Base station
WOP-2ac-LR2
User manual

Firmware version 1.10.0

IP address: 192.168.1.10
Username: admin
Password: password

Contents

1 Introduction

Annotation

Modern tendencies of telecommunication development necessitate operators to search for the most optimal technologies, allowing you to satisfy drastically 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-2ac-LR2 is designed to organize Broadband wireless networks in private housing, that provide broadband access to the Internet in the range of 3 km. The device is a good choice for wireless network construction in a difficult climatic conditions. WOP-2ac-LR2 operates well in a wide operating temperature range and in high humidity (different climatic zones). The device allows connecting different sector antennas.

This manual specifies intended purpose, main technical parameters, design, installation procedure, safe operation rules and installation recommendations for WOP-2ac-LR2.

Symbols

Notes and warnings

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

> ⬥ **Warnings are used to inform the user about harmful situations for the device and the user alike, which could cause malfunction or data loss.**

2 Device description

2.1 Purpose

The base station WOP-2ac-LR2 (herein after 'the device') is designed to provide broadband Internet access to subscribers within a range of up to 3 km and to organize wireless bridges (WDS).
The base station – an up-to-date flexible solution that provides extending coverage zone due to its power of the transmitter (up to 26 dBm) and sectoral antennas. It is possible to deploy wireless IT infrastructure fast and easily by virtue of high-performance hardware, scalability and intuitive interface.
The PoE+ technology makes it possible to install the equipment virtually anywhere, regardless of the power supply location, reduces total cost by discarding power cables and performs the installation easier and faster.

2.2 Device specification

Interfaces:

- 1 Combo port 10/100/1000BASE-T (Ethernet)/100/1000BASE-X (SFP);
- 2 SMA (female) connectors for connecting external antennas. The choice of model depends on the use of the access point: for wireless bridges, it is preferable to choose narrowly oriented antennas, and in base station mode, sector antennas with a wider radiation pattern;
- Wi-Fi 2.4 GHz IEEE 802.11b/g/n.

The power is supplied via PoE injector (IEEE 802.3at-2009).

Functions:

WLAN capabilities:

- support for IEEE 802.11b/g/n;
- data aggregation, including A-MPDU (Tx /Rx) and A-MSDU (Rx);
- WMM-based priorities and packet planning;
- support for hidden SSID;
- 4 virtual access points;
- MAC ACL;
- external access point detection;
- APSD;
- spectrum analyzer;
- support for wireless bridges (WDS);
- Polling;
- support for fixed center frequency;
- intersectoral synchronization (PTP) [1] .

Network functions:

- autonegotiation of speed, duplex mode and switching between MDI and MDI-X modes;
- support for VLAN (Access, Trunk, General);
- DHCP client;
- VLAN mapping;
- support for NTP;
- support for Syslog;
- DHCP snooping;
- IGMP snooping (with possibility to limit the number of groups);
- BPDU filtering;
- support for Ping Watchdog.

---

[1]For WOP-2ac-LR2 SYNC only

QoS functions

- bandwidth limiting for each SSID;
- client data rate limiting for each SSID;
- changing WMM parameters for each radio interface;
- support for prioritization by CoS, DSCP and VLAN ID.

Security:

- centralized authorization via RADIUS server (WPA Enterprise);
- WPA/WPA2 data encryption;
- 64/128/152-bit WEP data encryption;

