protocol dhcp** (obtaining IPv6 network parameters via DHCP)
WOP-20L(config):/interface/br0/common/ipv6# **enabled true** (enabling access to the device via IPv6 protocol. To disable, enter **false**)
WOP-20L(config):/interface/br0/common/ipv6# **save** (save changes)

Configuring static IPv6 network settings for the access point

WOP-20L(root):/# **configure**
WOP-20L(config):/# **interface**
WOP-20L(config):/interface# **br0**
WOP-20L(config):/interface/br0# **common**
WOP-20L(config):/interface/br0/common# **ipv6**
WOP-20L(config):/interface/br0/common/ipv6# **address**
XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX (where XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX — static IPv6 address of WOP-20L)
WOP-20L(config):/interface/br0/common/ipv6# **address-prefix-length X** (where X — static IPv6 address prefix. Takes values from 0 to 128. By default — 64)
WOP-20L(config):/interface/br0/common/ipv6# **gateway XXXX:XXXX:XXXX:XXXX::/64** (IPv6 prefix is specified, for example 3211:0:0:1234::/64)
WOP-20L(config):/interface/br0/common/ipv6# **dns-server-1**
XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX/Y (where XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX/Y — IPv6 address of the DNS server №1 with prefix)
WOP-20L(config):/interface/br0/common/ipv6# **dns-server-2**
XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX/Y (where XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX/Y — IPv6 address of the DNS server №2 with prefix)
WOP-20L(config):/interface/br0/common/ipv6# **protocol static-ip** (enable use of static IPv6 networks parameters. For obtaining the IPv6 network parameters via DHCP enter **dhcp**)
WOP-20L(config):/interface/br0/common/ipv6# **enabled true** (enable access to the device via IPv6 protocol. To disable, enter **false**)
WOP-20L(config):/interface/br0/common/ipv6# **save** (save changes)

Configuring IPv6 access settings

WOP-20L(root):/# **configure**
WOP-20L(config):/# **interface**
WOP-20L(config):/interface# **br0**
WOP-20L(config):/interface/br0# **common**
WOP-20L(config):/interface/br0/common# **ipv6**
WOP-20L(config):/interface/br0/common/ipv6# **access-rules** (go to the section of access settings)
WOP-20L(config):/interface/br0/common/ipv6/access-rules# **telnet false** (where false — restriction of access via the TELNET protocol to the device by its IPv6 address. This setting applies only to connection to the device via IPv6, access via IPv4 will remain if the corresponding prohibition setting has not been made in the section for IPv4. To remove the restriction, enter **true**)
WOP-20L(config):/interface/br0/common/ipv6/access-rules# **save** (save changes)

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

5.3 Virtual Wi-Fi access points (VAP) configuration

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

Table 6 — Commands for configuring security mode on VAP

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

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

5.3.1 Configuration of VAP without encryption

Creating a VAP without encryption

```
WOP-20L(root):/# configure
WOP-20L(config):/# interface
WOP-20L(config):/interface# wlan1-va0
WOP-20L(config):/interface/wlan1-va0# vap
WOP-20L(config):/interface/wlan1-va0/vap# ssid 'SSID_WOP-20L_open' (change SSID name)
WOP-20L(config):/interface/wlan1-va0/vap# security-mode off (encryption mode off — no password)
WOP-20L(config):/interface/wlan1-va0/vap# exit
WOP-20L(config):/interface/wlan1-va0# common
WOP-20L(config):/interface/wlan1-va0/common# enabled true (enable VAP)
WOP-20L(config):/interface/wlan1-va0/common# save (save changes)
```

5.3.2 Configuration of VAP with WPA-Personal security mode

Creating a VAP with WPA-Personal security mode

WOP-20L(root):/# **configure**
WOP-20L(config):/# **interface**
WOP-20L(config):/interface# **wlan1-va0**
WOP-20L(config):/interface/wlan1-va0# **vap**
WOP-20L(config):/interface/wlan1-va0/vap# **ssid 'SSID_WOP-20L_Wpa2'** (change SSID name)
WOP-20L(config):/interface/wlan1-va0/vap# **security-mode WPA_WPA2** (encryption mode — WPA/WPA2)
WOP-20L(config):/interface/wlan1-va0/vap# **key-wpa password123** (key/password required to connect to the virtual access point. The key should be between 8 and 63 characters long)
WOP-20L(config):/interface/wlan1-va0/vap# **exit**
WOP-20L(config):/interface/wlan1-va0# **common**
WOP-20L(config):/interface/wlan1-va0/common# **enabled true** (enable VAP)
WOP-20L(config):/interface/wlan1-va0/common# **save** (save changes)

5.3.3 Configuration of VAP with Enterprise authorization

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

WOP-20L(root):/# **configure**
WOP-20L(config):/# **interface**
WOP-20L(config):/interface# **wlan1-va0**
WOP-20L(config):/interface/wlan1-va0# **vap**
WOP-20L(config):/interface/wlan1-va0/vap# **ssid 'SSID_WOP-20L_enterprise'** (change SSID name)
WOP-20L(config):/interface/wlan1-va0/vap# **security-mode WPA_WPA2_1X** (encryption mode — WPA/WPA2-Enterprise)
WOP-20L(config):/interface/wlan1-va0/vap# **radius**
WOP-20L(config):/interface/wlan1-va0/vap/radius# **domain root** (where root — user domain)
WOP-20L(config):/interface/wlan1-va0/vap/radius# **auth-address X.X.X.X** (where X.X.X.X — IP address of RADIUS server)
WOP-20L(config):/interface/wlan1-va0/vap/radius# **auth-port X** (where X — port of RADIUS server used for authentication and authorization. By default: 1812)
WOP-20L(config):/interface/wlan1-va0/vap/radius# **auth-password secret** (where secret — password for RADIUS server used for authentication and authorization)
WOP-20L(config):/interface/wlan1-va0/vap/radius# **acct-enable true** (enable sending of "Accounting" messages to the RADIUS server. By default: **false**)
WOP-20L(config):/interface/wlan1-va0/vap/radius# **acct-address X.X.X.X** (where X.X.X.X — IP address of RADIUS server used for accounting)
WOP-20L(config):/interface/wlan1-va0/vap/radius# **acct-password secret** (where secret — password for RADIUS server used for accounting)
WOP-20L(config):/interface/wlan1-va0/vap/radius# **acct-periodic true** (enable periodic sending of "Accounting" messages to the RADIUS server. By default: **false**)
WOP-20L(config):/interface/wlan1-va0/vap/radius# **acct-interval 600** (interval for sending "Accounting" messages to the RADIUS server)
WOP-20L(config):/interface/wlan1-va0/vap# **exit**
WOP-20L(config):/interface/wlan1-va0# **common**
WOP-20L(config):/interface/wlan1-va0/common# **enabled true** (enable VAP)
WOP-20L(config):/interface/wlan1-va0/common# **save** (save changes)

