

Wireless access point

WOP-2L

User manual

Firmware version 1.2.2

IP address: 192.168.1.10

Username: admin

Password: password

Contents

1	Introduction	5
1.1	Annotation.....	5
1.2	Symbols	5
2	Device description.....	6
2.1	Purpose.....	6
2.2	Device specification	6
2.3	The device technical parameters	7
2.4	Design	9
2.5	Light indication	10
2.6	Reset to the default settings.....	11
2.7	Delivery package	11
3	Rules and recommendations for device installation	12
3.1	Safety rules	12
3.2	Installation recommendations.....	12
3.3	Frequency bands and channels in the range of 5 GHz for Wi-Fi	12
3.4	Calculating the number of required access points	13
3.5	Channel selection for neighboring access points.....	13
4	The device installation	15
4.1	Antenna connector sealing procedure	16
5	Device management via the web interface	20
5.1	Getting started	20
5.2	Applying configuration and discarding changes.....	21
5.3	Web interface basic elements	22
5.4	The “Monitoring” menu	23
5.4.1	The “Wi-Fi Clients” submenu.....	23
5.4.2	The "WDS" submenu.....	24
5.4.3	The “Traffic Statistics” submenu	25
5.4.4	The “Scan Environment” submenu.....	27
5.4.5	The “Events” submenu	28
5.4.6	The “Network Information” submenu	29
5.4.7	The “Radio Information” submenu.....	31
5.4.8	The “Device Information” submenu	32
5.5	The “Radio” menu.....	33
5.5.1	The “Radio 2.4 GHz” submenu	33

5.5.2	The “Radio 5 GHz” submenu	36
5.5.3	The “Advanced” submenu	40
5.6	The “VAP” menu	41
5.6.1	The “Summary” submenu	41
5.6.2	The “VAP” submenu	42
5.7	The “WDS” menu.....	45
5.7.1	The “WDS” submenu.....	45
5.8	The “Network Settings” menu.....	47
5.8.1	The “System Configuration” submenu	47
5.8.2	The “Access” submenu	48
5.9	The “External Services” menu	50
5.9.1	The “Captive Portal” submenu.....	50
5.10	The “System” menu	51
5.10.1	The “Device Firmware Upgrade” submenu	51
5.10.2	The “Configuration” submenu	52
5.10.3	The “Reboot” submenu	52
5.10.4	The “Password” submenu	53
5.10.5	The “Log” submenu	53
5.10.6	The “Date and Time” submenu	54
6	Managing the device using the command line	56
6.1	Connection to the device.....	56
6.2	Network parameters configuration	57
6.2.1	Network parameters configuration via set-management-vlan-mode utility	58
6.2.2	IPv6 network parameters configuration.....	59
6.3	Virtual Wi-Fi access points (VAP) configuration.....	60
6.3.1	Configuration of VAP without encryption	60
6.3.2	Configuration of VAP with WPA-Personal security mode.....	61
6.3.3	Configuration of VAP with Enterprise authorization	62
6.3.4	Configuration of VAP with Captive Portal	63
6.3.5	Advanced VAP settings.....	63
6.4	Radio configuration	70
6.4.1	Advanced Radio settings	70
6.5	WDS configuring.....	73
6.6	System settings	73
6.6.1	Device firmware update.....	73

6.6.2	Device configuration management.....	74
6.6.3	Device reboot	74
6.6.4	Setting the date and time	75
6.6.5	Advanced system settings	75
6.7	APB service configuration.....	76
6.8	Monitoring	76
6.8.1	Wi-Fi Clients.....	76
6.8.2	WDS.....	83
6.8.3	Device info	89
6.8.4	Network information	90
6.8.5	Wireless interfaces	91
6.8.6	Event logging.....	91
6.8.7	Environment scan	92
6.8.8	Spectrum Analyzer	92
7	The list of changes.....	94

1 Introduction

1.1 Annotation

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

WOP-2L device is a Wi-Fi access point. The device enclosed into hermetic case which allows to use 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-2L.

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-2L wireless access point is designed for provision of user access to high-speed secure network.

The device provides high-speed and secure wireless network combining a lot of opportunities and services that are necessary for comfortable user access to operator services in crowded areas. WOP-2ac provides connection of up to 40 users.

The device is used to organize wireless network for different climate conditions in the wide range of operation temperature and high humidity (parks, factories, stadium, etc.) and it is the perfect platform for organization of connection in cottage settlements and remote communities.

Power supply of the access point is realized by PoE+ technology.

2.2 Device specification

Interfaces:

- 1 port of Ethernet 10/100/1000BASE-T (RJ-45);
- 2 SMA-type connectors for external antennas (Omni, sectoral, panel, etc.);
- Wi-Fi 2.4 GHz IEEE 802.11b/g/n;
- Wi-Fi 5 GHz IEEE 802.11a/n/ac.

Functions:

WLAN capabilities:

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

Network functions:

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

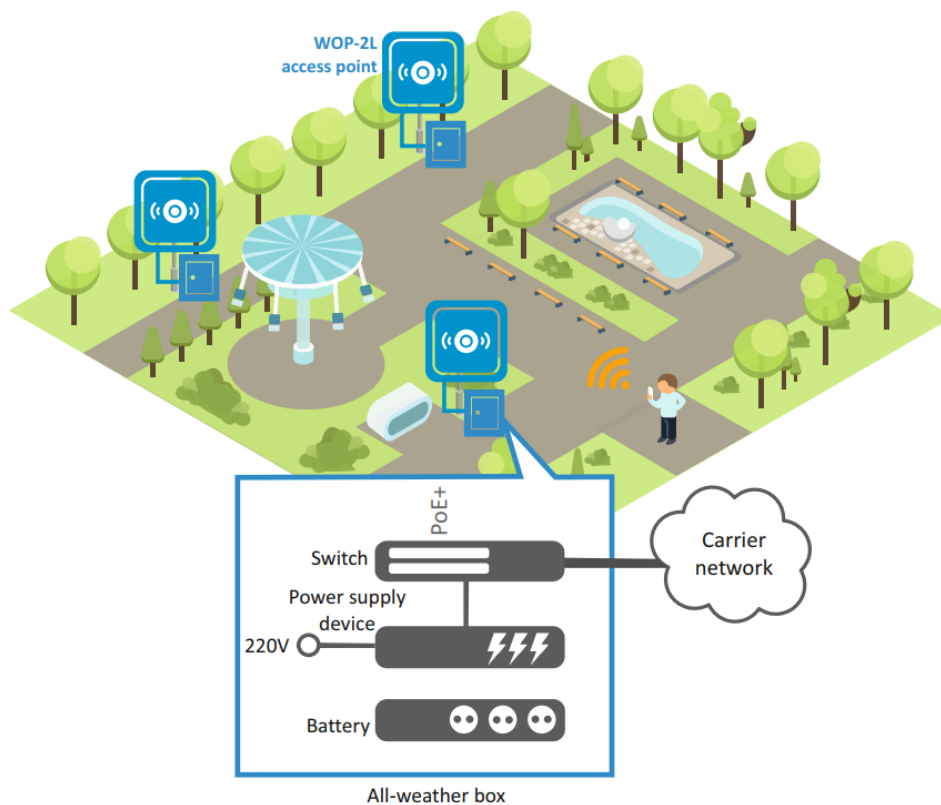
QoS functions:

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

Security:

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

The WOP-2L application diagram is shown in the figure below.



2.3 The device technical parameters

Main specifications

WAN interface parameters	
Number of ports	1
Electrical connector	RJ-45
Data rate, Mbps	10/100/1000, auto-negotiation
Standards	BASE-T
Wireless interface parameters	
Standards	802.11a/b/g/n/ac
Frequency range, MHz	2400–2483,5 MHz, 5150–5850 MHz

Modulation	DSSS, CCK, BPSK, QPSK, 16QAM, 64QAM, 256QAM
Operating channels	802.11b/g/n: 1–13 (2402–2482 MHz) 802.11a/n/ac: • 36–64 (5170–5320 MHz) • 100–144 (5490–5720 MHz) • 149–165 (5745–5835 MHz)
Data rate	802.11a: up to 54 Mbps 802.11b: up to 11 Mbps 802.11g: up to 54 Mbps 802.11n: up to 300 Mbps 802.11ac: up to 867 Mbps
Maximum output power of the transmitter	2.4 GHz: up to 20 dBm 5 GHz: up to 20 dBm
Receiver sensitivity	2.4 GHz: up to -94 dBm 5 GHz: up to -92 dBm
Security	Centralized authorization via RADIUS server (WPA Enterprise) WPA/WPA2 data encryption Captive Portal
Selection of antenna model depends on access point usage	
Support for 2x2 MIMO	
Control	
Remote control	Web interface, Telnet, SSH, CLI, SNMP (monitoring), NETCONF, EMS management system
Access restriction	by password
General parameters	
Flash	32 MB NAND Flash
RAM	128 MB RAM DDR3
Power supply	PoE+ 48V/54V (IEEE 802.3at-2009)
IP protection class	IP-54
Maximum power consumption	8 W
Range of operating temperatures	from -45 to +65°C
Relative humidity at 25°C	from 5% to 90%, non-condensing
Dimensions	80x232.5x47 mm
Weight	0.32 kg

2.4 Design

WOP-2L housed in a plastic case, industrial version. The size of the device: 80x232.5x47 mm. The design of WOP-2L is shown below.



WOP-2L design

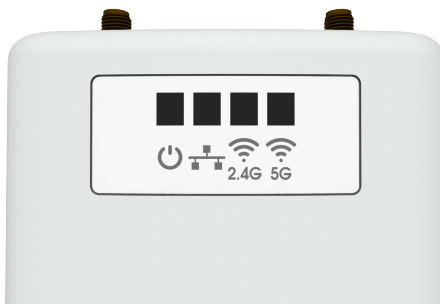
Port of 10/100/1000BASE-T (Ethernet) for local network connection and power supply via PoE and the button for resetting to factory settings (F) are located on the bottom panel of the device.



The bottom panel of WOP-2L

2.5 Light indication

The layout of WOP-2L indication panel is shown in the figure below.



WOP-2L indication panel

Device status LED indication

LED	LED status	Description
	Power – device power and operation status LED	solid green the device power supply is enabled, normal operation
		solid orange IP address is not received via DHCP
		solid red the device is loading
	LAN – Ethernet interface port indicator	solid green (10, 100 Mbps)/ solid orange (1000 Mbps) the channel between Ethernet interface of WOP-2L and connected device is active
		flashes packet data transmission between Ethernet interface of WOP-2L and connected device
	Wi-Fi 2.4 GHz – wireless status indicator in the 2.4 GHz range	solid green active 2.4 GHz Wi-Fi network
	Wi-Fi 5 GHz – wireless status indicator in the 5 GHz range	solid green active 5 GHz Wi-Fi network

2.6 Reset to the default settings

You can reset the device configuration using the “F” button on the device. When the device is loaded, press and hold the “F” button located on the bottom panel (approximately 10–15 seconds) until “Power” indicator is flashing orange;

Device will be rebooted automatically. DHCP client will be launched by default. If the address is not obtained via DHCP, the device will have the following address — *192.168.1.10*, and the following netmask — *255.255.255.0*.

2.7 Delivery package

The delivery package includes:

- WOP-2L wireless access point;
- Mounting kit;
- 1 patch-cord of RJ-45, 5e cat. – 1.5 m;
- Operations manual on a CD (optional);
- Conformity certificate;
- Technical passport.

3 Rules and recommendations for device installation

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

3.1 Safety rules

1. Do not open the device case. There are no user serviceable parts inside.
2. It is required to cover unused antenna connectors by safety cover included in the device delivery package.
3. Do not install the device during a thunderstorm. There is a risk of being struck by lightning.
4. You must follow requirements for voltage, current and frequency specified in the user manual.
5. Measuring devices and computer must be grounded before connecting to the device. Potential difference between cases of equipment and measurement devices must be no more than 1 V.
6. Check the cable integrity and security of mounting to the connectors.
7. Do not install the device near heat source and at places where temperature may reach values below -40°C or higher 60°C.
8. You should satisfy established standards and requirements for working at height during the device installation on the high-rise constructions.
9. The device exploitation should be performed by specially prepared engineering and technical personnel.
10. Connect only to operational service equipment.

3.2 Installation recommendations

1. The recommended installation: attaching to a mast/pole or wall;
2. Before you install and enable device, check the device for visible mechanical defects. If defects are observed, you should stop the device installation, draw up corresponding act and contact the supplier.
3. During the device installation to provide Wi-Fi coverage area with the best characteristics take into account the following rules:
 - a. Install the device at the center of a wireless network;
 - b. Minimize the number of obstacles (walls, roof, furniture and etc.) between WOP-2L and other wireless network devices;
 - c. Do not install the device near (about 2 m) electrical and radio devices;
 - d. It is not recommended to use radiophone and other equipment operating on the frequency of 2.4 GHz, 5 GHz in Wi-Fi effective radius;
 - e. Obstacles in the form of glass/metal constructions, brick/concrete walls, water cans and mirrors can significantly reduce Wi-Fi action radius.
4. During the installation of several access points, cell action radius must overlap with action radius of a neighboring cell at level of -65 ÷ -70 dBm. Decreasing of the signal level on cells borders to -75 dBm is permitted if it involves the use of VoIP, streaming video and other traffic that is sensitive to losses in wireless network.

3.3 Frequency bands and channels in the range of 5 GHz for Wi-Fi

Data transmission in the 5 GHz band is used for IEEE 802.11a/n/ac standards. WOP-2L supports frequency channels in the range of 5 GHz with the bandwidth of 20, 40 and 80 MHz.

To calculate the Wi-Fi channel central frequency – f , MHz, use the equation:

$f = 5000 + (5 \cdot N)$, where N – Wi-Fi channel number.