Figure 1 shows an equipment operation diagram for WOP-2ac-LR2.
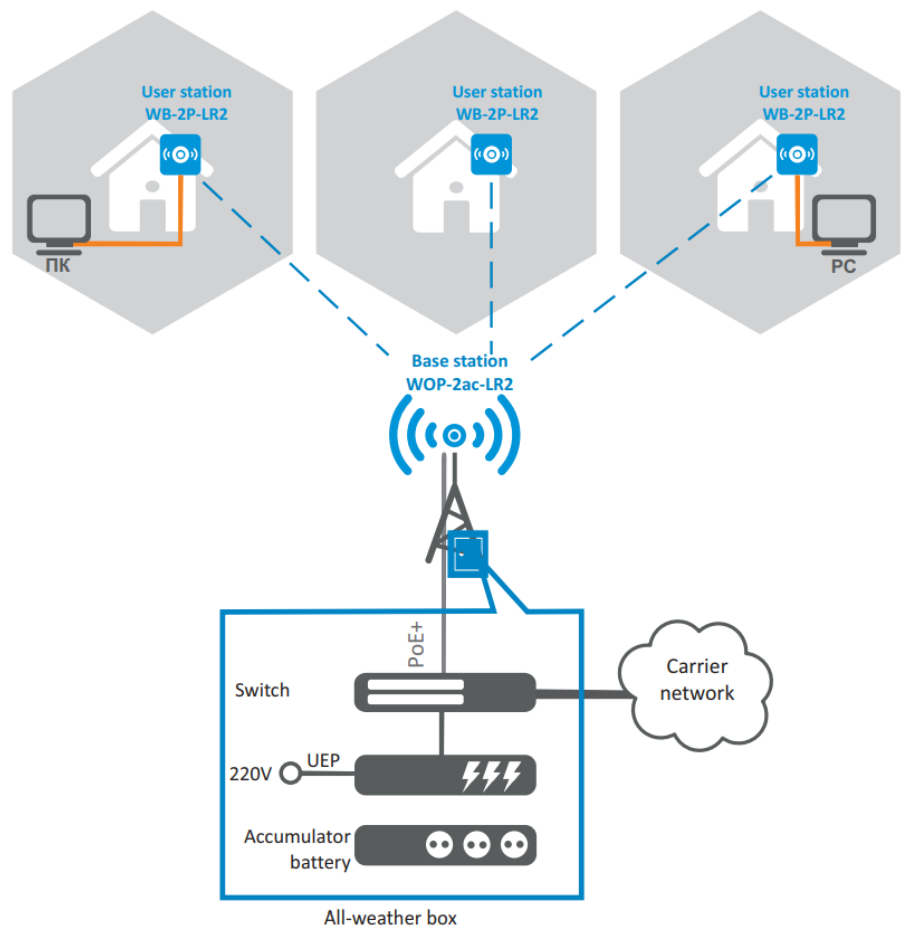
Figure 1 – WOP-2ac-LR2 operation diagram

2.3 Technical features

Table 1 shows main specifications of the device.

Table 1 – Main specifications

Ethernet interface parameters	
Number of ports	1
Electrical connector	RJ-45/SFP

Data rate, Mbps	10/100/1000, auto-negotiation
Standards	BASE-T/BASE-X
Port features	Combo port
Wireless interface parameters	
Standards	802.11b/g/n
Frequency range	2402–2482 MHz
Modulation	DSSS, CCK, BPSK, QPSK, 16QAM, 64QAM
Data transfer rate[1]	**802.11b:** up to 11 Mbps **802.11g:** up to 54 Mbps **802.11n:** up to 300 Mbps
Maximum transmitter output power[2]	**2.4 GHz:** 26 dBm
Receiver sesitivity	**2.4 GHz:** up to -98 dBm
Security	64/128/152- bit WEP encryption, WPA/WPA2, centralized authorization via RADIUS server (WPA/WPA2 Enterprise)
Control	
Remote control	Web interface, CLI, Telnet, SSH, SNMP (), NETCONF
Access restriction	Local authentication and authentication via RADIUS server
General parameters	
RAM	128 MB
Flash	32 MB
Power supply	PoE+ (IEEE 802.3at-2009)

Power consumption	up to 13 W
Operating temperature	from -45 to +65°C
Relative humidity at 25°C	up to 95%
Ingress Protection Marking	IP54
Dimensions	88x232,5x47 mm
Weight	0,32 kg

[1] The maximum wireless data rate is defined according to IEEE 802.11b/g/n standard. The real bandwidth can be different. Conditions of the network, environment, the amount of traffic, building materials and constructions and network service data can decrease the real bandwidth. The environment can influence on the network coverage range.

[2] The number of channels and the value of the maximum output power will vary according to the rules of radio frequency regulation in your country.

2.4 Design

WOP-2ac-LR2 housed in a plastic case, industrial version. The size of the device: 88x232.5x47 mm. The layout of WOP-2ac-LR2 is shown in the Figure 2.

Figure 2 – WOP-2ac-LR2 layout

Combo port 10/100/1000BASE-T (Ethernet)/100/1000BASE-X (SFP) for local network connection and power supply via PoE, grounding connector and the button for resetting to factory settings (F) are located on the bottom panel of the device, Figure 3.