5.3.4 Configuration of VAP with Captive Portal

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

WOP-20L(root):/# **configure**
WOP-20L(config):/# **interface**
WOP-20L(config):/interface# **wlan1-va0**
WOP-20L(config):/interface/wlan1-va0# **vap**
WOP-20L(config):/interface/wlan1-va0/vap# **vlan-id X** (where X — VLAN ID on VAP)
WOP-20L(config):/interface/wlan1-va0/vap# **security-mode off** (encryption mode off — no password)
WOP-20L(config):/interface/wlan1-va0/vap# **ssid 'Portal_WOP-20L'** (change SSID name)
WOP-20L(config):/interface/wlan1-va0/vap# **captive-portal**
WOP-20L(config):/interface/wlan1-va0/vap/captive-portal# **scenarios**
WOP-20L(config):/interface/wlan1-va0/vap/captive-portal/scenarios# **scenario-redirect**
WOP-20L(config):/interface/wlan1-va0/vap/captive-portal/scenarios/scenario-redirect# **redirect-url http://<IP>:<PORT>/eltex_portal/** (specify URL of virtual portal)
WOP-20L(config):/interface/wlan1-va0/vap/captive-portal/scenarios/scenario-redirect# **index 1**
WOP-20L(config):/interface/wlan1-va0/vap/captive-portal/scenarios/scenario-redirect# **virtual-portal-name default** (specify portal name. By default: **default**)
WOP-20L(config):/interface/wlan1-va0/vap/captive-portal/scenarios/scenario-redirect# **exit**
WOP-20L(config):/interface/wlan1-va0/vap/captive-portal/scenarios# **exit**
WOP-20L(config):/interface/wlan1-va0/vap/captive-portal# **enabled true**
WOP-20L(config):/interface/wlan1-va0/vap/captive-portal# **exit**
WOP-20L(config):/interface/wlan1-va0/vap# **radius**
WOP-20L(config):/interface/wlan1-va0/vap/radius# **domain root** (where root — user domain)
WOP-20L(config):/interface/wlan1-va0/vap/radius# **acct-enable true** (enable sending of "Accounting" messages to the RADIUS server. By default: **false**)
WOP-20L(config):/interface/wlan1-va0/vap/radius# **acct-address X.X.X.X** (where X.X.X.X — IP address of RADIUS server used for accounting)
WOP-20L(config):/interface/wlan1-va0/vap/radius# **acct-password secret** (where secret — password for RADIUS server used for accounting)
WOP-20L(config):/interface/wlan1-va0/vap/radius# **acct-periodic true** (enable periodic sending of "Accounting" messages to the RADIUS server. By default: **false**)
WOP-20L(config):/interface/wlan1-va0/vap/radius# **acct-interval 600** (interval for sending "Accounting" messages to the RADIUS server)
WOP-20L(config):/interface/wlan1-va0/vap# **exit**
WOP-20L(config):/interface/wlan1-va0# **common**
WOP-20L(config):/interface/wlan1-va0/common# **enabled true** (enable VAP)
WOP-20L(config):/interface/wlan1-va0/common# **save** (save changes)

5.3.5 Advanced VAP settings

Assigning VLAN ID on VAP

WOP-20L(config):/interface/wlan1-va0/vap# **vlan-id X** (where X — VLAN ID number on VAP)

Enabling Band Steer mode

WOP-20L(config):/interface/wlan1-va0/vap# **band-steer-mode true** (enabling Band Steer mode. To disable, enter **false**)

Enabling VLAN trunk on VAP

WOP-20L(config):/interface/wlan1-va0/vap# **vlan-trunk true** (enabling VLAN trunk on VAP. To disable, enter **false**)

Enabling General VLAN on VAP

WOP-20L(config):/interface/wlan1-va0/vap# **general-vlan-mode true** (enabling General VLAN on SSID. To disable, enter **false**)
WOP-20L(config):/interface/wlan1-va0/vap# **general-vlan-id X** (where X — General VLAN number)

Selecting the prioritization method

WOP-20L(config):/interface/wlan1-va0/vap# **priority-by-dscp false** (priority analysis from CoS field (Class of Service) of the tagged packets. Value by default: **true**. In this case, the priority from DSCP header field of the IP packet is analyzed)

Enabling MFP (802.11W)

WOP-20L(config):/interface/wlan1-va0/vap# **mfp required** (enable management frame protection. **required** — requires MFP support from client, clients without an MFP support will not be able to connect. **capable** — compatible with MFP, clients without an MFP support can connect. To disable, enter **off**)

Enabling use of TLS at authorization

WOP-20L(config):/interface/wlan1-va0/vap/radius# **tls-enable true** (use TLS for authorization process. To disable, enter **false**)

Enabling hidden SSID

WOP-20L(config):/interface/wlan1-va0/vap# **hidden true** (enabling hidden SSID. To disable, enter **false**)

Enabling client isolation on VAP

WOP-20L(config):/interface/wlan1-va0/vap# **station-isolation true** (enable traffic isolation between clients within a single VAP. To disable, enter **false**)