3.4 Calculating the number of required access points

Attenuation values

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

3.5 Channel selection for neighboring access points

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

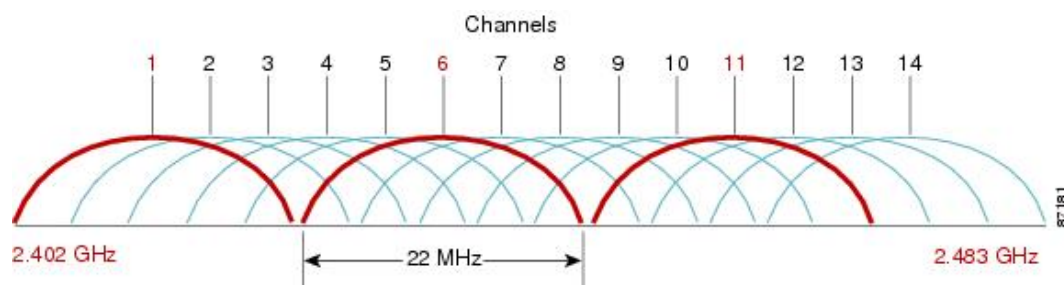


Figure 3 – General diagram of frequency channel closure in the range of 2.4 GHz

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

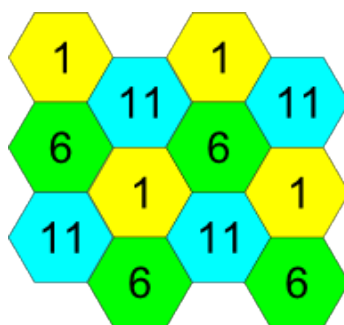


Figure 4 – Scheme of channel allocation among neighboring access points in the frequency range of 2.4 GHz when channel width is 20 MHz

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

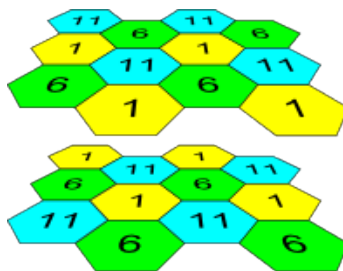


Figure 5 – Scheme of channel allocation between neighboring access points that are located between floors
When width of used channel is 40 MHz there is no non-overlapping channels in frequency range of 2.4 GHz. In such cases, you should select channels maximally separated from each other.

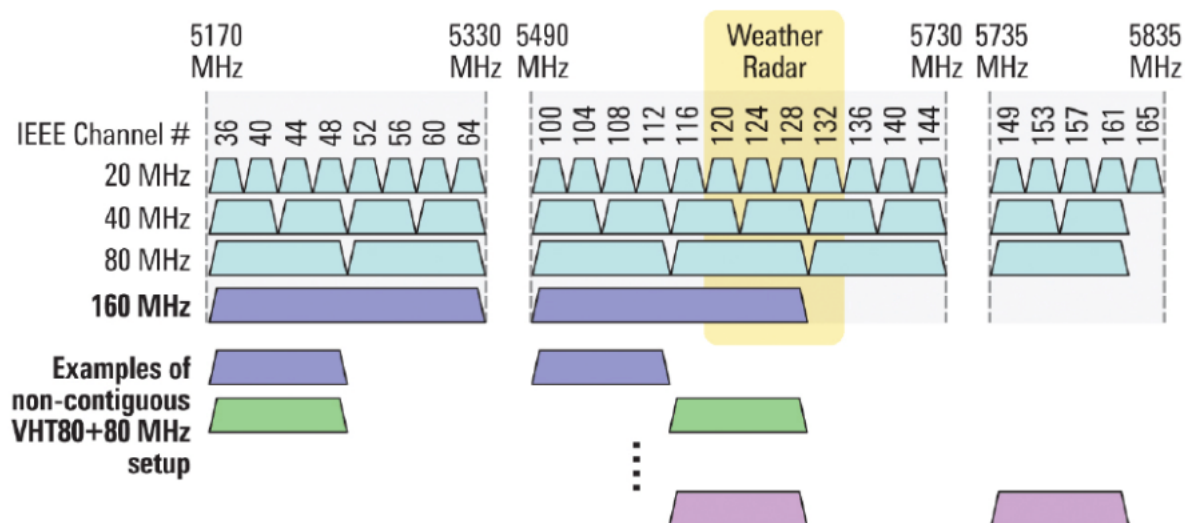
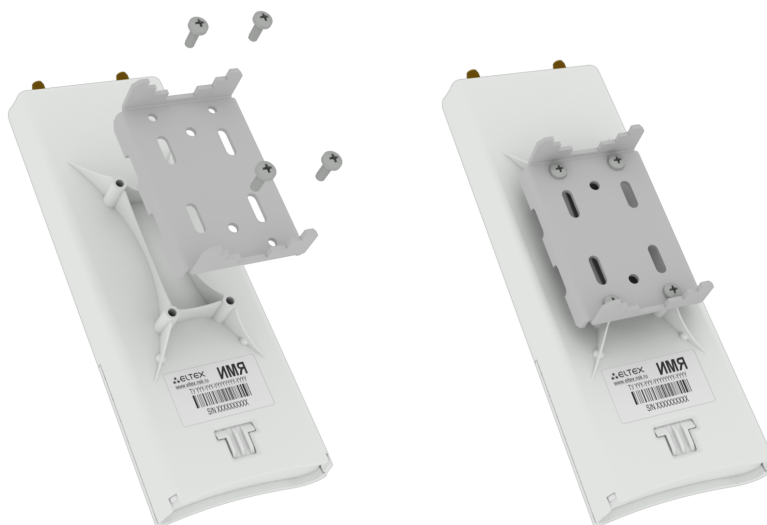


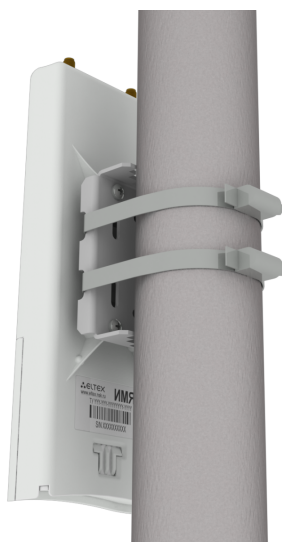
Figure 6 – Channels used in range of 5 GHz when channel width is 20, 40 or 80 MHz

4 The device installation

1. Attach the bracket to the device with the screws provided, as shown in the figure below.



2. Install the device on communications mast/pole pointing Ethernet port down as it is shown on the figure below. Attach the device using clamps supplied in the device package. Comply the safety rules and recommendations given in Safety rules and Installation recommendations.



3. Remove the bottom cover which close Ethernet port. Ground the device through a grounding connector (for H/W version: 1v5 and higher), then connect the Ethernet cable to the PoE port.



4. Close the bottom cover.
5. Connect the antenna to the device using the cable assembly.
6. Align the antenna position so that the subscriber devices fall within the coverage area of the installed antenna.
7. Connect the Ethernet cable outgoing from WOP-2L to the injector PoE port or the switch port (IEEE 802.3at-2009).
8. If you using PoE injector connect it to 220 V power supply network using the cable.

⚠ To avoid damage to the device, it is recommended to use lightning protection!

4.1 Antenna connector sealing procedure

⚠ Sealing should be performed on both sides of the cable.

1. Before connecting the cable to the connector, inspect the cable braid for damage and check for an O-ring in the nut of the connector, the location is shown in Figure 7 (a, b).



Figure 7a



Figure 7b

2. Connect the cable to the connector of the device (antenna) and tighten the nut, as shown in Figure 8 (a, b).



Figure 8a



Figure 8b

3. Cut the rubber sealing tape to the appropriate length: 0.15 m of waterproofing tape is required to seal one SMA connector (Figure 8a), 0.3 m of waterproofing tape is required for an N-type connector (Figure 8b), as shown in Figure 9 (a,b).

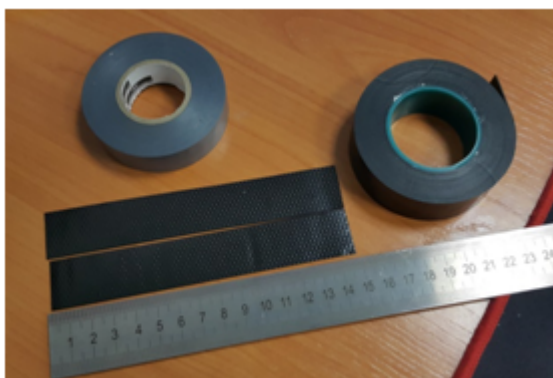


Figure 9a



Figure 9b

4. Remove the protective layer from the rubber band as shown in Figure 10.



Figure 10

5. Start wrapping from the cable side, with a 10-15 mm step away from the crimped part. Fix the end of the tape on the cable braid at an angle of 15...25 degrees to the cable axis, and, stretching the tape slightly, start wrapping the cable and the connector, advancing towards the device body. Lay the coils overlapping each other, no folds are allowed on the coils. The cable wrapping is shown in Figure 11 (a, b).



Figure 11a



Figure 11b

6. Having reached the housing of the device (antenna) by the edge of the tape, it is required to make a turn around the connector, pressing as much as possible the edge of the tape to the housing, then continue winding the tape at a different angle, moving away from the housing. When winding, do not forget to stretch the tape and press it tightly to the previously wound coils. At the tip of the ribbon, reduce the stretch and press it tightly against the coils on the cable braid, as shown in Figure 12 (a, b).



Figure 12a



Figure 12b

7. Cut PVC tape (duct tape) to the appropriate length: 0.28 m of duct tape is required to seal one SMA connector, 0.6 m of duct tape is required for an N-type connector. Tape is required to protect the rubber band from UV rays. The duct tape is shown in Figure 13.

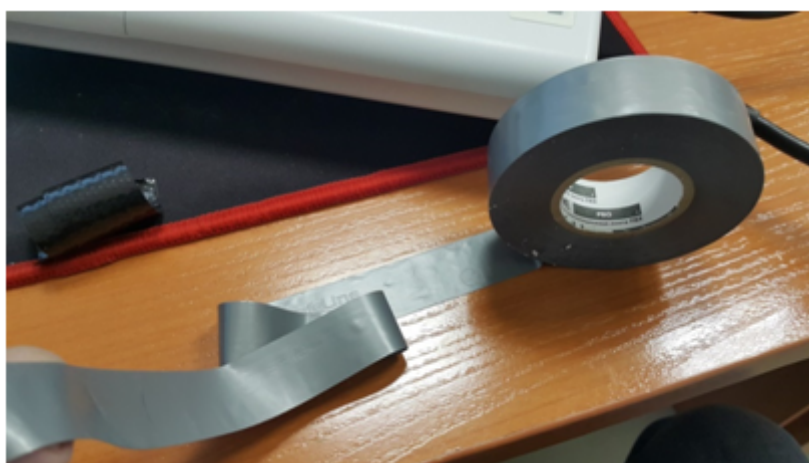


Figure 13

8. Start wrapping from the cable braid, having preliminarily stepped back from the first coil of the rubber tape by 5-10 mm. Fix the end of the tape on the cable at an angle of 15...25 degrees to the cable axis, and, slightly stretching the tape, start wrapping the cable and the connector, advancing towards the device body. Lay the coils overlapping each other, no folds are allowed on the coils. The winding of the cable is shown in Figure 14.



Figure 14

9. Having reached the housing by the edge of the tape, it is required to make a turn around the connector, pressing the edge of the tape to the housing as much as possible, then continue winding the tape at a different angle, moving away from the housing. When winding the tape tightly, do not allow any folds. On the last turns of the tape, reduce the stretch to zero and lay the last turn without stretching, as shown in Figure 15 (a, b).



Figure 15a



Figure 15b

10. Check the sealed connector for visible areas of rubber tape.

5 Device management via the web interface

5.1 Getting started

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

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

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

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

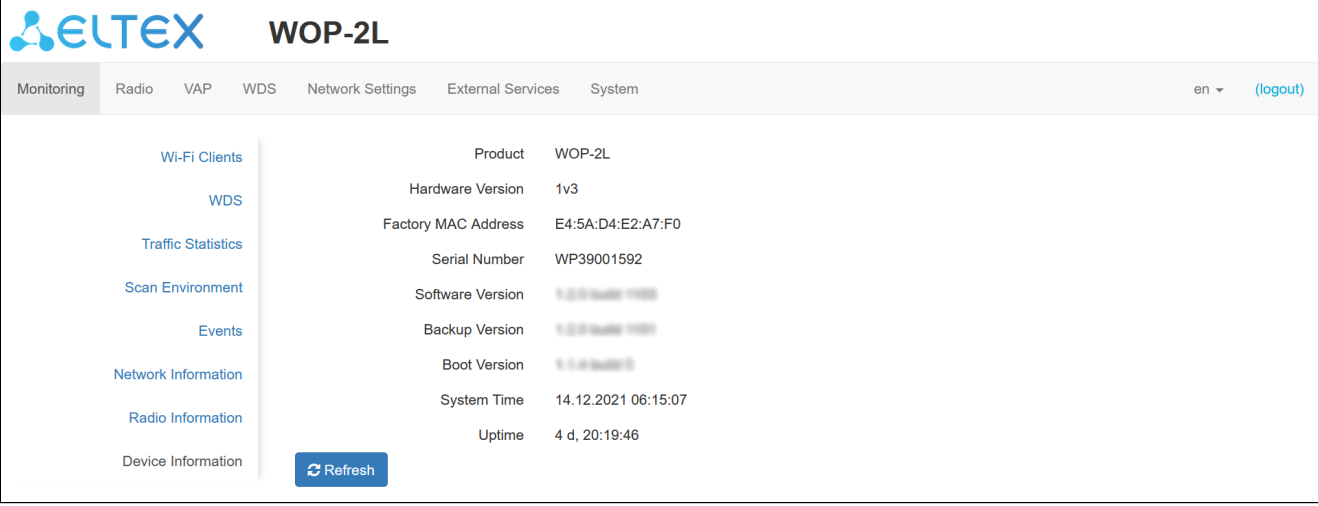


The image shows the login page for the WOP-2L device. It features the title "WOP-2L" at the top. Below the title, there are two input fields: "Enter login" and "Enter password". At the bottom of the form, there is a blue button labeled "Log In".