Figure 3 – WOP-2ac-LR2 ports

2.5 Light indication

The layout of WOP-2ac-LR2 indication panel is shown in the Figure 4.

Figure 4 – WOP-2ac-LR2 indication panel layout

The current state of the device is shown with the help of light indicators located on the front panel of WOP-2ac-LR2. The list of indicators and their description is shown in the table below.

Table 2 – Indicator description

	LED	LED status	Description
	Power – power and operation status indicator	solid green	the device power supply is enabled, normal operation
		solid orange	the device is loaded but IP address is not received via DHCP
		solid red	the device is loading
	LAN – Ethernet interface port indicator	solid green (10, 100 Mbps)/solid orange (1000 Mbps)	the channel between Ethernet interface of WOP-2ac-LR2 and connected device is active

		flashes	packet data transmission between Ethernet interface of WOP-2ac-LR2 and connected device
	WLAN – received signal strength indicator (RSSI)	solid red	the signal level is more than -98 dBm
		solid yellow	the signal level is more than -80 dBm
		solid green	the signal level is more than -70 dBm
		solid green	the signal level is more than -60 dBm
		none of the LEDs is on	no signal

2.6 Reset to factory 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.

> ✅ The device will be rebooted automatically. DHCP client will be launched by default. If the address is not received via DHCP the device will have IP address — *192.168.1.10*, subnet mask — *255.255.255.0*; User Name/Password to access via Web interface — admin/password.

2.7 Delivery package

The basic supply package of WOP-2ac-LR2 includes:

- Base station WOP-2ac-LR2;
- Mounting kit;
- Patch cord RJ-45, 5e cat. 1.5 m;
- User manual on a CD (optional);
- Conformity certificate;
- Information leaflet;
- Technical passport.

3 Installation order

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. Do not install the device during a thunderstorm. There is a risk of lightning stroke.
3. You must follow requirements for voltage, current and frequency specified in the user manual.
4. Measuring devices and computer must be grounded before connecting to the device. The electric potential differnce between devices' cases should not exceed 1 V.
5. Make sure that all the cables are intact and they are reliably attached to connectors.
6. You should satisfy established standards and requirements for working at height during the device installation on the high-rise constructions.
7. The device exploitation should be performed by specially prepared engineering and technical personnel.
8. Connect only to operational service equipment.

3.2 Installation recommendations

1. Recommended location for device installation: communications mast/pole.
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. Install the device on communications mast or pole in the way that the Ethernet port is pointed down.
4. During the device installation to provide Wi-Fi coverage area with the best characteristics take into account the following rules:
   a. Install the device in such a way that all subscriber stations that should be connected to this BS fall into the antenna radiation range;
   b. Do not install the device near (about 2 m) electrical and radio devices;
   c. It is not advised to use radio-phones and other devices, working on frequency of 2.4 GHz, within a range of Wi-Fi wireless network;
   d. Obstacles in the form of glass/metal constructions, brick/concrete walls, water cans and mirrors can significantly reduce Wi-Fi action radius.
5. During the installation of several access points on the same mast it is recommended to distribute them vertically at least 2 meters.

3.2.1 Frequency bands and channels in the range of 2.4 GHz for Wi-Fi

Data transmission in the 2.4 GHz band is used for IEEE 802.11b/g/n standards. WOP-2ac-LR2 supports frequency channels in the range of 2.4 GHz with the bandwidth of 5, 10, 20 and 40 MHz.
To calculate the Wi-Fi channel central frequency, MHz, use the equation:
$f=2407+(5*N)$, where N – Wi-Fi channel number.