Client limitation on VAP

WOP-20L(config):/interface/wlan1-va0/vap# **sta-limit X** (where X — the maximum allowable number of clients connected to the virtual network)

Enabling multicast replication on VAP

WOP-20L(config):/interface/wlan1-va0/vap# **wmf-bss-enable true** (enable multicast traffic replication on VAP. To disable, enter **false**)

Enabling Minimal Signal

WOP-20L(config):/interface/wlan1-va0/vap# **minimal-signal -X** (where X — RSSI threshold, when reached, the point will disconnect the client from the VAP. The parameter can take values from -100 to 0)

Enabling subscribers traffic transmission outside of GRE tunnel

WOP-20L(config):/interface/wlan1-va0/vap# **local-switching true** (enabling subscribers traffic transmission outside of GRE tunnel. To disable, enter **false**. By default: disabled)

Configuring speed limit

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

WOP-20L(config):/interface/wlan1-va0/vap# **shaper-per-sta-rx**
WOP-20L(config):/interface/wlan1-va0/vap/shaper-per-sta-rx# **value X** (where X — maximum speed in Kbps)
WOP-20L(config):/interface/wlan1-va0/vap/shaper-per-sta-rx# **mode kbps** (enabling shaper. To disable, enter **off**)
WOP-20L(config):/interface/wlan1-va0/vap/shaper-per-sta-rx# **exit**
WOP-20L(config):/interface/wlan1-va0/vap# **save** (save changes)

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

WOP-20L(config):/interface/wlan1-va0/vap# **shaper-per-sta-tx**
WOP-20L(config):/interface/wlan1-va0/vap/shaper-per-sta-tx# **value X** (where X — maximum speed in Kbps)
WOP-20L(config):/interface/wlan1-va0/vap/shaper-per-sta-tx# **mode kbps** (enabling shaper. To disable, enter **off**)
WOP-20L(config):/interface/wlan1-va0/vap/shaper-per-sta-tx# **exit**
WOP-20L(config):/interface/wlan1-va0/vap# **save** (save changes)

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

WOP-20L(config):/interface/wlan1-va0/vap# **shaper-per-vap-rx**
WOP-20L(config):/interface/wlan1-va0/vap/shaper-per-vap-rx# **value X** (where X — maximum speed in Kbps)
WOP-20L(config):/interface/wlan1-va0/vap/shaper-per-vap-rx# **mode kbps** (enabling shaper. To disable, enter **off**)
WOP-20L(config):/interface/wlan1-va0/vap/shaper-per-vap-rx# **exit**
WOP-20L(config):/interface/wlan1-va0/vap# **save** (save changes)

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

WOP-20L(config):/interface/wlan1-va0/vap# **shaper-per-vap-tx**
WOP-20L(config):/interface/wlan1-va0/vap/shaper-per-vap-tx# **value X** (where X — maximum speed in Kbps)
WOP-20L(config):/interface/wlan1-va0/vap/shaper-per-vap-tx# **mode kbps** (enabling shaper. To disable, enter **off**)
WOP-20L(config):/interface/wlan1-va0/vap/shaper-per-vap-tx# **exit**
WOP-20L(config):/interface/wlan1-va0/vap# **save** (save changes)

802.11r configuration

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

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

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

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

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

Configuring 802.11r on AP1

WOP-20L(config):/interface/wlan1-va0/vap/ft-config# **enabled false**
WOP-20L(config):/interface/wlan1-va0/vap/ft-config# **r1-key-holder-id E8:28:C1:FC:D6:80** (MAC address of the VAP. Can be viewed in the **ifconfig** command output)
WOP-20L(config):/interface/wlan1-va0/vap/ft-config# **r0-key-holder-id 12345** (unique key for this VAP)
WOP-20L(config):/interface/wlan1-va0/vap/ft-config# **mobility-domain 100** (domain should match on remote VAPs)
WOP-20L(config):/interface/wlan1-va0/vap/ft-config# **mac**
WOP-20L(config):/interface/wlan1-va0/vap/ft-config/mac# **add E4:5A:D4:E2:C4:B0** (MAC address of VAP interface of remote access point — AP2)
WOP-20L(config):/interface/wlan1-va0/vap/ft-config/mac# **E4:5A:D4:E2:C4:B0**
WOP-20L(config):/interface/wlan1-va0/vap/ft-config/mac/E4:5A:D4:E2:C4:B0# **r0-kh-id 23456** (unique key of remote VAP access point AP2 — r0-key-holder-id)
WOP-20L(config):/interface/wlan1-va0/vap/ft-config/mac/E4:5A:D4:E2:C4:B0# **r1-kh-id E4:5A:D4:E2:C4:B0** (MAC address of remote VAP on AP2)
WOP-20L(config):/interface/wlan1-va0/vap/ft-config/mac/E4:5A:D4:E2:C4:B0# **r0-kh-key 0102030405060708** (random key. It shouldn't match with r1-kh-key of AP1, but it should match with r1-kh-key of remote AP2)
WOP-20L(config):/interface/wlan1-va0/vap/ft-config/mac/E4:5A:D4:E2:C4:B0# **r1-kh-key 0001020304050607** (random key. It shouldn't match with r0-kh-key of AP1, but it should match with r0-kh-key of remote AP2)
WOP-20L(config):/interface/wlan1-va0/vap/ft-config/mac/E4:5A:D4:E2:C4:B0# **exit**
WOP-20L(config):/interface/wlan1-va0/vap/ft-config/mac# **exit**
WOP-20L(config):/interface/wlan1-va0/vap/ft-config# **enabled true** (enable access point operation by 802.11r protocol)
WOP-20L(config):/interface/wlan1-va0/vap/ft-config# **save** (save changes)