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

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

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

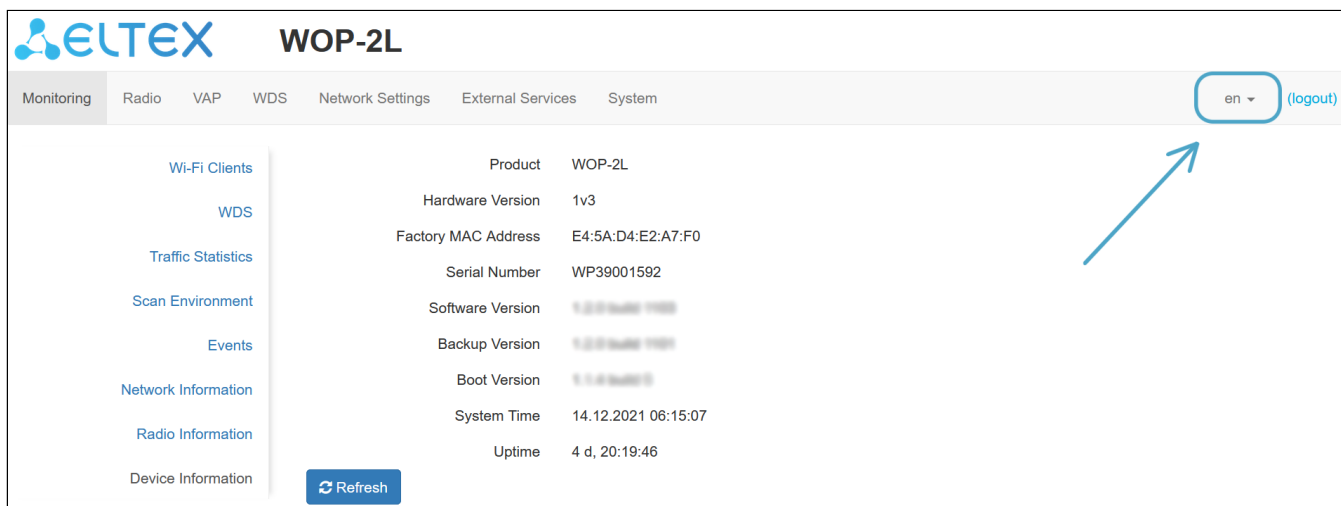


The image shows the monitoring dashboard for the WOP-2L device. The dashboard has a header with the ELTEX logo and the title "WOP-2L". Below the header, there is a navigation menu with tabs: Monitoring, Radio, VAP, WDS, Network Settings, External Services, and System. The "Monitoring" tab is selected. On the left side, there is a sidebar with a list of monitoring options: Wi-Fi Clients, WDS, Traffic Statistics, Scan Environment, Events, Network Information, Radio Information, and Device Information. The main content area displays the following information:

Product	WOP-2L
Hardware Version	1v3
Factory MAC Address	E4:5A:D4:E2:A7:F0
Serial Number	WP39001592
Software Version	1.2.0.0 (build 1100)
Backup Version	1.2.0.0 (build 1100)
Boot Version	1.1.0.0 (build 0)
System Time	14.12.2021 06:15:07
Uptime	4 d, 20:19:46

At the bottom of the main content area, there is a blue button labeled "Refresh".

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



5.2 Applying configuration and discarding changes

1. Applying configuration



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

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

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

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

2. Discarding changes



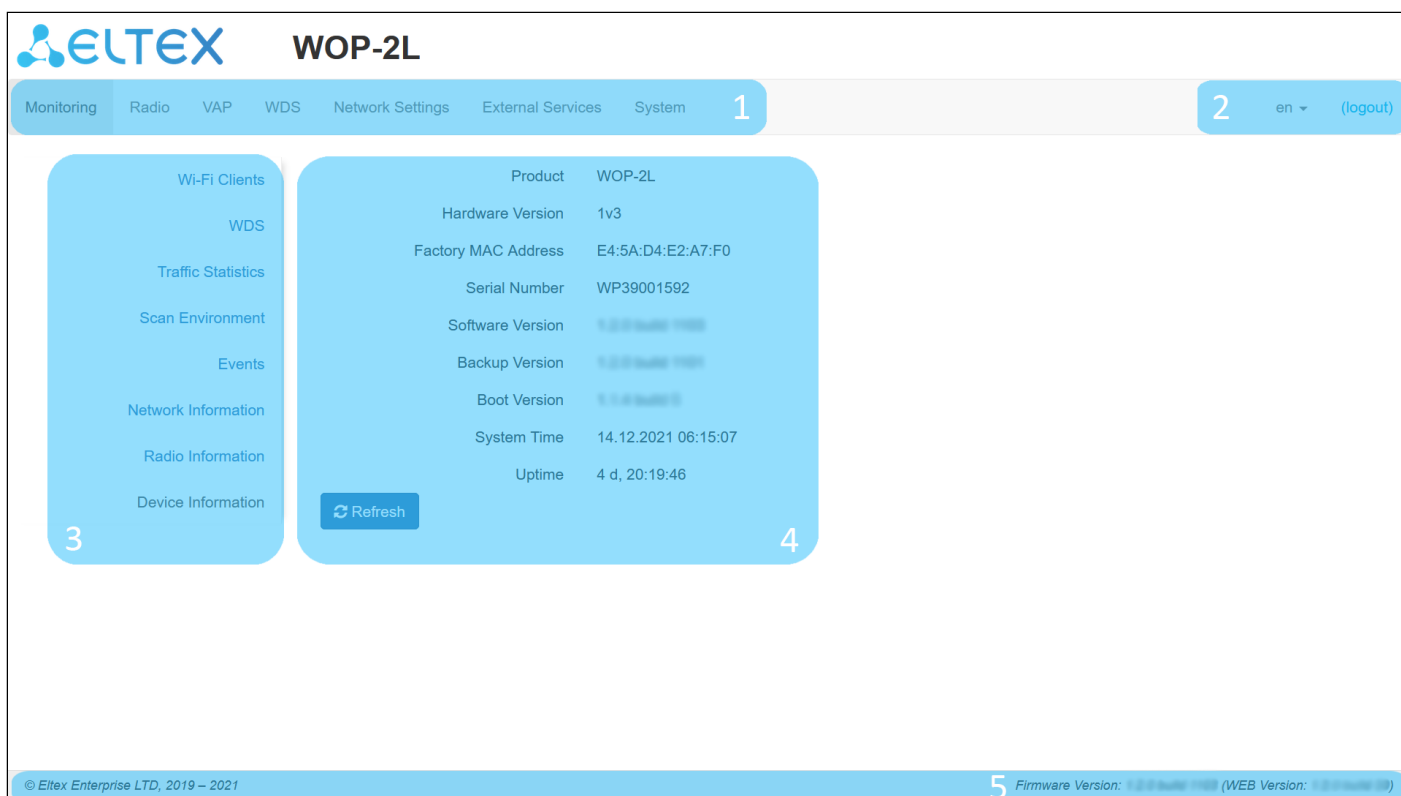
You can discard changes only before pressing "Apply" button. If you press "Apply" button, all the changed parameters will be applied and saved to device memory. You will not be able to return to previous configuration after pressing "Apply".

The button for discarding changes appears as follows:



5.3 Web interface basic elements

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



User interface window is divided into five general areas:

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

5.4 The “Monitoring” menu

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

5.4.1 The “Wi-Fi Clients” submenu

The “**Wi-Fi Clients**” submenu displays information about the status of connected Wi-Fi clients.

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

Monitoring

Radio

VAP

WDS

Network Settings

External Services

System

en (logout)

Wi-Fi Clients >

WDS

Traffic Statistics

Scan Environment

Events

Network Information

Radio Information

Device Information

Refresh

#	Hostname	IP Address	MAC	Interface	Link Capacity	Link Quality	Link Quality Common	RSSI, dBm	SNR, dB	TxRate	RxRate	TX BW, MHz	RX BW, MHz	Uptime																														
1		10.24.80.87	ae:6b:07:74:e6:fd	wlan1-va0	0	0	100	-55 / -72	31 / 21	VHT NSS2-MCS4 78	VHT NSS2-MCS8 156	20	20	00:00:03																														
Total TX / RX, bytes					1 687 / 1 690					Fails, packets																																		
Total TX / RX, packets					8 / 13					TX Period Retry, packets																																		
Data TX / RX, bytes					1 337 / 1 236					TX Retry Count, packets																																		
Data TX / RX, packets					5 / 8					Actual TX / RX Rate, kbps																																		
					<table><thead><tr><th>Rate</th><th colspan="2">TX Packets</th><th colspan="2">RX Packets</th></tr></thead><tbody><tr><td>OFDM6</td><td>5</td><td>63%</td><td>2</td><td>17%</td></tr><tr><td>OFDM24</td><td>0</td><td>0%</td><td>3</td><td>25%</td></tr><tr><td>NSS1-MCS5</td><td>2</td><td>25%</td><td>0</td><td>0%</td></tr><tr><td>NSS2-MCS8</td><td>0</td><td>0%</td><td>7</td><td>58%</td></tr><tr><td>NSS2-MCS9</td><td>1</td><td>13%</td><td>0</td><td>0%</td></tr></tbody></table>					Rate	TX Packets		RX Packets		OFDM6	5	63%	2	17%	OFDM24	0	0%	3	25%	NSS1-MCS5	2	25%	0	0%	NSS2-MCS8	0	0%	7	58%	NSS2-MCS9	1	13%	0	0%					
Rate	TX Packets		RX Packets																																									
OFDM6	5	63%	2	17%																																								
OFDM24	0	0%	3	25%																																								
NSS1-MCS5	2	25%	0	0%																																								
NSS2-MCS8	0	0%	7	58%																																								
NSS2-MCS9	1	13%	0	0%																																								

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

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

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

5.4.2 The "WDS" submenu

The WDS submenu displays information about the status of WOP-2L access points connected via WDS.

ELTEX

WOP-2L

Monitoring

Radio

VAP

WDS

Network Settings

External Services

System

en

(logout)

Wi-Fi Clients

WDS >

Traffic Statistics

Scan Environment

Events

Network Information

Radio Information

Device Information

Refresh

#	Hostname	IP Address	MAC	Interface	Link Capacity	Link Quality	Link Quality Common	RSSI, dBm	SNR, dB	TxRate	RxRate	TX BW, MHz	RX BW, MHz	Uptime
1	WOP-2L	10.24.80.95	e8:28:c1:d1:43:15	wlan1	6	4	11	-90 / -90	0 / -5	VHT NSS2-MCS0 13	0	20	20	00:02:45
Total TX / RX, bytes					72 091 / 5 852					Fails, packets 6				
Total TX / RX, packets					565 / 31					TX Period Retry, packets 173				
Data TX / RX, bytes					47 144 / 1 682					TX Retry Count, packets 470				
Data TX / RX, packets					439 / 14					Actual TX / RX Rate, kbps 4 / 0				
Rate					TX Packets			RX Packets						
DSSS2					192	34%	0	0%						
OFDM6					129	23%	30	100%						
OFDM54					31	5%	0	0%						
NSS1-MCS1					87	15%	0	0%						
NSS2-MCS0					126	22%	0	0%						

- **#** – 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** – interface of WOP-2L and the connected device interaction;
- **Link Capacity** – parameter that displays efficiency of modulation to transmission use by access point. Calculated based on the number of packets transmitted on each modulation to the client, and the reduction factors. Maximum value – 100% (means that all packets are transmitted to the client at maximum modulation for the maximum nss type supported by the client). Minimum value – 2% (in case when packets are transmitted on nss1mcs0 modulation for a client with 3x3 MIMO support). The parameter value is calculated over the last 10 seconds;
- **Link Quality** – parameter that displays the state of the link to the client, calculated based on the number of packet retransmissions 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 over the last 10 seconds;
- **Link Quality Common** – parameter that displays the state of the link to the client, calculated based on packet retransmission 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 entire time of the client connection;
- **RSSI** – received signal level, dBm;
- **SNR** – ratio signal/noise, dB;
- **TxRate** – channel transmission rate, Mbps;
- **RxRate** – receive channel rate, Mbps;

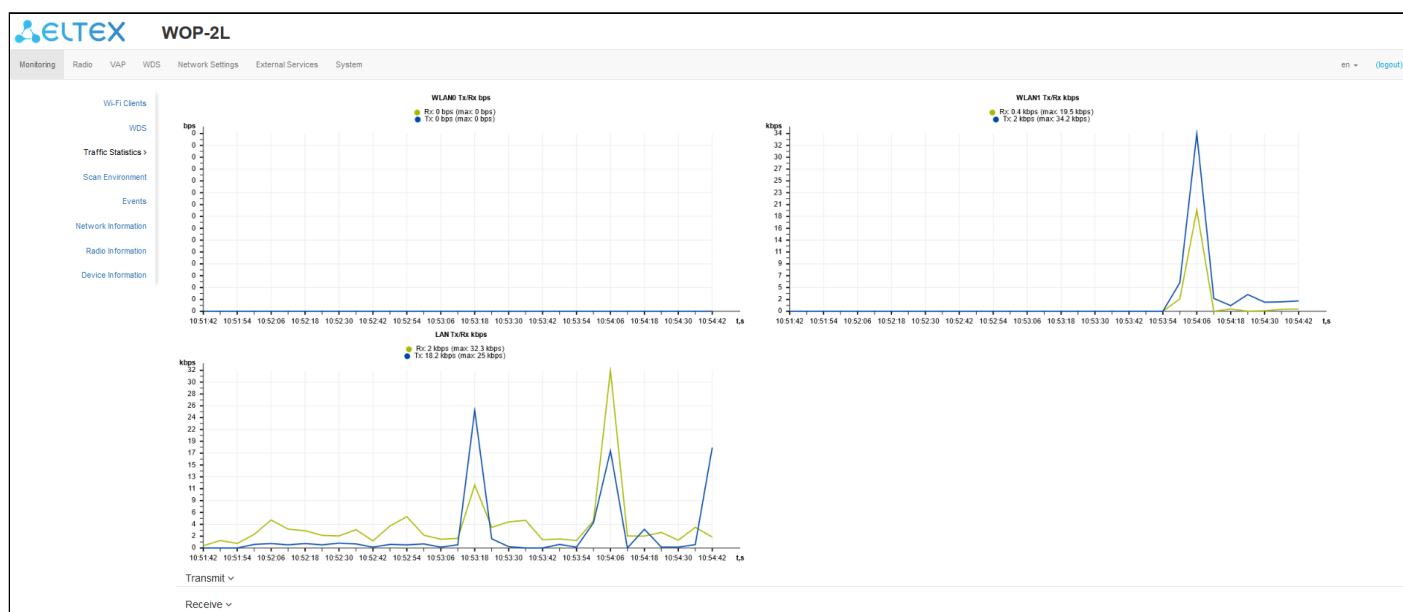
- *TX BW* — transmission bandwidth, MHz;
- *RX BW* — reception bandwidth, MHz;
- *Uptime* — Wi-Fi client connection uptime.