3.3 Recommendations for lightning protection

1. The grounding shall be made with insulated stranded wire. The grounding device and the cross-section of the grounding wire must comply with the requirements of the Electrical Code of Practice.
2. The first outdoor lightning protection should be installed as close as possible to the base station, connecting them with a short outdoor FTP cable with shielded connectors.
3. The second outdoor lightning protection should be installed as close as possible to the PoE switch (PoE injector), connecting them with a short outdoor FTP cable with shielded connectors.
4. The lightning protectors are connected to each other by an outdoor FTP cable up to 100 m long.
5. The sector antenna must be grounded through the antenna mount mast.
6. It is necessary to ground the base station (for more information, see Mounting the device).
7. The PoE switch (PoE injector) must be connected to a 220V electrical outlet with ground or grounded through the housing.
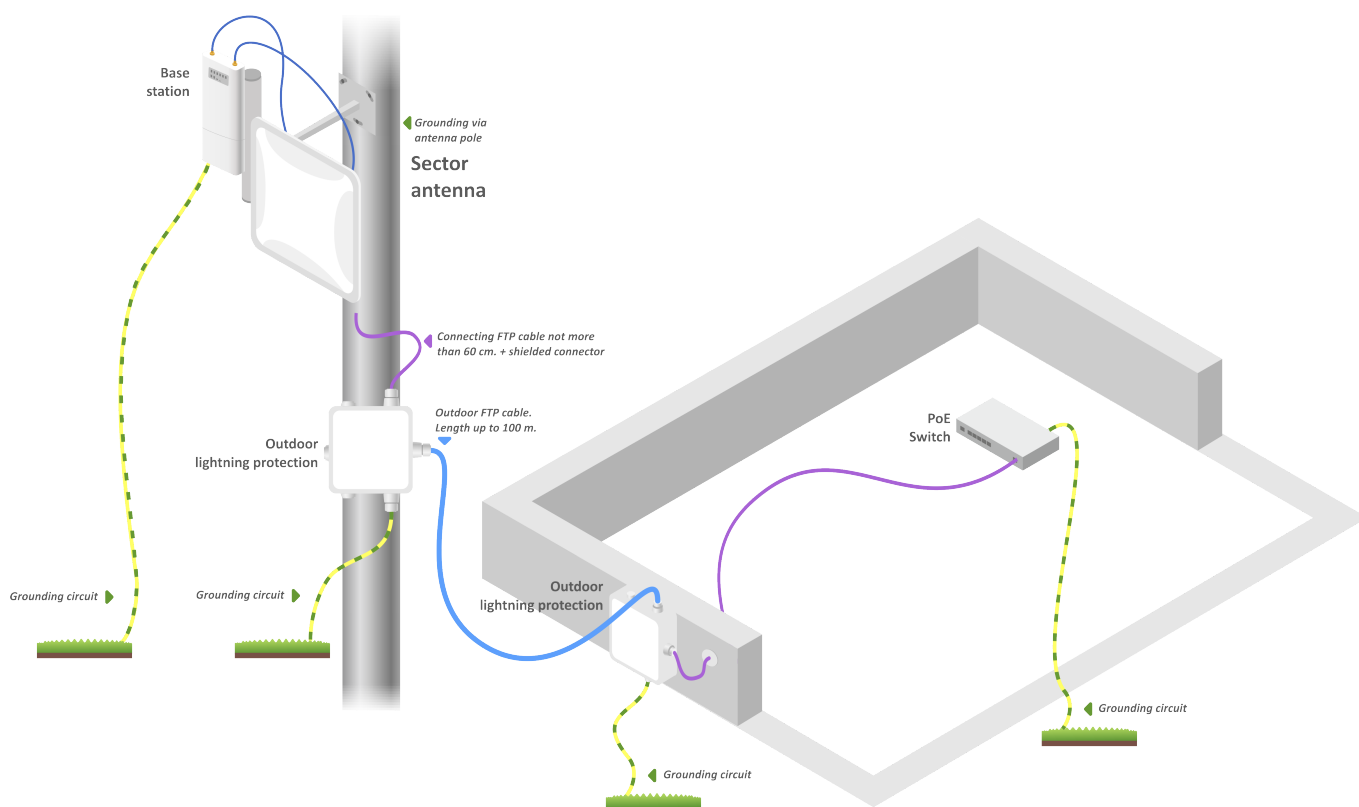
Wiring diagram of the base station to provide lightning protection