Configuring 802.11r on AP2

WOP-20L(config):/interface/wlan1-va0/vap/ft-config# **enabled false**
WOP-20L(config):/interface/wlan1-va0/vap/ft-config# **r1-key-holder-id E4:5A:D4:E2:C4:B0** (MAC address of the VAP. Can be viewed in the **ifconfig** command output)
WOP-20L(config):/interface/wlan1-va0/vap/ft-config# **r0-key-holder-id 23456** (unique key for this VAP)
WOP-20L(config):/interface/wlan1-va0/vap/ft-config# **mobility-domain 100** (domain should match on remote VAPs)
WOP-20L(config):/interface/wlan1-va0/vap/ft-config# **mac**
WOP-20L(config):/interface/wlan1-va0/vap/ft-config/mac# **add E8:28:C1:FC:D6:80** (MAC address of VAP interface of remote access point — AP1)
WOP-20L(config):/interface/wlan1-va0/vap/ft-config/mac# **E8:28:C1:FC:D6:80**
WOP-20L(config):/interface/wlan1-va0/vap/ft-config/mac/E8:28:C1:FC:D6:80# **r0-kh-id 12345** (unique key of remote VAP access point AP1 — r0-key-holder-id)
WOP-20L(config):/interface/wlan1-va0/vap/ft-config/mac/E8:28:C1:FC:D6:80# **r1-kh-id E8:28:C1:FC:D6:80** (MAC address of remote VAP on AP1)
WOP-20L(config):/interface/wlan1-va0/vap/ft-config/mac/E8:28:C1:FC:D6:80# **r0-kh-key 0001020304050607** (random key. It shouldn't match with r1-kh-key of AP2, but it should match with r1-kh-key of remote AP1)
WOP-20L(config):/interface/wlan1-va0/vap/ft-config/mac/E8:28:C1:FC:D6:80# **r1-kh-key 01020304050607 08** (random key. It shouldn't match with r0-kh-key of AP2, but it should match with r0-kh-key of remote AP1)
WOP-20L(config):/interface/wlan1-va0/vap/ft-config/mac/E8:28:C1:FC:D6:80# **exit**
WOP-20L(config):/interface/wlan1-va0/vap/ft-config/mac# **exit**
WOP-20L(config):/interface/wlan1-va0/vap/ft-config# **enabled true** (enable access point operation by 802.11r protocol)
WOP-20L(config):/interface/wlan1-va0/vap/ft-config# **save** (save changes)

802.11k configuration

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

The use of 802.11k allows to reduce the time for finding another network when roaming, since the client does not need to scan channels on which there are no target access points available for switching.

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

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

802.11k configuring

WOP-20L(config):/interface/wlan1-va0/vap/w80211kv-config# **enabled false**
WOP-20L(config):/interface/wlan1-va0/vap/w80211kv-config# **mac**
WOP-20L(config):/interface/wlan1-va0/vap/w80211kv-config/mac# **add E8:28:C1:FC:D6:90** (where E8:28:C1:FC:D6:90 — MAC address of “friendly” access point)
WOP-20L(config):/interface/wlan1-va0/vap/w80211kv-config/mac# **E8:28:C1:FC:D6:90**
WOP-20L(config):/interface/wlan1-va0/vap/w80211kv-config/mac/E8:28:C1:FC:D6:90# **channel 132** (where 132 — channel on which access point with E8:28:C1:FC:D6:90 MAC address operates)
WOP-20L(config):/interface/wlan1-va0/vap/w80211kv-config/mac/E8:28:C1:FC:D6:90# **exit**
WOP-20L(config):/interface/wlan1-va0/vap/w80211kv-config/mac# **add E8:28:C1:FC:D6:70** (where E8:28:C1:FC:D6:70 — MAC address of “friendly” access point)
WOP-20L(config):/interface/wlan1-va0/vap/w80211kv-config/mac# **E8:28:C1:FC:D6:70**
WOP-20L(config):/interface/wlan1-va0/vap/w80211kv-config/mac/E8:28:C1:FC:D6:70# **channel 36** (where 36 — channel on which access point with E8:28:C1:FC:D6:70 MAC address operates)
WOP-20L(config):/interface/wlan1-va0/vap/w80211kv-config/mac/E8:28:C1:FC:D6:70# **exit**
WOP-20L(config):/interface/wlan1-va0/vap/w80211kv-config/mac# **exit**
WOP-20L(config):/interface/wlan1-va0/vap/w80211kv-config# **enabled true** (enabling access point operation via 802.11k protocol)
WOP-20L(config):/interface/wlan1-va0/vap/w80211kv-config# **save** (save changes)

5.4 Radio configuration

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

Change of operation channel and radio interface power

WOP-20L(root):/# **configure**
WOP-20L(config):/# **interface**
WOP-20L(config):/interface# **wlan0**
WOP-20L(config):/interface/wlan0# **wlan**
WOP-20L(config):/interface/wlan0/wlan# **radio-2g** (for wlan1 the section is called radio-5g)
WOP-20L(config):/interface/wlan0/wlan/radio-2g# **channel X** (where X is the number of the static channel on which the point will operate)
WOP-20L(config):/interface/wlan0/wlan/radio-2g# **auto-channel false** (disabling Auto Channel. To enable, enter **true**)
WOP-20L(config):/interface/wlan0/wlan/radio-2g# **use-limit-channels false** (disabling Use Limit Channels. To enable, enter **true**)
WOP-20L(config):/interface/wlan0/wlan/radio-2g# **bandwidth X** (where X — channel bandwidth. Parameter can take the following value: for Radio 1: 20, 40; Radio 2: 20, 40, 80)
WOP-20L(config):/interface/wlan0/wlan/radio-2g# **tx-power X** (where X — power level, dBm. Parameter can take the following value: for Radio 1: 8–16 dBm; for Radio 2: 11–19 dBm)
WOP-20L(config):/interface/wlan0/wlan/radio-2g# **save** (save changes)

Lists of available channels

Channels available for selection for radio 2.4 GHz :

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

Channels available for selection for radio 5 GHz:

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

5.4.1 Advanced Radio settings

Configuring a limited list of channels

WOP-20L(config):/interface/wlan0/wlan/radio-2g# **use-limit-channels true** (enabling use of limited list of channels in channel autoselection operation. To disable, enter **false**)
WOP-20L(config):/interface/wlan0/wlan/radio-2g# **limit-channels '1 6 11'** (where 1, 6, 11 — are channels of range in which the configurable radio interface can operate)