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

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

5.4.3 The “Traffic Statistics” submenu

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



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

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

Transmit ▾				
Interface	Total Packets	Total Bytes	Total Drop	Errors
LAN	8101	5532185	0	0
WLAN0	1116	165370	661034	38
WLAN1	226	44052	661694	0
sit0	0	0	0	0
wlan0-va0	1116	165370	661034	38
wlan0-va1	0	0	0	0
wlan0-va2	0	0	0	0
wlan0-va3	0	0	0	0
wlan0-wds0	0	0	0	0
wlan0-wds1	0	0	0	0
wlan0-wds2	0	0	0	0

“Transmit” table description:

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

Receive ▾				
Interface	Total Packets	Total Bytes	Total Drop	Errors
LAN	812365	129033224	11138	0
WLAN0	251	43357	0	0
WLAN1	94	17778	0	0
sit0	0	0	0	0
wlan0-va0	251	43357	0	0
wlan0-va1	0	0	0	0
wlan0-va2	0	0	0	0
wlan0-va3	0	0	0	0
wlan0-wds0	0	0	0	0
wlan0-wds1	0	0	0	0
wlan0-wds2	0	0	0	0

“Receive” table description:

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

5.4.4 The “Scan Environment” submenu

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

WOP-2L

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

Wi-Fi Clients

WDS

Traffic Statistics

Scan Environment >

Events

Network Information

Radio Information

Device Information

Scan Last scan was 13.12.2021 13:48:30

Range	SSID	Security Mode	MAC	Channel / Bandwidth	RSSI, dBm
2.4 GHz	2L_301_nsk	Open	E8:28:C1:DA:C8:12	6/20	-46
2.4 GHz	WOP-2ac-LR2-1	Open	E8:28:C1:DA:E6:72	1/20	-53
2.4 GHz	ci_cd_data10	Open	E4:5A:D4:F6:CD:B1	6/20	-54
2.4 GHz	ESH_MULT1	WPA/WPA2	E8:28:C1:DA:E6:73	1/20	-54
2.4 GHz	Test_LR2	WPA/WPA2	E8:28:C1:DA:E6:21	1/20	-59
2.4 GHz	!test1234	Open	E8:28:C1:FC:D6:70	1/20	-60
2.4 GHz	test	Open	E8:28:C1:FC:D6:76	1/20	-60
2.4 GHz	lesia_esdk	Open	E8:28:C1:FC:D6:74	1/20	-61
2.4 GHz	Karandashev_Enterprise2	WPA2_1X	E8:28:C1:FC:D6:72	1/20	-61
2.4 GHz	HOT_SSID	Open	E8:28:C1:FC:D6:73	1/20	-61

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

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

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

5.4.5 The “Events” submenu

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

ELTEX WOP-2L	
Monitoring	Radio VAP WDS Network Settings External Services System en (logout)
Wi-Fi Clients	Refresh Clear
WDS	
Traffic Statistics	
Scan Environment	
Events >	
Network Information	
Radio Information	
Device Information	
Date and Time	Type Service Message
Dec 13 13:48:30	daemon.info scanwlan[3052] scan on interface 'wlan1' finished
Dec 13 13:48:29	daemon.info scanwlan[3052] scan on interface 'wlan0' finished
Dec 13 13:48:03	daemon.info scanwlan[3052] start scan on interface 'wlan1'
Dec 13 13:48:03	daemon.info scanwlan[3052] start scan on interface 'wlan0'
Dec 13 12:10:58	daemon.info networkd[1092] DHCP-client: Interface br0 renew lease on 10.24.80.92.
Dec 13 11:25:43	daemon.info monitord[1184] event: 'deauthenticated by AP' mac: AE:6B:07:74:E6:FD ssid: 'WOP-2L_5GHz' interface: wlan1-va0 channel: 165 rssi-1: -85 rssi-2: -90 location: 'AP_for_documentation.root' reason: 4 description: 'Inactivity'
Dec 13 06:53:55	daemon.info monitord[1184] event: 'authenticated' mac: AE:6B:07:74:E6:FD ssid: 'WOP-2L_5GHz' interface: wlan1-va0 channel: 165 rssi-1: -59 rssi-2: -62 location: 'AP_for_documentation.root' reason: 0 description: 'Successful'

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

Table 7 — Event importance categories description

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

To receive new messages in the event log, click the “Update” button.

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

5.4.6 The “Network Information” submenu

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

Monitoring

Radio

VAP

WDS

Network Settings

External Services

System

en - (logout)

Wi-Fi Clients

WDS

Traffic Statistics

Scan Environment

Events

Network Information >

Radio Information

Device Information

WAN Status

Interfacebr0

ProtocolDHCP

IP Address10.24.80.92

RX Bytes134.9 MiB (141 493 376 bytes)

TX Bytes32.5 MiB (34 101 982 bytes)

Ethernet

Link StatusUp

Speed1000

DuplexFull

ARP

#	IP Address	MAC
0	10.24.80.68	10:7B:44:A3:A6:71
1	10.24.80.98	18:C0:4D:DD:5F:14
2	10.24.80.31	60:45:CB:9E:BB:6A
3	10.24.80.24	F9:B4:D2:2C:8A:41
4	10.24.80.62	38:2C:4A:71:DC:D9
5	10.24.80.83	60:E3:27:00:FC:D8
6	10.24.80.37	14:CC:20:05:A9:7E
7	10.24.80.1	E0:D9:E3:E8:E1:40
8	10.24.80.49	2C:56:DC:4B:1E:04
9	10.24.80.20	D4:5D:64:26:3E:DB

Routes

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

WAN Status:

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

Ethernet:

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

ARP

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

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

Routes:

- *Interface* — name of the bridge interface;
- *Destination* — IP address of destination host or subnet that the route is established to;
- *Gateway* — gateway IP address that allows for the access to the Destination;
- *Netmask* — subnet mask;
- *Flags* — certain route characteristics. The following flag values exist:
 - **U** — means that the route is created and passable;
 - **H** — identifies the route to the specific host;

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

5.4.7 The “Radio Information” submenu

In the “**Radio Information**” submenu the current status of WOP-2L radio interfaces is displayed.

Radio 2.4 GHz	
Status	On
MAC	E4:5A:D4:E2:A7:F0
Mode	IEEE 802.11b/g/n
Channel	1 (2412 MHz)
Channel Bandwidth, MHz	20

Radio 5 GHz	
Status	On
MAC	E4:5A:D4:E2:A7:F5
Mode	IEEE 802.11a/n/ac
Channel	165 (5825 MHz)
Channel Bandwidth, MHz	20

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

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

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

“Off”:

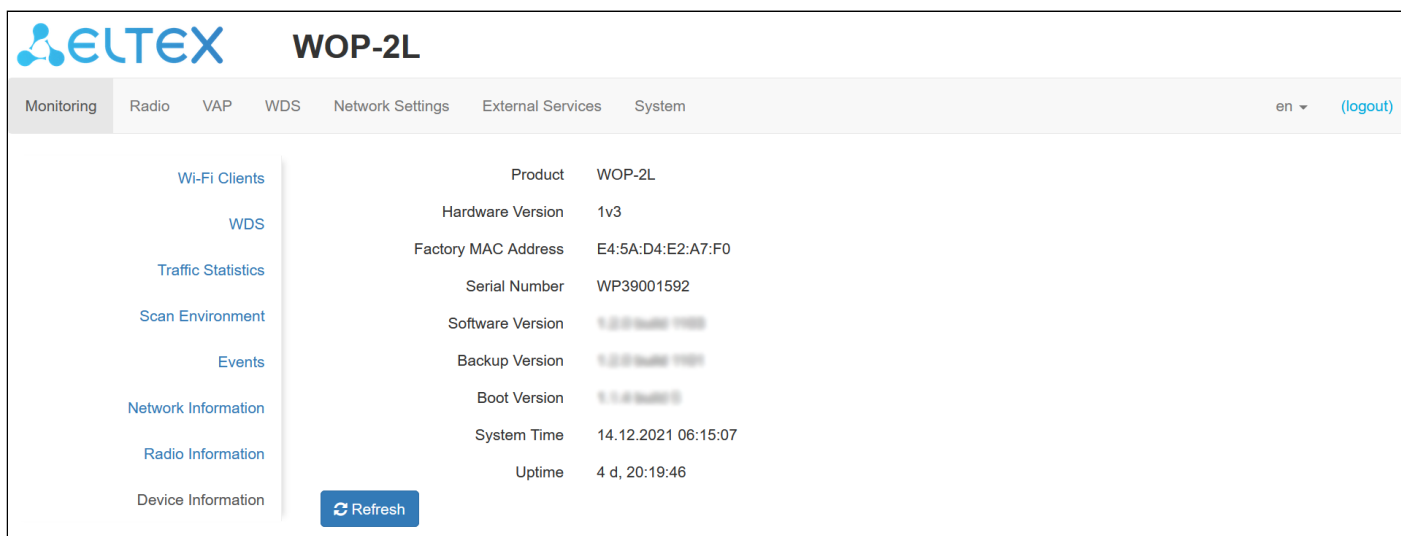
- *Status* — radio interface state;
- *MAC* — radio interface MAC address;
- *Mode* — radio interface operation mode according to IEEE 802.11 standards.

“On”:

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

5.4.8 The “Device Information” submenu

The “**Device Information**” submenu displays main WOP-2L parameters.



The screenshot shows the ELTEX WOP-2L web interface. The top navigation bar includes links for Monitoring, Radio, VAP, WDS, Network Settings, External Services, and System. The left sidebar lists various monitoring options, with 'Device Information' selected at the bottom. The main content area displays a table of device parameters:

Parameter	Value
Product	WOP-2L
Hardware Version	1v3
Factory MAC Address	E4:5A:D4:E2:A7:F0
Serial Number	WP39001592
Software Version	1.2.0.19a488-1100
Backup Version	1.2.0.19a488-1100
Boot Version	1.1.0.19a488-0
System Time	14.12.2021 06:15:07
Uptime	4 d, 20:19:46

A 'Refresh' button is located at the bottom of the table.

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

5.5 The “Radio” menu

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

5.5.1 The “Radio 2.4 GHz” submenu

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

- *Mode* – select interface operation mode:
 - IEEE 802.11b/g;
 - IEEE 802.11b/g/n;
 - IEEE 802.11n.
- *Auto Channel* – when checked, the device will automatically select the least loaded radio channel for the Wi-Fi interface. Removing the flag opens the access to install the static operation channel;
- *Channel* – select channel for data transmission;
- *Use Limit Channels* – when checked, the access point will use a user-defined list of channels to work in automatic channel selection mode. If the “Use Limit channels” flag is not checked or there are no channels in the list, the access point will select the operation channel from all available channels in the given band. 2.4 GHz range channels: 1-13;
- *Channel Bandwidth, MHz* – channel bandwidth, on which the access point operates. The parameter may take values of 20 and 40 MHz;
- *Primary Channel* – the parameter can only be changed if the bandwidth of a statically specified channel is equal to 40 MHz. The 40 MHz channel can be considered as consisting of two 20 MHz channels, which border in the frequency range. These two 20 MHz channels are called primary and secondary channels. The primary channel is used by clients who only support 20 MHz channel bandwidth:
 - *Upper* – the primary channel will be the upper 20 MHz channel in the 40 MHz band;
 - *Lower* – the primary channel will be the lower 20 MHz channel in the 40 MHz band.
- *Transmission Power Limit, dBm* – transmitting Wi-Fi signal power adjustment, dBm. May take values between 11 and 16 dBm;

- *Fixed Transmit Rate* – fixed wireless data transmission rate which is defined by IEEE 802.11b/g/n standards.

- ✓ If the “Use Limit channels” list contains a channel that is not available for selection, it will be marked in grey. In order for the new configuration to be applied to an access point, only available (blue highlighted) channels must be specified in the “Use Limit channels” list.

Example. No settings have been made on the access point yet, Radio 2.4 GHz is set to 20 MHz “Channel Bandwidth” by default, and channels are specified in the “Use Limit channels” list: 1, 6, 11. Suppose the parameter “Channel Bandwidth” is set to 40 MHz. When you change this parameter from 20 MHz to 40 MHz, the following happens:

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

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

In the “Advanced” section, you can configure advanced device’s radio interface parameters.

Advanced ▾

Short Guard Interval	☒
STBC	☐
Beacon Interval, ms	100
Fragmentation Threshold	2346
RTS Threshold	2347
Frame Aggregation	☒
Short Preamble	☒
Broadcast/Multicast Rate Limiting, p/s	0
Wi-Fi Multimedia (WMM)	☒
Enable QoS	☐

- *OBSS Coexistence* – automatic channel bandwidth reduction when the air is loaded. When the flag is set, the mode is enabled;
- *Short Guard interval* – support for Short Guard interval. Access point transmits data using 400 ns Guard interval (instead of 800 ns) to clients which also support Short GI;
- *STBC* – Space-Time Block Coding method dedicated to improve data transmission reliability. The field is available only if the selected mode of operation of the radio interface includes 802.11n. When checked, the device transmits one data flow through several antennas. When unchecked, the device does not transmit one data flow through several antennas;

- *Beacon Interval, ms* – beacon frames transmission period. The frames are sent to detect access points. The parameter takes values from 20 to 2000 ms, by default – 100 ms;
- *Fragmentation Threshold* – frame fragmentation threshold, bytes. The parameter takes values 256-2346, by default – 2346;
- *RTS Threshold* – after what quantity of bytes the Request to Send will be sent. Decreasing of the parameter's value might improve access point operation when there are a lot of clients connected. However, decreasing of the parameter's value will reduce general bandwidth of wireless network. The parameter takes values from 0 to 2347, by default – 2347;
- *Aggregation* – enable support for AMPDU/AMSDU;
- *Short Preamble* – use of the packet short preamble;
- *Broadcast/Multicast Rate Limiting, p/s* – when the flag is set, transmission of broadcast / multicast traffic over the wireless network is restricted. Specify the limit for broadcast traffic in the popup window (p/s);
- *Wi-Fi Multimedia (WMM)* – WMM support activation (Wi-Fi Multimedia);
- *Enable QoS* – when the flag is set, the setting of Quality of Service functions is available.

The following functions are available for quality assurance configuration:

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

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

- *cwMin* – the initial timeout value before resending a frame, specified in milliseconds, takes the values 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023. The value of *cwMin* cannot exceed the value of *cwMax*;
- *cwMax* – the maximum timeout value before resending a frame, specified in milliseconds, takes the values 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023. The value of *cwMax* must exceed the value of *cwMin*;
- *TXOP Limit* – this parameter is used only for data transmitted from the client station to the access point. The transmission capability is the time interval, in milliseconds, when the client WME station has the rights to initiate data transmission over the wireless medium to the access point, the maximum value is 65535 milliseconds;
- *Station EDCA parameters* – table of client station parameter settings (traffic is transmitted from the client station to the access point). For description of table fields, see above.