3.4 WOP-2ac-LR2 mounting

1. Attach the bracket to the device with the screws provided, as shown in the figure below.
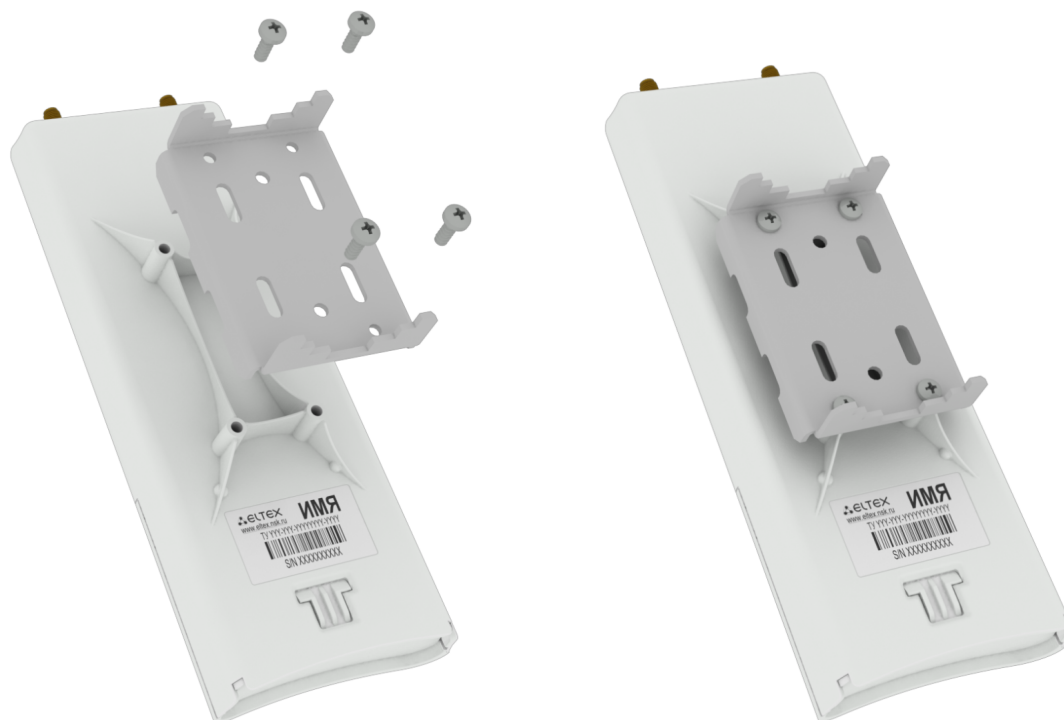
2. Install the device on communications mast/pole pointing Ethernet port down as it is shown on the figure below. Attach the device using clamps supplied in the device package. Comply the safety rules and recommendations given in Safety rules and Installation recommendations.
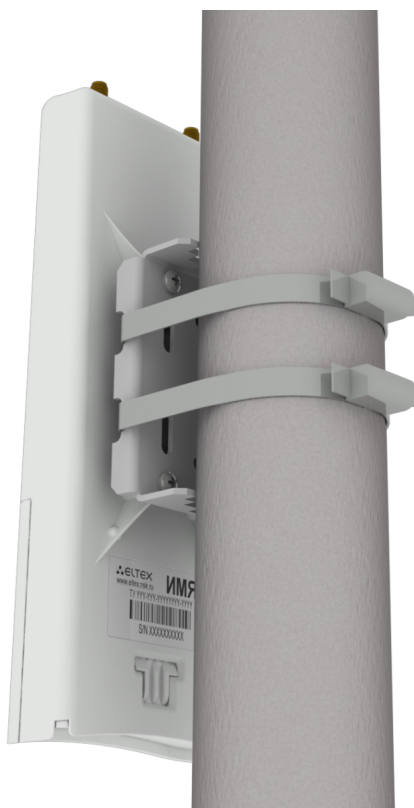
3. Remove the bottom cover which close Ethernet port. Ground the device through a grounding connector, then connect the Ethernet cable to the PoE port. When building a network over fiber, install the transceiver and make the connection.

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 form WOP-2ac-LR2 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.
9. Align the antenna more accurately using the LEDs on the device.

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

3.4.1   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 5 (a, b).