Changing the primary channel

WOP-20L(config):/interface/wlan0/wlan/radio-2g# **control-sideband lower** (parameter may take values: lower, upper. By default: for Radio 1: lower; for Radio 2: upper)

Enabling the use of Short Guard Interval

WOP-20L(config):/interface/wlan0/wlan/radio-2g# **sgi true** (enabling the use of a Short Guard Interval for data transmission of 400 ns instead of 800 ns. To disable, enter **false)**

Enabling STBC

WOP-20L(config):/interface/wlan0/wlan/radio-2g# **stbc true** (enabling the Space-Time Block Coding (STBC) method, aimed at improving the reliability of data transmission. To disable, enter **false)**

Enabling aggregation

WOP-20L(config):/interface/wlan0/wlan/radio-2g# **aggregation true** (enabling aggregation on Radio — support for AMPDU/AMSDU. To disable, enter **false**)

Enabling the short preamble

WOP-20L(config):/interface/wlan0/wlan/radio-2g# **short-preamble true** (enabling the short packet preamble. To disable, enter **false**)

Enabling the Wi-Fi Multimedia (WMM)

WOP-20L(config):/interface/wlan0/wlan/radio-2g# **wmm true** (enabling the support for WMM (Wi-Fi Multimedia). To disable, enter **false**)

Configuring DFS mechanism

Configuring is done only on Radio 5 GHz (wlan1)

WOP-20L(config):/interface/wlan1/wlan/radio-5g# **dfs X** (where X — DFS mechanism operating mode. Possible values: **forced** — the mechanism is disabled, DFS channels are available for selection; **auto** — the mechanism is enabled; **disabled** — the mechanism is disabled, DFS channels are unavailable for selection)

Enabling automatic channel width switch mode

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

Enabling Broadcast/Multicast shaper

WOP-20L(config):/interface/wlan0/wlan/radio-2g# **tx-broadcast-limit X** (where X — restricting broadcast/multicast traffic over a wireless network, the limit for broadcast traffic is specified, packets/s)

Enabling QoS and parameter changes

WOP-20L(config):/interface/wlan0/wlan/radio-2g# **qos**
WOP-20L(config):/interface/wlan0/wlan/radio-2g/qos# **enable true** (enabling the use of Quality of Service functions. To disable, enter **false**)
WOP-20L(config):/interface/wlan0/wlan/radio-2g/qos# **edca-ap** (configuring QoS parameters of the access point, traffic is transmitted from the access point to the client)
WOP-20L(config):/interface/wlan0/wlan/radio-2g/qos/edca-ap# **bk** (configuring QoS parameters for low-priority high-bandwidth queues (802.1p priorities: cs1, cs2))
WOP-20L(config):/interface/wlan0/wlan/radio-2g/qos/edca-ap/bk# **aifs X** (where X — waiting time for frames of data, measured in slots. Takes the values 1–255)
WOP-20L(config):/interface/wlan0/wlan/radio-2g/qos/edca-ap/bk# **cwmin X** (X — the initial value of the time to wait before resending a frame, specified in milliseconds. Accepts values: 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023. The cwMin value cannot exceed the cwMax value)
WOP-20L(config):/interface/wlan0/wlan/radio-2g/qos/edca-ap/bk# **cwmax X** (where X — maximum timeout value before resending a frame, specified in milliseconds. Accepts values: 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023. The cwMax value must be greater than the cwMin value)
WOP-20L(config):/interface/wlan0/wlan/radio-2g/qos/edca-ap/bk# **txop X** (where X — the time interval in milliseconds when the WME client station has the right to initiate data transmission over the wireless medium to the access point. Max value 65535 milliseconds)
WOP-20L(config):/interface/wlan0/wlan/radio-2g/qos/edca-ap/bk# **exit**
WOP-20L(config):/interface/wlan0/wlan/radio-2g/qos/edca-ap# **exit**
WOP-20L(config):/interface/wlan0/wlan/radio-2g/qos# **edca-sta** (configuring QoS parameters of the client station: traffic is transmitted from the client station to the access point)

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

5.5 DHCP option 82 Configuration

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

DHCP snooping operating modes:

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

Changing the operation mode of DHCP option 82

WOP-20L(root):/# **configure**
WOP-20L(config):/# **interface**
WOP-20L(config):/interface# **wlan0** (configuring will be done for Radio 2.4 GHz. To configure option 82 on Radio 5 GHz, enter **wlan1**)
WOP-20L(config):/interface/wlan0# **common**
WOP-20L(config):/interface/wlan0/common# **dhcp-snooping**
WOP-20L(config):/interface/wlan0/common/dhcp-snooping# **dhcp-snooping-mode replace** (selection of DHCP snooping operation in the mode of replacement or substitution of option 82)

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

Configuring Option 82 parameters

WOP-20L(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**)

WOP-20L(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**)

WOP-20L(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>)

WOP-20L(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)

WOP-20L(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)

5.6 WDS Configuration

When configuring a WDS connection, on the devices that will be connected via WDS, it is necessary to select the same channel and channel width in the radio interface settings. More information about configuring the radio interface via the command line can be found in the Radio configuration section.