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

5.5.2 The “Radio 5 GHz” submenu

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

The screenshot shows the ELTEX WOP-2L web interface. The top navigation bar includes 'Monitoring', 'Radio', 'VAP', 'WDS', 'Network Settings', 'External Services', and 'System'. The 'Radio' tab is active. On the left, there's a sidebar with 'Radio 2.4 GHz' and 'Radio 5 GHz >'. The 'Radio 5 GHz >' option is selected, and the 'Advanced' link is visible below it. The main content area is titled 'Common' and contains the following settings:

- Mode:** A dropdown menu set to 'IEEE 802.11a/n/ac'.
- Auto Channel:** A checkbox that is checked.
- Use Limit Channels:** A checkbox that is checked.
- Channel List:** A list of channels with a pencil icon for editing. The channels are: 36 (5180 MHz), 40 (5200 MHz), 44 (5220 MHz), and 48 (5240 MHz). Each channel has a small 'x' icon next to it.
- Channel Bandwidth, MHz:** A dropdown menu set to '20'.
- Transmit Power Limit, dBm:** A dropdown menu set to '19'.
- Fixed Transmit Rate:** A dropdown menu set to 'Auto'.
- Advanced:** A collapsed section indicated by a downward arrow.

At the bottom of the form, there are two buttons: 'Apply' (with a checkmark icon) and 'Cancel' (with an 'x' icon).

- *Mode* – select interface operation mode:
 - IEEE 802.11a;
 - IEEE 802.11a/n;
 - IEEE 802.11a/n/ac.
- *Auto Channel* – when checked, the device will automatically select the least loaded radio channel for the Wi-Fi interface. Removing the flag opens the access to install the static operation channel;
- *Channel* – select channel for data transmission;
- *Use Limit Channels* – when checked, the access point will use a user-defined list of channels to work in automatic channel selection mode. If the “Use Limit channels” flag is not checked or there are no

channels in the list, the access point will select the operation channel from all available channels in the given band. 5 GHz range channels: 36-64, 132-144, 149-165;

- *Channel Bandwidth, MHz* – channel bandwidth, on which the access point operates. The parameter may take values of 20, 40 and 80 MHz;
- *Primary Channel* – the parameter can only be changed if the bandwidth of a statically specified channel is equal to 40 MHz. The 40 MHz channel can be considered as consisting of two 20 MHz channels, which border in the frequency range. These two 20 MHz channels are called primary and secondary channels. The primary channel is used by clients who only support 20 MHz channel bandwidth:
 - *Upper* – the primary channel will be the upper 20 MHz channel in the 40 MHz band;
 - *Lower* – the primary channel will be the lower 20 MHz channel in the 40 MHz band.
- *Transmission Power Limit, dBm* – transmitting Wi-Fi signal power adjustment, dBm. May take values between 11 and 19 dBm;
- *Fixed Transmit Rate* – fixed wireless data transmission rate which is defined by IEEE 802.11a/n/ac standards.

- ✓ If the “Use Limit channels” list contains a channel that is not available for selection, it will be marked in grey. In order for the new configuration to be applied to an access point, only available (blue highlighted) channels must be specified in the “Use Limit channels” list.

Example. No settings have been made on the access point yet, Radio 5 GHz is set to 20 MHz “Channel Bandwidth” by default, and channels are specified in the “Use Limit channels” list: 36, 40, 44, 48. Suppose the parameter “Channel Bandwidth” is set to 40 MHz. When you change this parameter from 20 MHz to 40 MHz, the following happens:

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

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

In the “Advanced” section, you can configure advanced device’s radio interface parameters.

Advanced ▾

DFS Support	Enabled ▾
Short Guard Interval	☒
STBC	☐
Beacon Interval, ms	100
Fragmentation Threshold	2346
RTS Threshold	2347
Frame Aggregation	☒
Short Preamble	☒
Broadcast/Multicast Rate Limiting, p/s	☒
	0
Wi-Fi Multimedia (WMM)	☒
Enable QoS	☐

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

- *Broadcast/Multicast Rate Limiting, p/s* – when the flag is set, transmission of broadcast / multicast traffic over the wireless network is restricted. Specify the limit for broadcast traffic in the popup window (p/s);
- *Wi-Fi Multimedia (WMM)* – WMM support activation (Wi-Fi Multimedia);
- *Enable QoS* – when the flag is set, the setting of Quality of Service functions is available.

The following functions are available for quality assurance configuration:

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

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

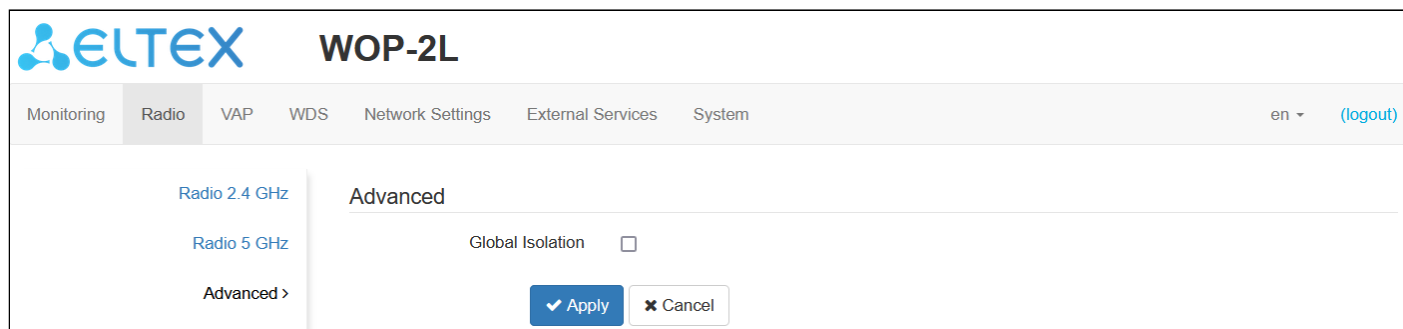
- *AP EDCA parameters* – access point settings table (traffic is transmitted from the access point to the client):
 - *Queue* – predefined queues for various kinds of traffic:
 - *Data 3 (Background)* – low priority queue, high bandwidth (802.1p: cs1, cs2 priorities);
 - *Data 2 (Best Effort)* – middle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

- *Station EDCA parameters* — table of client station parameter settings (traffic is transmitted from the client station to the access point). For description of table fields, see above.

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

5.5.3 The “Advanced” submenu

In the “**Advanced**” section, you can configure advanced device’s radio interface parameters.



The screenshot shows the ELTEX WOP-2L web interface. At the top, there is a navigation bar with the ELTEX logo and the device name 'WOP-2L'. Below this is a menu with tabs: Monitoring, Radio, VAP, WDS, Network Settings, External Services, and System. The 'Radio' tab is selected. On the right side of the navigation bar, there is a language dropdown set to 'en' and a '(logout)' link. The main content area is divided into a left sidebar and a right main panel. The sidebar has three links: 'Radio 2.4 GHz', 'Radio 5 GHz', and 'Advanced >'. The 'Advanced >' link is highlighted. The main panel is titled 'Advanced' and contains a single setting: 'Global Isolation' with an unchecked checkbox. At the bottom right of the main panel, there are two buttons: '✓ Apply' and '✗ Cancel'.

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

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

5.6 The “VAP” menu

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

5.6.1 The “Summary” submenu

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

The screenshot shows the WOP-2L configuration interface. The top navigation bar includes Monitoring, Radio, VAP (selected), WDS, Network Settings, External Services, and System. The VAP menu is open, showing a Summary submenu. The interface is divided into two main sections: 2.4 GHz and 5 GHz. Each section contains a table of VAP configurations. The 2.4 GHz section shows VAP0, VAP1, VAP2, and VAP3. The 5 GHz section shows VAP0, VAP1, VAP2, and VAP3. Each VAP row includes fields for Enabled, Security Mode, VLAN ID, SSID, Broadcast SSID, Band Steer, VLAN Trunk, General Mode, General VLAN ID, and Station Isolation. The VAP0 row in both sections is highlighted, indicating it is the selected VAP. At the bottom of the interface, there are buttons for Apply and Cancel.

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

5 GHz											
VAP	Enabled	Security Mode	VLAN ID	SSID	Broadcast SSID	Band Steer	VLAN Trunk	General Mode	General VLAN ID	Station Isolation	
VAP0	☒	Off		WOP-2L_5GHz	☒	☐	☐	☐		☐	
VAP1	☐	Off		WOP-2L_5GHz-1	☒	☐	☐	☐		☐	
VAP2	☐	Off		WOP-2L_5GHz-2	☒	☐	☐	☐		☐	
VAP3	☐	Off		WOP-2L_5GHz-3	☒	☐	☐	☐		☐	

At the bottom of the interface, there are buttons for **Apply** and **Cancel**.

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

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

5.6.2 The “VAP” submenu

ELTEX WOP-2L

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

Summary

2.4 GHz ▾

VAP0 ▸

VAP1

VAP2

VAP3

5 GHz ▾

VAP0

VAP1

VAP2

VAP3

Common Settings

Enabled ☒

VLAN ID ☒

SSID WOP-2L_2.4GHz

Broadcast SSID ☒

Band Steer ☐

VLAN Trunk ☒

General Mode ☒

General VLAN ID ☒

Station Isolation ☐

802.11k/v ☐

Priority DSCP ▾

Maximum Stations 0 ▾

Minimal Signal -100 ▾

Security Mode WPA/WPA2-Enterprise ▾

Common settings

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

- *Station Isolation* – when checked, traffic isolation between clients in the same VAP is enabled;
- Support for 802.11k/v – enable support for 802.11k/v standards on virtual access point;
- *Priority* – select prioritization means. Defines the field on the basis of which the traffic transmitted to the radio interface will be distributed in WMM queues:
 - *DSCP* – will analyze the priority from the DSCP field of the IP packet header;
 - *802.1p* – will analyze the priority from the CoS (Class of Service) field of the tagged packets.
- *Maximum Stations* – the maximum number of clients connected to the virtual network;
- *Minimal Signal* – signal level in dBm below which the client equipment is disconnected from the virtual network;

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

- *Security Mode* – wireless access security mode:
 - *Off* – do not use encryption for data transfer. The access point is available for any subscriber to connect;
 - *WPA, WPA2, WPA/WPA2* – encryption methods, if you select one of the methods, the following setting will be available:
 - *WPA Key* – key/password required to connect to the virtual access point. The length of the key makes from 8 to 63 characters.
 - *WPA-Enterprise, WPA2-Enterprise, WPA/WPA2-Enterprise* – wireless channel encryption mode, in which the client is authorized on the centralized RADIUS server. To configure this security mode, you must specify the parameters of the RADIUS server. You also need to specify a key for the RADIUS server. If you select one of the methods, the following setting will be available:
 - *Domain* – user domain;
 - *IP Address of RADIUS Server* – RADIUS server address;
 - *Port of RADIUS Server* – port of the RADIUS server that used for aithentication and authorization;
 - *Password of RADIUS Server* – password for the RADIUS server used for authentication and authorization;
 - *Use Accounting through RADIUS* – when checked, “Accounting” messages will be sent to the RADIUS server;
 - *Use Other Settings For Accounting*:

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

Captive Portal

Enable ☒

Virtual Portal Name

Redirect URL

RADIUS

Use Accounting through RADIUS ☒

Domain

IP Address of RADIUS Server for Accounting

Port of RADIUS Server for Accounting

Password of RADIUS Server for Accounting 

Use Periodic Accounting ☒

Accounting Interval

Shapers

Enable ☒

VAP Limit Down ☐ kbps

VAP Limit Up ☐ kbps

STA Limit Down ☐ kbps

STA Limit Up ☐ kbps

✓ Apply

✗ Cancel

Captive Portal

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

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

RADIUS

- *Use Accounting through RADIUS* — when checked, “Accounting” messages will be sent to the RADIUS server;
- *Domain* — user domain;
- *IP Address of RADIUS Server for Accounting* — address of the RADIUS server, used for accounting;
- *Port of RADIUS Server for Accounting* — port that will be used to collect accounts on the RADIUS server;

- *Password of RADIUS Server for Accounting* – password for the RADIUS server used for accounting;
- *Use Periodic Accounting* – enable periodic sending of “Accounting” messages to the RADIUS server. You can set the interval for sending messages in the “Accounting Interval” field.

Shapers

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

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

5.7 The “WDS” menu

In the WDS menu you can configure wireless bridges between WOP-2L.

- ✓ When configuring WDS connection, it is necessary that the same channel and channel width are selected in the radio interface settings on the devices that will connect via WDS.

5.7.1 The “WDS” submenu

ELTEX WOP-2L

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

WDS > 2.4 GHz 5 GHz

Enabled ☒

Security Mode WPA2

WPA Key •••••

WDS Interfaces

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

✓ Apply ✕ Cancel

- # – 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* – interface of WOP-2L and the connected device interaction;
- *Link Capacity* – parameter that displays efficiency of modulation to transmission use by access point. Calculated based on the number of packets transmitted on each modulation to the client, and the reduction factors. Maximum value – 100% (means that all packets are transmitted to the client at maximum modulation for the maximum nss type supported by the client). Minimum value – 2% (in case when packets are transmitted on nss1mcs0 modulation for a client with 3x3 MIMO support). The parameter value is calculated over the last 10 seconds;
- *Link Quality* – parameter that displays the state of the link to the client, calculated based on the number of packet retransmissions 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 over the last 10 seconds;
- *Link Quality Common* – parameter that displays the state of the link to the client, calculated based on packet retransmission 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 entire time of the client connection;
- *RSSI* – received signal level, dBm;
- *SNR* – ratio signal/noise, dB;
- *TxRate* – channel transmission rate, Mbps;
- *RxRate* – receive channel rate, Mbps;
- *TX BW* – transmission bandwidth, MHz;
- *RX BW* – reception bandwidth, MHz;
- *Uptime* – Wi-Fi client connection uptime.

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

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

5.8 The “Network Settings” menu

5.8.1 The “System Configuration” submenu

The screenshot displays the 'System Configuration' submenu within the 'Network Settings' section of the WOP-2L web interface. The sidebar on the left shows 'System Configuration >' and 'Access'. The main configuration area includes the following fields:

- Hostname:** WOP-2L
- AP Location:** root
- Management VLAN:** Forwarding (dropdown menu)
- VLAN ID:** (empty field with a small up/down arrow icon)
- Protocol:** Static (dropdown menu)
- Static IP:** 192.168.1.10
- Netmask:** 255.255.255.0
- Gateway:** XXX:XXX:XXX:XXX
- Primary DNS Server:** XXX:XXX:XXX:XXX
- Secondary DNS Server:** XXX:XXX:XXX:XXX

At the bottom of the form are two buttons: 'Apply' (with a checkmark icon) and 'Cancel' (with an 'X' icon).

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

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

5.8.2 The “Access” submenu

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

The screenshot shows the 'Access' configuration page in the WOP-2L web interface. The page is titled 'WOP-2L' and has a navigation bar with tabs: Monitoring, Radio, VAP, WDS, Network Settings (selected), External Services, and System. The language is set to 'en' and there is a '(logout)' link. On the left, a sidebar shows 'System Configuration' and 'Access >'. The main content area lists various access protocols with checkboxes and input fields:

- WEB**: ☒ (checked)
- HTTP Port**: 80 (input field)
- WEB-HTTPS**: ☒ (checked)
- HTTPS Port**: 443 (input field)
- Telnet**: ☒ (checked)
- SSH**: ☒ (checked)
- NETCONF**: ☒ (checked)
- SNMP**: ☒ (checked)
- roCommunity**: public (input field)
- rwCommunity**: private (input field)
- TrapSink**: (empty input field)
- Trap2Sink**: (empty input field)
- InformSink**: (empty input field)
- Sys Name**: WOP-2L (input field)
- Sys Contact**: Contact (input field)
- Sys Location**: Russia (input field)
- Trap Community**: trap (input field)

At the bottom, there are two buttons: 'Apply' (with a checkmark icon) and 'Cancel' (with an 'x' icon).

- 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”.

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

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

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

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

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

where *eltexLtd* – 1.3.6.1.4.1.35265 is Eltex Enterprise ID.

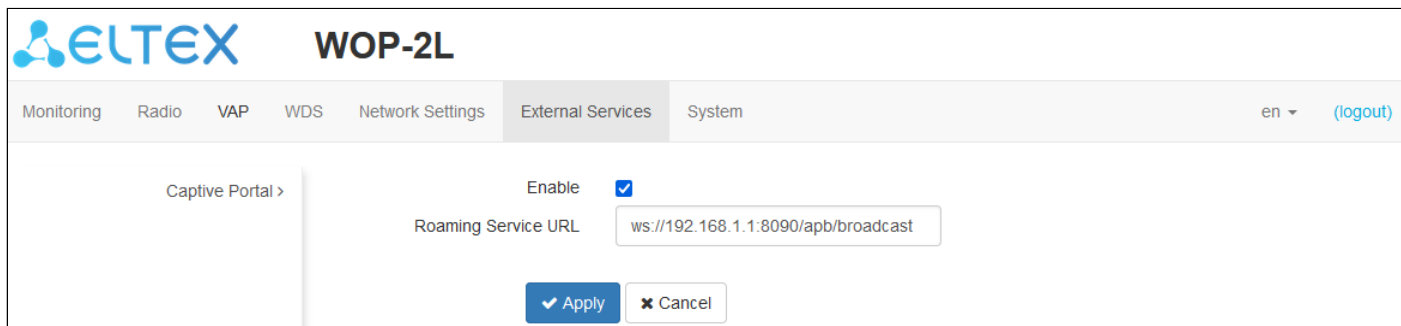
To apply a new configuration and save setting to non-volatile memory, press "Apply". Press "Cancel" to discard the changes.

5.9 The “External Services” menu

5.9.1 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.



The screenshot displays the ELTEX WOP-2L web interface. At the top, there is a navigation bar with tabs: Monitoring, Radio, VAP, WDS, Network Settings, External Services (selected), and System. On the right of the navigation bar, there is a language dropdown set to 'en' and a '(logout)' link. Below the navigation bar, the 'Captive Portal' submenu is expanded on the left. The main content area shows the 'Enable' checkbox checked. Below it, the 'Roaming Service URL' is displayed as 'ws://192.168.1.1:8090/apb/broadcast'. At the bottom of the configuration area, there are two buttons: 'Apply' (with a checkmark icon) and 'Cancel' (with an 'x' icon).

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

5.10 The “System” menu

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

5.10.1 The “Device Firmware Upgrade” submenu

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

The screenshot shows the ELTEX WOP-2L web interface. The top navigation bar includes links for Monitoring, Radio, VAP, WDS, Network Settings, External Services, and System (which is active). On the right of the navigation bar are language settings (en) and a (logout) link. The left sidebar under 'Device Firmware Upgrade >' contains links for Configuration, Reboot, Password, Log, and Date and Time. The main content area displays the 'Active Version' and 'Backup Version' of the firmware. Below these, there is a link to the latest firmware version: 'The latest firmware version is available at: <http://eltex-co.ru/support/downloads/>'. The 'Firmware Image' section has a 'Browse...' button and the text 'No file selected.'. At the bottom of this section is a 'Start Upgrading' button.

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

Firmware update

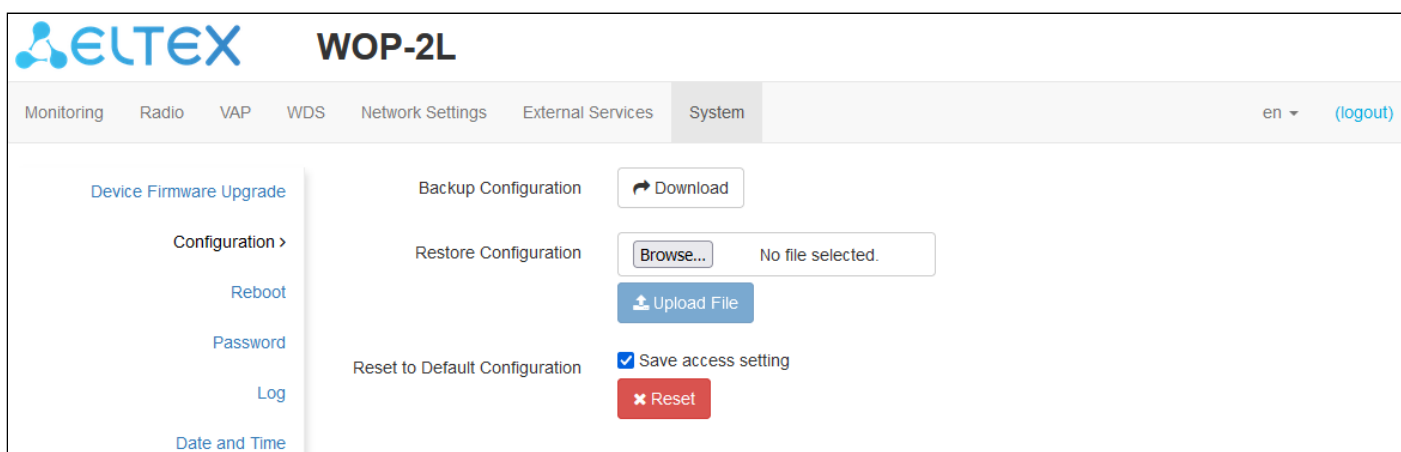
Download the firmware file from <http://eltex-co.com/support/downloads/> and save it on your computer. To do this, click the “Browse” button in the Firmware Image field and specify the path to the firmware file in .tar.gz format.

To start the update process, you must click the “Start Upgrading” button. The process may take several minutes (its current status will be shown on the page). The device will be automatically rebooted when the update is completed.

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

5.10.2 The “Configuration” submenu

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



Backup Configuration

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

Restore Configuration

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

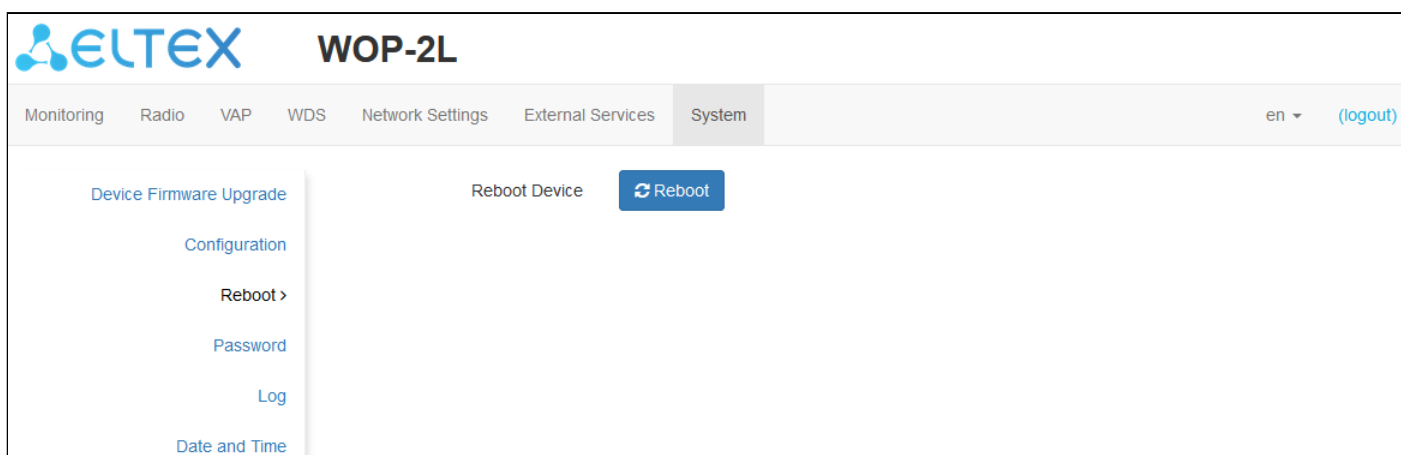
To change the passwords open the configuration file in text editor and change passwords. Then save the changes in configuration archive. The example of password changing is shown below:

Reset to Default Configuration

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

5.10.3 The “Reboot” submenu

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



5.10.4 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 the “Apply” button to save the new password.

The screenshot shows the WOP-2L web interface with the 'System' tab selected. On the left sidebar, the 'Password' option is highlighted. The main content area contains two text input fields labeled 'Password' and 'Confirm Password', each with a toggle icon to the right. Below these fields are two buttons: 'Apply' (with a checkmark icon) and 'Cancel' (with an 'X' icon). The top navigation bar includes links for Monitoring, Radio, VAP, WDS, Network Settings, External Services, and System. The language is set to 'en' and there is a '(logout)' link.

5.10.5 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.

The screenshot shows the WOP-2L web interface with the 'System' tab selected. On the left sidebar, the 'Log' option is highlighted. The main content area contains a 'Mode' dropdown menu set to 'Server and File'. Below it are three input fields: 'Syslog Server Address' (containing 'syslog.server'), 'Syslog Server Port' (containing '514'), and 'File Size, KiB' (containing '1000'). At the bottom are 'Apply' and 'Cancel' buttons. The top navigation bar and language settings are the same as in the previous screenshot.

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

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

5.10.6 The “Date and Time” submenu

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

Manual

The screenshot shows the 'Date and Time' configuration page in Manual mode. The left sidebar contains links for 'Device Firmware Upgrade', 'Configuration', 'Reboot', 'Password', 'Log', and 'Date and Time >'. The main content area has a 'Mode' section with 'Manual' selected. Below it, the 'Date and Time device' is set to '14.12.2021 05:52:45' with an 'Edit' button. The 'Time Zone' is set to 'Moscow, Russia'. The 'Enable daylight saving time' checkbox is checked. The 'DST Start' and 'DST End' fields are set to '(not selected)'. The 'DST Offset (minutes)' is set to '60'. At the bottom, there are 'Apply' and 'Cancel' buttons.

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

NTP server

The screenshot shows the 'Date and Time' configuration page in NTP Server mode. The left sidebar is the same as the previous screenshot. The main content area has a 'Mode' section with 'NTP Server' selected. Below it, the 'Date and Time device' is set to '14.12.2021 05:53:20'. The 'NTP Server' is set to 'pool.ntp.org'. The 'Time Zone' is set to 'Moscow, Russia'. The 'Enable daylight saving time' checkbox is checked. The 'DST Start' and 'DST End' fields are set to '(not selected)'. The 'DST Offset (minutes)' is set to '60'. At the bottom, there are 'Apply' and 'Cancel' buttons.

- **Date and Time device** — date and time set on the device;
- **NTP Server** — time synchronization server IP address/domain name. You can specify an address or select from an existing list;

- *Time Zone* – allows to set the timezone according to the nearest city for your region from the list.
- *Daylight Saving Time Enable* – when selected, automatic daylight saving change will be performed automatically within the defined time period:
 - *DST Start* – day and time, when daylight saving time is starting;
 - *DST End* – day and time, when daylight saving time is ending;
 - *DST Offset (minutes)* – time period in minutes, on which time offset is performing.

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

6 Managing the device using the command line

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

6.1 Connection to the device

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

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

Connection to the device is performed via SSH/Telnet:

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

6.2 Network parameters configuration

Configuration of access point static network parameters

```

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

```

Static routing

```

WOP-2L(config):/interface/br0/common# exit
WOP-2L(config):/interface/br0# exit
WOP-2L(config):/interface# exit
WOP-2L(config):/# route
WOP-2L(config):/route# add default (where default – route name)
WOP-2L(config):/route# default
WOP-2L(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-2L(config):/route/default# netmask X.X.X.X (where X.X.X.X – destination network mask, for default route – 0.0.0.0)
WOP-2L(config):/route/default# gateway X.X.X.X (where X.X.X.X – gateway IP address)
WOP-2L(config):/route/default# save (Save changes)

```

Configuration of reception of the network parameters via DHCP

```

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

```

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

Untagged access

Reception of the network parameters via DHCP:

WOP-2L(root):/# **set-management-vlan-mode off protocol dhcp**

Static settings:

WOP-2L(root):/# **set-management-vlan-mode off protocol static-ip ip-addr X.X.X.X netmask Y.Y.Y.Y gateway Z.Z.Z.Z** (where X.X.X.X – static IP address, Y.Y.Y.Y – subnet mask, Z.Z.Z.Z – gateway)

Access via Management VLAN in Terminating mode

Reception of the network parameters via DHCP:

WOP-2L(root):/# **set-management-vlan-mode terminating vlan-id X protocol dhcp** (where X – VLAN ID used for access to the device. Possible values: 1-4094)

Static settings:

WOP-2L(root):/# **set-management-vlan-mode terminating vlan-id X protocol static-ip ip-addr X.X.X.X netmask Y.Y.Y.Y gateway Z.Z.Z.Z** (where X – VLAN ID used for access to the device. Possible values: 1-4094; X.X.X.X – static IP address, Y.Y.Y.Y – subnet mask, Z.Z.Z.Z – gateway)

Access via Management VLAN in Forwarding mode

Reception of the network parameters via DHCP:

WOP-2L(root):/# **set-management-vlan-mode forwarding vlan-id X protocol dhcp** (where X – VLAN ID used for access to the device. Possible values: 1-4094)

Static settings:

WOP-2L(root):/# **set-management-vlan-mode forwarding vlan-id X protocol static-ip ip-addr X.X.X.X netmask Y.Y.Y.Y gateway Z.Z.Z.Z** (where X – VLAN ID used for access to the device. Possible values: 1-4094; X.X.X.X – static IP address, Y.Y.Y.Y – subnet mask, Z.Z.Z.Z – gateway)