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

WDS configuration

WOP-20L(root):/# **configure**
WOP-20L(config):/# **interface**
WOP-20L(config):/interface# **wlan1-wds0** (WDS link selection. Available values for Radio 2.4 GHz: wlan0–wds0 – wlan0–wds3; for Radio 5 GHz: wlan1–wds0 – wlan1–wds3)
WOP-20L(config):/interface/wlan1-wds0# **wds-5** (when configuring WDS on Radio 2.4 GHz enter **wds-2**)
WOP-20L(config):/interface/wlan1-wds0/wds-5# **mac-addr XX:XX:XX:XX:XX:XX** (MAC address of the remote access point radio interface, which can be found if you enter on the remote access point the **monitoring radio-interface** command)
WOP-20L(config):/interface/wlan1-wds0/wds-5# **exit**
WOP-20L(config):/interface/wlan1-wds0# **common**
WOP-20L(config):/interface/wlan1-wds0/common# **enabled true** (enabling WDS link. To disable, enter **false**)
WOP-20L(config):/interface/wlan1-wds0/common# **exit**
WOP-20L(config):/interface/wlan1-wds0# **exit**
WOP-20L(config):/interface# **wlan1** (when configuring WDS on Radio 2.4 GHz enter **wlan0**)
WOP-20L(config):/interface/wlan1# **wlan**
WOP-20L(config):/interface/wlan1/wlan# **wds**
WOP-20L(config):/interface/wlan1/wlan/wds# **security-mode WPA2** (selection of WPA2 security mode. Available values: WPA2, off — without password)
WOP-20L(config):/interface/wlan1/wlan/wds# **key-wpa password123** (key/password required for connection to the remote access point. Key length should be between 8 and 63 characters)
WOP-20L(config):/interface/wlan1/wlan/wds# **enabled true** (enabling WDS. To disable, enter **false**)
WOP-20L(config):/interface/wlan1/wlan/wds# **save**

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

5.7 System settings

5.7.1 Device firmware update

Device firmware update via TFTP

WOP-20L(root):/# **firmware upload tftp <ip address of tftp server> <Firmware file name>** (example: firmware upload tftp 192.168.1.15 WOP-20L-1.7.1_build_X.tar.gz)
WOP-20L(root):/# **firmware upgrade**

Device firmware update via HTTP

WOP-20L(root):/# **firmware upload http <URL for firmware uploading>** (example: firmware upload http http://192.168.1.100:8080/files/WOP-20L-1.7.1_build_X.tar.gz)
WOP-20L(root):/# **firmware upgrade**

Switching to access point firmware backup

WOP-20L(root):/# **firmware switch**

5.7.2 Device configuration management

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

WOP-20L(root):/# **manage-config reset-to-default**

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

WOP-20L(root):/# **manage-config reset-to-default-without-management**

Download the device configuration file to TFTP server

WOP-20L(root):/# **manage-config download tftp <tftp server ip address>** (example: manage-config download tftp 192.168.1.15)

Upload configuration file from TFTP server to the device

WOP-20L(root):/# **manage-config upload tftp <tftp server ip address> <Configuration file name>** (example: manage-config upload tftp 192.168.1.15 config.json)
WOP-20L(root):/# **manage-config apply** (apply configuration to the access point)

5.7.3 Device reboot

The command to reboot the device

WOP-20L(root):/# **reboot**

5.7.4 Authentication mode configuration

The device has a factory account *admin* with password *password*. To delete this account recording is not possible. The password can be changed using the following commands.

Changing the password for the admin account

WOP-20L(root):/# **configure**
WOP-20L(config):/# **authentication**
WOP-20L(config):/authentication# **admin-password <New password for admin account>** (from 1 up to 64 characters, including latin letters and digits)
WOP-20L(config):/authentication# **save**

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

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

Adding new users

WOP-20L(root):/# **configure**
WOP-20L(config):/# **authentication**
WOP-20L(config):/authentication# **user**
WOP-20L(config):/authentication/user# **add userX** (where userX — the name of the new account. To delete, use the **del** command)
WOP-20L(config):/authentication/user# **userX**
WOP-20L(config):/authentication/user/userX# **login userX** (where userX — the name of the new account)
WOP-20L(config):/authentication/user/userX# **password <Password for userX account>** (from 1 up to 64 characters, including latin letters and digits)
WOP-20L(config):/authentication/user/userX# **role admin** (the user is given the rights to configure. Possible value **viewer** — only monitoring will be available to the account)
WOP-20L(config):/authentication/user/userX# **save**

Configuring RADIUS Server Access Settings

WOP-20L(root):/# **configure**
WOP-20L(config):/# **authentication**
WOP-20L(config):/authentication# **radius**
WOP-20L(config):/authentication/radius# **auth-address X.X.X.X** (where X.X.X.X — IP address of the RADIUS server)
WOP-20L(config):/authentication/radius# **auth-port X** (where X — RADIUS server port, used for authentication and authorization. By default: 1812)
WOP-20L(config):/authentication/radius# **auth-password secret** (where secret — key for the RADIUS server, used for authentication and authorization)
WOP-20L(config):/authentication/radius# **exit**
WOP-20L(config):/authentication# **radius-auth true** (enabling authentication mode via the RADIUS server. To disable, enter **false**)
WOP-20L(config):/authentication# **save**

When authenticatiion via RADIUS server is used, be sure to create a local account that will be similar to an account on the RADIUS server.
In this case, the local account should contain a role that determines access rights (admin or viewer).
If the RADIUS server is unavailable, authentication will take place on the local account.

5.7.5 Setting the date and time

Commands to configure NTP server time synchronization

WOP-20L(root):/# **configure**
WOP-20L(config):/# **date-time**
WOP-20L(config):/date-time# **mode ntp** (enabling NTP operation mode)
WOP-20L(config):/date-time# **ntp**
WOP-20L(config):/date-time/ntp# **server <IP address of NTP server>** (NTP server configuration)
WOP-20L(config):/date-time/ntp# **exit**
WOP-20L(config):/date-time# **common**
WOP-20L(config):/date-time/common# **timezone 'Asia/Novosibirsk (Novosibirsk)'** (timezone configuration)
WOP-20L(config):/date-time/common# **save** (save changes)

5.7.6 Advanced system settings

Enabling global isolation

WOP-20L(root):/# **configure**
WOP-20L(config):/# **system**
WOP-20L(config):/system# **global-station-isolation true** (enabling global traffic isolation between clients of different VAPs and different radio interfaces. To disable, enter **false**)
WOP-20Lconfig):/system# save (save changes)

Changing device name

WOP-20L(root):/# **configure**
WOP-20L(config):/# **system**
WOP-20L(config):/system# **hostname WOP-20L_room2** (where WOP-20L_room2 is a new device name. The parameter can accept values from 1 to 63 characters: capital and lowercase latin letters, digits, hyphen character “-” (hyphen can not be the last character in name). By default: WOP-20L)
WOP-20L(config):/system# **save** (save changes)

Changing geographical domain

WOP-20L(root):/# **configure**
WOP-20L(config):/# **system**
WOP-20L(config):/system# **ap-location ap.test.root** (where ap.test.root — EMS management system device tree node domain, where access point is located. By default: root)
WOP-20L(config):/system# **save** (save changes)

5.8 APB service configuration

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

Commands for APB service configuration

WOP-20L(root):/# **configure**
WOP-20L(config):/# **captive-portal**
WOP-20L(config):/captive-portal# **apbd**
WOP-20L(config):/captive-portal/apbd# **roam_service_url <APB service address>**
(example: roam_service_url ws://192.168.1.100:8090/apb/broadcast)
WOP-20L(config):/captive-portal/apbd# **enabled true** (enabling APB service. To disable, enter **false**)
WOP-20L(config):captive-portal/apbd# **save** (save changes)

5.9 Monitoring

5.9.1 Wi-Fi clients

WOP-20L(root):/# **monitoring associated-clients**

```
  index                    | 0
  interface                | wlan0-va0
  state                    | ASSOC AUTH_SUCCESS
  hw-addr                  | 26:af:0a:30:ef:29
  ssid                     | !!!DOC_test
  ip-addr                  | 169.254.68.250
  authorized               | true
  captive-portal-vap       | false
  enterprise-vap           | false
  rx-retry-count           | 76
  tx-fails                 | 0
  tx-period-retry          | 0
  tx-retry-count           | 0
  rssi-1                   | -75
  rssi-2                   | -75
  rssi                     | -75
  snr-1                    | 17
  snr                      | 17
  snr-2                    | 16
  tx-rate                  | MCS7 SGI 72.2
  rx-rate                  | MCS7 NO SGI 65
  rx-bw                    | 20M
  rx-bw-all                | 20M
  tx-bw                    | 20M
  mfp                      | false
  uptime                   | 00:00:27
  multicast-groups-count   | 0
  wireless-mode            | n
  perftest-capable         | false
  snr-rssi-capable         | false
  link-capacity            | 0
  link-quality             | 0
  link-quality-common      | 0
  actual-tx-rate           | 0
  actual-rx-rate           | 0
  shaped-rx-rate           | 0
  actual-tx-pps            | 0
  actual-rx-pps            | 1
  shaped-rx-pps            | 0
  name                     | 0

Rate                    Transmitted              Received
----------------------  -----------------------  --------------------------
Total Packets:          2                        176
TX success:             100
Total Bytes:            173                      8877
Data Packets:           0                        31
Data Bytes:             0                        4488
Mgmt Packets:           2                        145
Mgmt Bytes:             173                      127
```

```
Dropped Packets:          0                       0
Dropped Bytes:            0                       0
Lost Packets:             0

Rate                      Transmitted             Received
----------------------    ----------------------  ------------------------
dsss1                     2               | 100%  37              |  21%
ofdm6                     0               |   0%  19              |  10%
ofdm24                    0               |   0%  88              |  50%
mcs3                      0               |   0%  2               |   1%
mcs4                      0               |   0%  15              |   8%
mcs7                      0               |   0%  14              |   8%

Multicast groups: none
```

5.9.2 WDS

WOP-20L(root):/# **monitoring wds-entries**

```
  index                    | 0
  interface                | wlan1
  state                    | WIFI_WDS
  hw-addr                  | e8:28:c1:d1:43:15
  ip-addr                  | 10.24.80.35
  hostname                 | WOP-20L
  authorized               | false
  captive-portal-vap       | false
  enterprise-vap           | false
  rx-retry-count           | 10
  tx-fails                 | 0
  tx-period-retry          | 0
  tx-retry-count           | 0
  rssi-1                   | -25
  rssi-2                   | -20
  snr-1                    | 40
  snr-2                    | 39
  wds-interface            | wlan1-wds1
  tx-rate                  | VHT NSS2-MCS8 SGI 173.3
  rx-rate                  | VHT NSS2-MCS8 NO SGI 156
  rx-bw                    | 20M
  rx-bw-all                | 20M
  tx-bw                    | 20M
  uptime                   | 00:02:44
  multicast-groups-count   | 0
  wireless-mode            | ac
  eltex-firmware-version   | 1.6.0 build X
  eltex-board-type         | WOP-20L
  perftest-capable         | false
  snr-rssi-capable         | false
  link-capacity            | 90 (not changed)
  link-quality             | 100 (not changed)
  link-quality-common      | 100
  actual-tx-rate           | 0
  actual-rx-rate           | 5
  shaped-rx-rate           | 0
  actual-tx-pps            | 0
  actual-rx-pps            | 8
  shaped-rx-pps            | 0
  name                     | 0

  Rate                  Transmitted            Received
-----------------------------------------------------------------------
  Total Packets:       | 53                   | 2125                 |
  TX success:          | 100                  |                      |
  Total Bytes:         | 4300                 | 261666               |
  Data Packets:        | 48                   | 2120                 |
  Data Bytes:          | 2496                 | 193382               |
  Mgmt Packets:        | 5                    | 5                    |
  Mgmt Bytes:          | 268                  | 444                  |
-----------------------------------------------------------------------

  Rate                  Transmitted            Received
```

```
-------------------------------------------------------------------
 ofdm6                | 7              |  13%|              12 |   0%|
 ofdm54               | 1              |   1%|               0 |   0%|
 nss2-mcs0            | 4              |   7%|               6 |   0%|
 nss2-mcs1            | 4              |   7%|               8 |   0%|
 nss2-mcs2            | 4              |   7%|               6 |   0%|
 nss2-mcs3            | 4              |   7%|               6 |   0%|
 nss2-mcs4            | 4              |   7%|               7 |   0%|
 nss2-mcs5            | 4              |   7%|               4 |   0%|
 nss2-mcs6            | 4              |   7%|               7 |   0%|
 nss2-mcs7            | 9              |  16%|              24 |   1%|
 nss2-mcs8            | 8              |  15%|            2044 |  96%|
-------------------------------------------------------------------

Multicast groups: none
```