Completion and changes save

WOP-2L(root):/# **save** (Save changes)

6.2.2 IPv6 network parameters configuration

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

Enabling access to the device via IPv6 protocol

```
WOP-2L(root):/# configure
WOP-2L(config):/# interface
WOP-2L(config):/interface# br0
WOP-2L(config):/interface/br0# common
WOP-2L(config):/interface/br0/common# ipv6
WOP-2L(config):/interface/br0/common/ipv6# protocol dhcp (Reception of the IPv6 network parameters via DHCP)
WOP-2L(config):/interface/br0/common/ipv6# enabled true (Enabling access to the device via IPv6 protocol. To disable, enter false)
WOP-2L(config):/interface/br0/common/ipv6# save (Save changes)
```

Configuring static IPv6 network settings for the access point

```
WOP-2L(root):/# configure
WOP-2L(config):/# interface
WOP-2L(config):/interface# br0
WOP-2L(config):/interface/br0# common
WOP-2L(config):/interface/br0/common# ipv6
WOP-2L(config):/interface/br0/common/ipv6# address
XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX (where
XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX – static IPv6 address of the WOP-2L device)
WOP-2L(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-2L(config):/interface/br0/common/ipv6# gateway XXXX:XXXX:XXXX:XXXX::/64 (IPv6 prefix is specified, for example 3211:0:0:1234::/64)
WOP-2L(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-2L(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-2L(config):/interface/br0/common/ipv6# protocol static-ip (Enabling use of static IPv6 networks parameters. For reception of IPv6 the network parameters via DHCP enter dhcp)
WOP-2L(config):/interface/br0/common/ipv6# enabled true (Enabling access to the device via IPv6 protocol. To disable enter false)
WOP-2L(config):/interface/br0/common/ipv6# save (Save changes)
```

6.3 Virtual Wi-Fi access points (VAP) configuration

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

Table 8 — Commands for configuration of security mode on VAP

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

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

6.3.1 Configuration of VAP without encryption

Creation of VAP without encryption

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


6.3.2 Configuration of VAP with WPA-Personal security mode

Creation of VAP with WPA-Personal security mode

```
WOP-2L(root):/# configure
WOP-2L(config):/# interface
WOP-2L(config):/interface# wlan1-va0
WOP-2L(config):/interface/wlan1-va0# vap
WOP-2L(config):/interface/wlan1-va0/vap# ssid 'SSID_WOP-2L_WPA2' (Change SSID name)
WOP-2L(config):/interface/wlan1-va0/vap# security-mode WPA_WPA2 (Encryption mode – WPA/WPA2)
WOP-2L(config):/interface/wlan1-va0/vap#key-wpa password123 (Key/password required to connect to
the virtual access point. The key must be between 8 and 63 characters long)
WOP-2L(config):/interface/wlan1-va0/common# exit
WOP-2L(config):/interface/wlan1-va0# common
WOP-2L(config):/interface/wlan1-va0/common# enabled true (Enable VAP)
WOP-2L(config):/interface/wlan1-va0/vap# save
```

6.3.3 Configuration of VAP with Enterprise authorization

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

```

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

```

6.3.4 Configuration of VAP with Captive Portal

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

```

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

```

6.3.5 Advanced VAP settings

Assignment of VLAN-ID to VAP

```

WOP-2L(config):/interface/wlan1-va0/vap# vlan-id X (where X – VLAN-ID number on VAP)

```

Enabling Band Steer mode

WOP-2L(config):/interface/wlan1-va0/vap# **band-steer-mode true** (Enabling Band Steer mode. To disable, enter **false**)

Enabling VLAN trunk on VAP

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

Enabling General VLAN on VAP

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

WOP-2L(config):/interface/wlan1-va0/vap# **general-vlan-id X** (where X – General VLAN number)

Selection of the prioritization method

WOP-2L(config):/interface/wlan1-va0/vap# **priority-by-dscp false** (Priority analysis from CoS field (Class of Service) tagged packets. Value by default: **true**. In this case, DSCP header field of the IP packet is analyzed)

Enabling use of TLS at authorization

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

Enabling hidden SSID

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

Enabling client isolation on VAP

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

Enabling Minimal Signal

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

Enabling subscribers traffic transmission outside of GRE tunnel

WOP-2L(config):/interface/wlan1-va0/vap/radius# **local-switching true** (Enabling subscribers traffic transmission outside of GRE tunnel. To disable, enter **false**)

Configuring speed limit

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

```
WOP-2L(config):/interface/wlan1-va0/vap# shaper-per-sta-rx
WOP-2L(config):/interface/wlan1-va0/vap/shaper-per-sta-rx# value X (where X — maximum speed in kbps)
WOP-2L(config):/interface/wlan1-va0/vap/shaper-per-sta-rx# mode kbps (Enabling shaper. To disable, enter off)
WOP-2L(config):/interface/wlan1-va0/vap/shaper-per-sta-rx# exit
WOP-2L(config):/interface/wlan1-va0/vap# save (Save changes)
```

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

```
WOP-2L(config):/interface/wlan1-va0/vap# shaper-per-sta-tx
WOP-2L(config):/interface/wlan1-va0/vap/shaper-per-sta-tx# value X (where X — maximum speed in kbps)
WOP-2L(config):/interface/wlan1-va0/vap/shaper-per-sta-tx# mode kbps (Enabling shaper. To disable, enter off)
WOP-2L(config):/interface/wlan1-va0/vap/shaper-per-sta-tx# exit
WOP-2L(config):/interface/wlan1-va0/vap# save (Save changes)
```

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

```
WOP-2L(config):/interface/wlan1-va0/vap# shaper-per-vap-rx
WOP-2L(config):/interface/wlan1-va0/vap/shaper-per-vap-rx# value X (where X — maximum speed in kbps)
WOP-2L(config):/interface/wlan1-va0/vap/shaper-per-vap-rx# mode kbps (Enabling shaper. To disable, enter off)
WOP-2L(config):/interface/wlan1-va0/vap/shaper-per-vap-rx# exit
WOP-2L(config):/interface/wlan1-va0/vap# save (Save changes)
```

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

```
WOP-2L(config):/interface/wlan1-va0/vap# shaper-per-vap-tx
WOP-2L(config):/interface/wlan1-va0/vap/shaper-per-vap-tx# value X (where X — maximum speed in kbps)
WOP-2L(config):/interface/wlan1-va0/vap/shaper-per-vap-tx# mode kbps (Enabling shaper. To disable, enter off)
WOP-2L(config):/interface/wlan1-va0/vap/shaper-per-vap-tx# exit
WOP-2L(config):/interface/wlan1-va0/vap# save (Save changes)
```

802.11r configuration

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

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

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

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

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

Configuring 802.11r on AP1

```
WOP-2L(config):/interface/wlan1-va0/vap/ft-config# enabled false
WOP-2L(config):/interface/wlan1-va0/vap/ft-config# r1-key-holder-id E8:28:C1:FC:D6:80 (MAC address
of VAP. Can be viewed in ifconfig output)
WOP-2L(config):/interface/wlan1-va0/vap/ft-config# r0-key-holder-id 12345 (Unique key for this VAP)
WOP-2L(config):/interface/wlan1-va0/vap/ft-config# mobility-domain 100 (Domain must match on
oncoming VAPs)
WOP-2L(config):/interface/wlan1-va0/vap/ft-config# mac
WOP-2L(config):/interface/wlan1-va0/vap/ft-config/mac# add E4:5A:D4:E2:C4:B0 (MAC address of VAP
interface of oncoming access point – AP2)
WOP-2L(config):/interface/wlan1-va0/vap/ft-config/mac# E4:5A:D4:E2:C4:B0
WOP-2L(config):/interface/wlan1-va0/vap/ft-config/mac/E4:5A:D4:E2:C4:B0# r0-kh-id 23456 (Unique key
of oncoming VAP access point AP2 – r0-key-holder-id)
WOP-2L(config):/interface/wlan1-va0/vap/ft-config/mac/E4:5A:D4:E2:C4:B0# r1-kh-
id E4:5A:D4:E2:C4:B0 (MAC address of oncoming VAP on AP2)
WOP-2L(config):/interface/wlan1-va0/vap/ft-config/mac/E4:5A:D4:E2:C4:B0# r0-kh-key
0102030405060708 (Random key. Must not match r1-kh-key AP1, but necessarily must match r1-kh-key
of oncoming AP2)
WOP-2L(config):/interface/wlan1-va0/vap/ft-config/mac/E4:5A:D4:E2:C4:B0# r1-kh-key
0001020304050607 (Random key. Must not match r0-kh-key AP1, but necessarily must match r0-kh-key
of oncoming AP2)
WOP-2L(config):/interface/wlan1-va0/vap/ft-config/mac/E4:5A:D4:E2:C4:B0# exit
WOP-2L(config):/interface/wlan1-va0/vap/ft-config/mac# exit
WOP-2L(config):/interface/wlan1-va0/vap/ft-config# enabled true (Enabling access point operation via
802.11r protocol)
WOP-2L(config):/interface/wlan1-va0/vap/ft-config# save (Save changes)
```

Configuring 802.11r on AP2

```

WOP-2L(config):/interface/wlan1-va0/vap/ft-config# enabled false
WOP-2L(config):/interface/wlan1-va0/vap/ft-config# r1-key-holder-id E4:5A:D4:E2:C4:B0 (MAC address
of VAP. Can be viewed in ifconfig output)
WOP-2L(config):/interface/wlan1-va0/vap/ft-config# r0-key-holder-id 23456 (Unique key for this VAP)
WOP-2L(config):/interface/wlan1-va0/vap/ft-config# mobility-domain 100 (Domain must match on
oncoming VAPs)
WOP-2L(config):/interface/wlan1-va0/vap/ft-config# mac
WOP-2L(config):/interface/wlan1-va0/vap/ft-config/mac# add E8:28:C1:FC:D6:80 (MAC address of VAP
interface of oncoming access point – AP1)
WOP-2L(config):/interface/wlan1-va0/vap/ft-config/mac# E8:28:C1:FC:D6:80
WOP-2L(config):/interface/wlan1-va0/vap/ft-config/mac/E8:28:C1:FC:D6:80# r0-kh-id 12345 (Unique key
of oncoming VAP access point AP1 – r0-key-holder-id)
WOP-2L(config):/interface/wlan1-va0/vap/ft-config/mac/E8:28:C1:FC:D6:80# r1-kh-
id E8:28:C1:FC:D6:80 (MAC address of oncoming VAP on AP1)
WOP-2L(config):/interface/wlan1-va0/vap/ft-config/mac/E8:28:C1:FC:D6:80# r0-kh-key
0001020304050607 (Random key. Must not match r1-kh-key AP2, but necessarily must match r1-kh-key
of oncoming AP1)
WOP-2L(config):/interface/wlan1-va0/vap/ft-config/mac/E8:28:C1:FC:D6:80# r1-kh-key
0102030405060708 (Random key. Must not match r0-kh-key AP2, but necessarily must match r0-kh-key
of oncoming AP1)
WOP-2L(config):/interface/wlan1-va0/vap/ft-config/mac/E8:28:C1:FC:D6:80# exit
WOP-2L(config):/interface/wlan1-va0/vap/ft-config/mac# exit
WOP-2L(config):/interface/wlan1-va0/vap/ft-config# enabled true (Enabling access point operation via
802.11r protocol)
WOP-2L(config):/interface/wlan1-va0/vap/ft-config# save (Save changes)

```


802.11k configuration

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

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

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

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

802.11k configuring

```
WOP-2L(config):/interface/wlan1-va0/vap/w80211kv-config# enabled false
WOP-2L(config):/interface/wlan1-va0/vap/w80211kv-config# mac
WOP-2L(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-2L(config):/interface/wlan1-va0/vap/w80211kv-config/mac# E8:28:C1:FC:D6:90
WOP-2L(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-2L(config):/interface/wlan1-va0/vap/w80211kv-config/mac/E8:28:C1:FC:D6:90# exit
WOP-2L(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-2Lx(config):/interface/wlan1-va0/vap/w80211kv-config/mac# E8:28:C1:FC:D6:70
WOP-2L(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-2L(config):/interface/wlan1-va0/vap/w80211kv-config/mac/E8:28:C1:FC:D6:70# exit
WOP-2L(config):/interface/wlan1-va0/vap/w80211kv-config/mac# exit
WOP-2L(config):/interface/wlan1-va0/vap/w80211kv-config# enabled true (Enabling access point
operation via 802.11k protocol)
WOP-2L(config):/interface/wlan1-va0/vap/w80211kv-config# save (Save changes)
```

6.4 Radio configuration

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

Change of operation channel and radio interface power

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

6.4.1 Advanced Radio settings

Configuring the limited list of channels

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

Enabling the use of Short Guard Interval

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

Enabling STBC

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

Enabling aggregation

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

Enabling the short preamble

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

Enabling the Wi-Fi Multimedia (WMM)

WOP-2L(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-2L(config):/interface/wlan1/wlan/radio-5g# **dfs X** (where X – DFS mechanism operating mode. May take values: **forced** – the mechanism is disabled, DFS channels available for selection; **auto** – the mechanism is enabled; **disabled** – the mechanism is disabled, DFS channels unavailable for selection)

Enabling automatic channel width switch mode

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

Enabling Broadcast/Multicast shaper

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

Enabling QoS and parameter changes

WOP-2L(config):/interface/wlan0/wlan/radio-2g# **qos**

WOP-2L(config):/interface/wlan0/wlan/radio-2g/qos# **enable true** (Enabling the use of Quality of Service functions. To disable, enter **false**)

WOP-2L(config):/interface/wlan0/wlan/radio-2g/qos# **edca-ap** (Configuring the access point's QoS parameters (traffic is transmitted from the access point to the client))

WOP-2L(config):/interface/wlan0/wlan/radio-2g/qos/edca-ap# **bk** (Configure QoS parameters for low-priority high-bandwidth queues (802.1p priorities: cs1, cs2))

WOP-2L(config):/interface/wlan0/wlan/radio-2g/qos/edca-ap/bk# **aifs X** (where X – the time frame(s) of data measured in slots. Takes the values 1-255)

WOP-2L(config):/interface/wlan0/wlan/radio-2g/qos/edca-ap/bk# **cwmin X** (X – The initial value of the waiting time before sending the frame again is set in milliseconds. Takes the following values: 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023. The value of cwMin may not exceed the value of cwMax)

WOP-2L(config):/interface/wlan0/wlan/radio-2g/qos/edca-ap/bk# **cwmax X** (where X – The maximum waiting time before resending a frame is set in milliseconds. Takes the following values: 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023. The value of cwMax must be greater than the value of cwMin)

WOP-2L(config):/interface/wlan0/wlan/radio-2g/qos/edca-ap/bk# **txop X** (where X – The time interval, in milliseconds, in which the client WME station is allowed to initiate data transmission over the wireless environment to the access point. Max value – 65535 ms)

WOP-2L(config):/interface/wlan0/wlan/radio-2g/qos/edca-ap/bk# **exit**

WOP-2L(config):/interface/wlan0/wlan/radio-2g/qos/edca-ap# **exit**

WOP-2L(config):/interface/wlan0/wlan/radio-2g/qos# **edca-sta** (Configuring the client station QoS parameters (traffic is transmitted from the client station to the access point))

The configuration method of **edca-sta** is the same as that of **edca-ap**.

Parameters configuration for queues **be**, **vi**, **vo** is similar to parameters configuration for queue **bk**.

6.5 WDS configuring

- ✓ When configuring WDS connection, it is necessary that the same channel and channel width are selected in the radio interface settings on the devices that will connect via WDS. For more information on configuring the radio interface via the command line, see the Radio Settings section.

Configuring WDS connection on Radio 5 GHz interface (wlan1) is given below.

WDS configuring

```
WOP-2L(root):/# configure
WOP-2L(config):/# interface
WOP-2L(config):/interface# wlan1-wds0 (Selecting WDS link. Possible values for Radio 2,4 GHz: wlan0-wds0 — wlan0-wds3); for Radio 5 GHz : wlan1-wds0 — wlan1-wds3)
WOP-2L(config):/interface/wlan1-wds0# wds-5 (When configuring WDS on Radio 2,4 GHz, enter wds-2)
WOP-2L(config):/interface/wlan1-wds0/wds-5# mac-addr XX:XX:XX:XX:XX:XX (MAC address of oncoming access point Radio interface, which can be viewed if entering the command monitoring radio-2 or monitoring radio-5 on the oncoming access point, depending on which range the configured WDS connection will operate in)
WOP-2L(config):/interface/wlan1-wds0/wds-5# exit
WOP-2L(config):/interface/wlan1-wds0# common
WOP-2L(config):/interface/wlan1-wds0/common# enabled true (Enabling WDS link. To disable, enter false)
WOP-2L(config):/interface/wlan1-wds0/common# exit
WOP-2L(config):/interface/wlan1-wds0# exit
WOP-2L(config):/interface# wlan1 (When configuring WDS on Radio 2,4 GHz, enter wlan0)
WOP-2L(config):/interface/wlan1# wlan
WOP-2L(config):/interface/wlan1/wlan# wds
WOP-2L(config):/interface/wlan1/wlan/wds# security-mode WPA2 (Selecting WPA2 security mode. Possible values: WPA, off — without password)
WOP-2L(config):/interface/wlan1/wlan/wds# key-wpa password123 (Key/password, necessary for connection to the oncoming access point. . Key length is from 8 to 63 characters)
WOP-2L(config):/interface/wlan1/wlan/wds# enabled true (Enabling WDS. To disable, enter false)
WOP-2L(config):/interface/wlan1/wlan/wds# save
```

Oncoming access point is configured analogically.

6.6 System settings

6.6.1 Device firmware update

Device firmware update via tftp

```
WOP-2L(root):/# firmware upload tftp <tftp server ip address> <Firmware image name> (Example: firmware upload tftp 192.168.1.15 WOP-2L-1.2.2_build_X.tar.gz)
WOP-2L(root):/# firmware upgrade
```

Device firmware update via http

WOP-2L(root):/# **firmware upload http** <URL to download Firmware image> (Example: firmware upload http http://192.168.1.100:8080/files/WOP-2L-1.2.2_build_X.tar.gz)
 WOP-2L(root):/# **firmware upgrade**

Switching to access point firmware backup

WOP-2L(root):/# **firmware switch**

6.6.2 Device configuration management

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

WOP-2L(root):/# **manage-config reset-to-default**

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

WOP-2L(root):/# **manage-config reset-to-default-without-management**

Download the device configuration file to tftp server

WOP-2L(root):/# **manage-config download tftp** <tftp server ip address> (Example: manage-config download tftp 192.168.1.15)

Download configuration file from tftp server to the device

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

6.6.3 Device reboot

The command to reboot the device

WOP-2L(root):/# **reboot**

6.6.4 Setting the date and time

Commands to configure NTP server time synchronization

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

6.6.5 Advanced system settings

Enabling global isolation

```
WOP-2L(root):/# configure
WOP-2L(config):/# system
WOP-2L(config):/system# global-station-isolation true (Enabling global traffic isolation between customers of different VAP и different radio interfaces. To disable, enter false)
WOP-2L(config):/system# save (Save changes)
```

Changing device name

```
WOP-2L(root):/# configure
WOP-2L(config):/# system
WOP-2L(config):/system# hostname WOP-2L_room2 (where WOP-2L_room2 – new name of the device. A parameter can contain from 1 to 63 symbols: capital и lowercase latin letters, numbers, hyphen character "-" (hyphen can not be the last character in name). By default: WOP-2L)
WOP-2L(config):/system# save (Save changes)
```

Changing geographical domain

```
WOP-2L(root):/# configure
WOP-2L(config):/# system
WOP-2L(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-2L(config):/system# save (Save changes)
```

Changing password

```
WOP-2L(root):/# configure
WOP-2L(config):/# authentication
WOP-2L(config):/authentication# admin-password newpassword (where newpassword — new password
to login to the access point. By default: password)
WOP-2L(config):/authentication# save (Save changes)
```

6.7 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-2L(root):/# configure
WOP-2L(config):/# captive-portal
WOP-2L(config):/captive-portal# apbd
WOP-2L(config):/captive-portal/apbd# roam_service_url < APB service address >
(Example: roam_service_url ws://192.168.1.100:8090/apb/broadcast)
WOP-2L(config):/captive-portal/apbd# enabled true (Enabling APB service. To disable it, enter false)
WOP-2L(config):captive-portal/apbd# save
```

6.8 Monitoring

6.8.1 Wi-Fi Clients

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

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

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

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

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

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

```
WOP-2L(root):/# monitoring associated-clients <Tab>
```

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

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

```
WOP-2L(root):/# monitoring associated-clients all filter <Tab>
```

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

Display information on all connected clients

WOP-2L(root):/# monitoring associated-clients (or monitoring associated-clients all)

```

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

```

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

Rate	Transmitted	Received
------	-------------	----------

ofdm6	9	0%	378	5%
mcs7	2	0%	0	0%
mcs11	0	0%	3	0%
mcs12	28	0%	66	1%
mcs14	1183	14%	0	0%
mcs15	6943	85%	5939	93%

Multicast groups:

MAC	IP
01:00:5E:00:00:FB	xxx.0.0.251

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

Rate	Transmitted	Received
Total Packets:	178	263
TX success:	100	
Total Bytes:	68476	38913
Data Packets:	174	207
Data Bytes:	63720	32019
Mgmt Packets:	4	56
Mgmt Bytes:	232	240

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

Multicast groups: none

Display information on specific client/clients

WOP-2L(root):/# **monitoring associated-clients bc:2e:f6:cc:85:46** (there is a possibility to specify several mac addresses, eg., **monitoring associated-clients bc:2e:f6:cc:85:46 32:5b:60:62:e0:a4**)

```

index                | 1
interface          | wlan1-va2
state                | ASSOC SLEEP AUTH_SUCCESS
hw-addr              | bc:2e:f6:cc:85:46
ssid                 | 2ac-enter
ip-addr              | 10.24.80.90
hostname             | HUAWEI_P40_Pro-81afe9c34a
username             | tutu
domain               | enterprise.service.root
authorized            | true
captive-portal-vap   | false
enterprise-vap       | true
rx-retry-count       | 9
tx-fails             | 0
tx-period-retry      | 0
tx-retry-count       | 1
rssi-1               | -39
rssi-2               | -57
snr-1                | 14
snr-2                | 13
tx-rate              | MCS15 NO SGI 130
rx-rate              | MCS15 NO SGI 130
rx-bw                | 20M
rx-bw-all           | 20M
tx-bw                | 20M
uptime               | 00:01:12
multicast-groups-count | 0
wireless-mode        | ac
perftest-capable     | false
snr-rssi-capable     | false
link-capacity        | 100
link-quality         | 100
link-quality-common   | 99
actual-tx-rate       | 1
actual-rx-rate       | 0
shaped-rx-rate       | 0
actual-tx-pps        | 1
actual-rx-pps        | 0
shaped-rx-pps        | 0
name                 | 1

```

Rate	Transmitted	Received
------	-------------	----------

Total Packets:	312	483
TX success:	100	
Total Bytes:	112678	55795
Data Packets:	308	295
Data Bytes:	104438	43445
Mgmt Packets:	4	188

Mgmt Bytes:	232	240		
Rate	Transmitted		Received	
ofdm6	21	6%	103	21%
ofdm24	0	0%	105	21%
mcs7	15	4%	0	0%
mcs12	41	13%	0	0%
mcs13	43	13%	0	0%
mcs14	0	0%	4	0%
mcs15	192	61%	270	56%

Multicast groups: none

Filtering monitoring parameters

WOP-2L(root):/# **monitoring associated-clients 32:5b:60:62:e0:a4 filter hw-addr ip-addr tx-rate rx-rate uptime** (display of a limited number of monitoring parameters for a certain client. It is possible to specify several mac addresses)

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

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

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

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

6.8.2 WDS

To monitor WDS connections, use the following command:

monitoring wds-entries <mac address of oncoming access point 1> ... <mac address of oncoming access point N> **filter** <parameter 1> ... <parameter N>, where <mac address of oncoming access point 1> ... <mac address of oncoming access point N> – mac addresses of oncoming access points, with which WDS bridges are built. In order to display information for all oncoming access points, instead of <mac address of oncoming access point> enter **all**;

filter – a special word followed by the monitoring parameters required for display of one or several oncoming access points;

<parameter 1> ... <parameter N> – monitoring parameter/parameters, necessary for display of one or several oncoming access points.

To display a list of access points with which WDS bridges are built, press Tab after **monitoring wds-entries**.

WOP-2L(root):/# **monitoring wds-entries** <Tab>

```
e8:28:c1:d1:43:15
e8:28:c1:da:cb:80
all
```

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

WOP-2L(root):/# **monitoring wds-entries all filter** <Tab>

```
index
interface
hw-addr
state
ip-addr
hostname
rx-retry-count
tx-fails
tx-period-retry
tx-retry-count
noise-1
noise-2
rssi-1
rssi-2
.....
```

Display information for all oncoming access points

WOP-2L(root):/# monitoring wds-entries (or monitoring wds-entries all)

```

index                | 0
interface            | wlan1
state                | WIFI_WDS
hw-addr              | e8:28:c1:d1:43:15
ip-addr              | 10.24.80.35
hostname              | WOP-2L
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 | 1.2.2 build X
eltex-board-type       | WOP-2L
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

```

index | 1
interface | wlan1
state | WIFI_WDS
hw-addr | e8:28:c1:da:cb:80
ip-addr | 10.24.80.40
hostname | WOP-2L
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 | -75
rssi-2 | -70
snr-1 | 40
snr-2 | 39
wds-interface | wlan1-wds2
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 | 00:07:15
multicast-groups-count | 0
wireless-mode | ac
eltex-firmware-version | 1.2.2 build X
eltex-board-type | WOP-2L
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

Display information on one or several oncoming access points

WOP-2L(root):/# monitoring wds-entries e8:28:c1:d1:43:15 (It is possible to specify several mac addresses, eg., monitoring wds-entries e8:28:c1:d1:43:15 e8:28:c1:da:cb:80)

```

index                | 0
interface          | wlan1
state                | WIFI_WDS
hw-addr              | e8:28:c1:d1:43:15
ip-addr              | 10.24.80.35
hostname              | WOP-2L
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 | 1.2.2 build X
eltex-board-type      | WOP-2L
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

Filtering monitoring parameters

WOP-2L(root):/# **monitoring wds-entries e8:28:c1:d1:43:15 filter hw-addr ip-addr tx-rate rx-rate uptime**
(display of a limited number of monitoring parameters for access point. It is possible to specify several mac addresses)

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

WOP-2L(root):/# **monitoring wds-entries all filter hw-addr rssi-1 rssi-2 wireless-mode wds-interface eltex-firmware-version**
(display of a limited number of monitoring parameters for all access points)

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

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

6.8.3 Device info

WOP-2L(root):/# monitoring information

```
system-time: 09:15:16 28.10.2021
uptime: 15:45:10
software-version: 1.2.2 build X
secondary-software-version: 1.2.2 build X
boot-version: 1.2.2 build X
memory-usage: 67
memory-free: 34
memory-used: 71
memory-total: 105
cpu: 0.28
is-default-config: true
board-type: WOP-2L
hw-platform: WOP-2L
factory-wan-mac: E8:28:C1:xx:xx:xx
factory-lan-mac: E8:28:C1:xx:xx:xx
factory-serial-number: WP39000059
hw-revision: 1v1
session-password-initialized: false
ott-mode: false
last-reboot-reason: firmware update
test-changes-mode: false
```

6.8.4 Network information

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

```

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

```

WOP-2L(root):/# monitoring ethernet

```

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

```

WOP-2L(root):/# monitoring arp

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

WOP-2L(root):/# monitoring route

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

6.8.5 Wireless interfaces

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

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

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

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

6.8.6 Event logging

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

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

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

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

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

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

6.8.7 Environment scan

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

WOP-2L(root):/# **monitoring scan-wifi**

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

6.8.8 Spectrum Analyzer

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

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

✓ The spectrum analyzer 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 section.

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

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

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

7 The list of changes

Document version	Issue date	Revisions
Version 1.2	24.01.2022	Sincronization with firmware version 1.2.2 Added sections: • 5.4.2 The "WDS" submenu • 5.7 The "WDS" menu • 6.2.1 Network parameters configuration via set-management-vlan-mode utility • 6.2.2 IPv6 network parameters configuration • 6.5 WDS configuring • 6.6.5 Advanced system settings • 6.8.2 WDS • 6.8.7 Environment scan Corrected: • 2.2 Device specification • 5.6.1 The "Summary" submenu • 5.6.2 The "VAP" submenu • 6.3.5 Advanced VAP settings • 6.8.1 Wi-Fi Clients • 6.8.3 Device info
Version 1.1	30.06.2020	Sincronization with firmware version 1.1.0
Version 1.0	16.03.2020	First issue
Firmware version 1.2.2		

TECHNICAL SUPPORT

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

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

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

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

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