5.9.3 Device information

WOP-20L(root):/# **monitoring information**

```
 system-time                 | 09:14:22 14.02.2023
 uptime                      | 6 d 01:59:11
 software-version            | 1.7.1 build X
 secondary-software-version  | 1.7.1 build X
 boot-version                | 1.7.1 build X
 memory-usage                | 39
 memory-free                 | 143
 memory-used                 | 95
 memory-total                | 238
 cpu-load                    | 1.9
 cpu-average                 | 5.23
 is-default-config           | false
 board-type                  | WOP-20L
 hw-platform                 | WOP-20L
 factory-wan-mac             | 68:13:E2:1B:6B:40
 factory-lan-mac             | 68:13:E2:1B:6B:40
 factory-serial-number       | WP4A000050
 hw-revision                 | 2v1
 session-password-initialized | false
 ott-mode                    | false
 last-reboot-reason          | unknown
 test-changes-mode           | false
```

5.9.4 Network information

WOP-20L(root):/# **monitoring wan-status**

```
Common information:

interface | br0
mac | 68:13:e2:1b:6b:40
rx-bytes | 543842355
rx-packets | 1745546
tx-bytes | 11589636
tx-packets | 25586

IPv4 information:

protocol | dhcp
ip-address | 192.168.1.10
netmask | 255.255.255.0
gateway | 192.168.1.1
DNS-1 | 172.16.0.100
DNS-2 | 172.16.0.250

IPv6 information:

addresses |
dns-servers |
```

WOP-20L(root):/# **monitoring ethernet**

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

WOP-20L(root):/# **monitoring arp**

```
#                  IP                 MAC
-----------------  -----------------  -----------------
0                  10.24.80.65        14:dd:a9:e1:xx:xx
1                  10.24.80.98        18:c0:4d:dd:xx:xx
2                  10.24.80.1         e0:d9:e3:e8:xx:xx
```

WOP-20L(root):/# **monitoring route**

```
Destination        Gateway            Mask               Flags              Interface
-----------------  -----------------  -----------------  -----------------  ---------
0.0.0.0            10.24.80.1         0.0.0.0            UG                 br0
10.24.80.0         0.0.0.0            255.255.255.0      U                  br0
```

5.9.5 Wireless interfaces

WOP-20L(root):/# **monitoring radio-interface**

```
    wlan0:
       name: wlan0
       band: 2.4
       hwaddr: CC:9D:A2:E9:14:70
       status: on
       noise-1: -100
       noise-2: -100
       utilization: 3
       channel: 2
       tx-power: 16
       thermal: 39
       bandwidth: 20
       frequency: 2417
    wlan1:
       name: wlan1
       band: 5
       hwaddr: CC:9D:A2:E9:14:75
       status: on
       noise-1: -100
       noise-2: -100
       utilization: 2
       channel: 48
       tx-power: 19
       thermal: 30
       bandwidth: 20
       frequency: 5240
```

5.9.6 Event logging

WOP-20L(root):/# **monitoring events**

```
Jan  23 00:00:07 WOP-20L daemon.info syslogd[925]: started: BusyBox v1.21.1

Jan  23 00:00:09 WOP-20L daemon.info configd[955]: The AP startup configuration was loaded
successfully.

Jan  1 03:00:14 WOP-20L daemon.info networkd[987]: Networkd started

Jan  1 03:01:17 WOP-20L daemon.info networkd[987]: DHCP-client: Interface br0 obtained
lease on 192.168.1.15.

Jan 23 07:17:14 WOP-20L daemon.info monitord[1055]: event: 'associated' mac:
E4:0E:EE:BD:AE:6B ssid: 'WOP-20L_2.4GHz' int0
```

5.9.7 Environment scan

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

WOP-20L(root):/# **monitoring scan-wifi**

```
SSID                    Mode  Security  BSSID             Channel  RSSI, dBm  Bandwidth,
MHz
----------------------  ----  --------  ----------------- -------  ---------  -------
!!!!Esh_test1111         AP    wpa      CC:9D:A2:C7:A2:E0    1        -39        20
EltexWiFi                AP    off      E0:D9:E3:49:D5:00    1        -50        20
Eltex-WLC-Local          AP    wpa      CC:9D:A2:FF:B2:03    6        -68        20
TEst_Ent                 AP    wpa      CC:9D:A2:C7:DF:D0    11       -75        20
sdd_wlc_enterprise       AP    wpa      E8:28:C1:FC:D6:41    1        -77        20
WLC30_sdd1               AP    wpa      E8:28:C1:FC:D6:40    1        -77        20
WLC                      AP    off      E0:D9:E3:49:79:01    1        -77        20
Rostelecom               AP    off      E8:28:C1:EC:DE:21    11       -78        20
VIP_test                 AP    off      E0:D9:E3:73:06:F2    6        -79        20
i-cisco-ent              AP    wpa      7C:21:0E:E2:76:C0    1        -80        20
Test_Astra_Ted           AP    off      E4:5A:D4:E4:D3:F3    1        -80        20
Karandashev_Enterprise   AP    wpa      E0:D9:E3:73:06:F3    6        -80        20
i-cis-MAB                AP    off      7C:21:0E:E2:76:C2    1        -80        20
```

5.9.8 Spectrum analyzer

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

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

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

WOP-20L(root):/# **monitoring spectrum-analyzer**

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

6 The list of changes

Document version	**Issue date**	**Revisions**
Version 1.2	28.04.2023	Synchronization with firmware version 1.7.1 Changed: • 5.7 System settings Added: • 3.6.2 Device installation on a wall
Version 1.1	17.03.2023	Synchronization with firmware version 1.6.2
Version 1.0	17.02.2023	First issue
Firmware version 1.7.1		

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 in our technical forum.

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

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