Figure 5a

Figure 5b

2. Connect the cable to the connector of the device (antenna) and tighten the nut, as shown in Figure 6 (a, b).

Figure 6a

Figure 6b

3. Cut the rubber sealing tape to the appropriate length: 0.15 m of waterproofing tape is required to seal one SMA connector (Figure 26a), 0.3 m of waterproofing tape is required for an N-type connector (Figure 6b), as shown in Figure 7 (a,b).
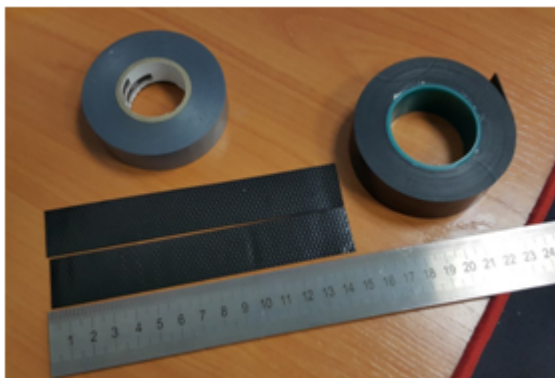
Figure 7a

Figure 7b

4. Remove the protective layer from the rubber band as shown in Figure 8.
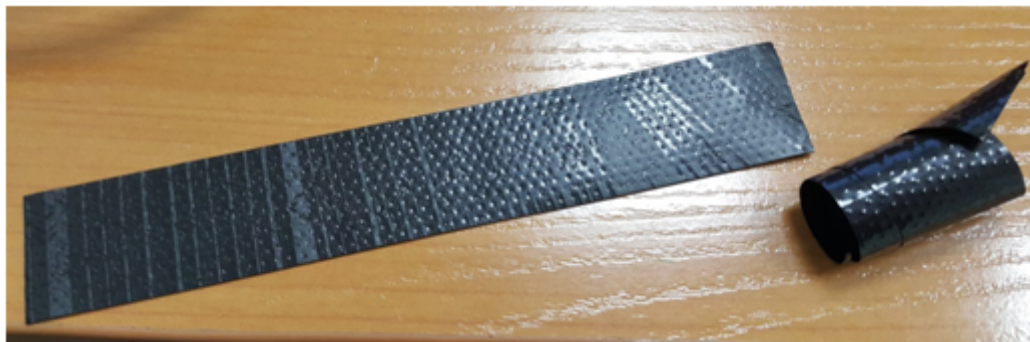
Figure 8

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 9 (a, b).

Figure 9a

Figure 9b

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 10 (a, b).

Figure 10a

Figure 10b

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 11.
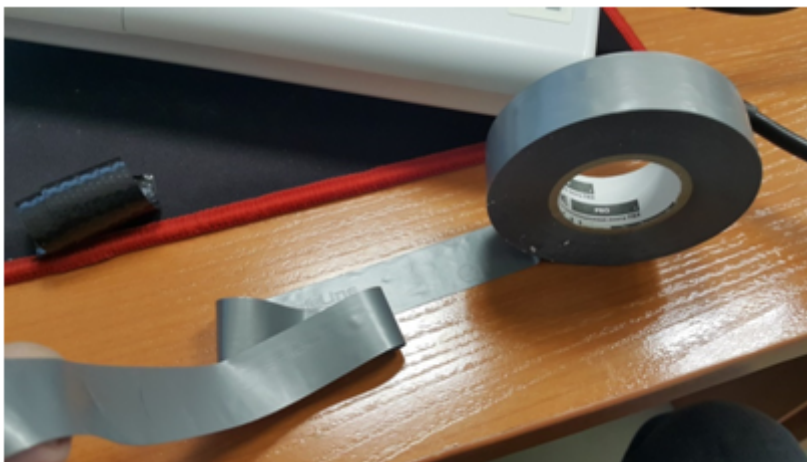
Figure 11

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 12.

Figure 12

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 13 (a, b).

Figure 13a

Figure 13b

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

4 Managing the device through a web interface
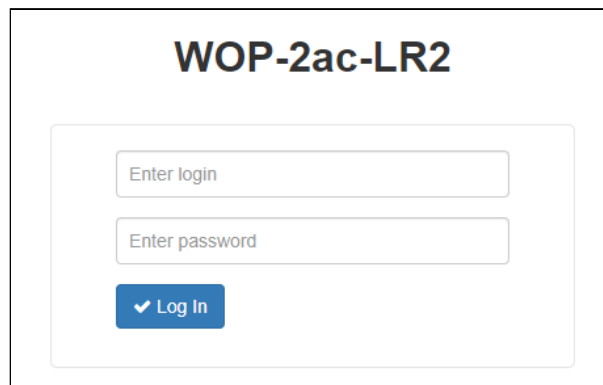
4.1 Getting started

To start, you need to connect the device through a browser:
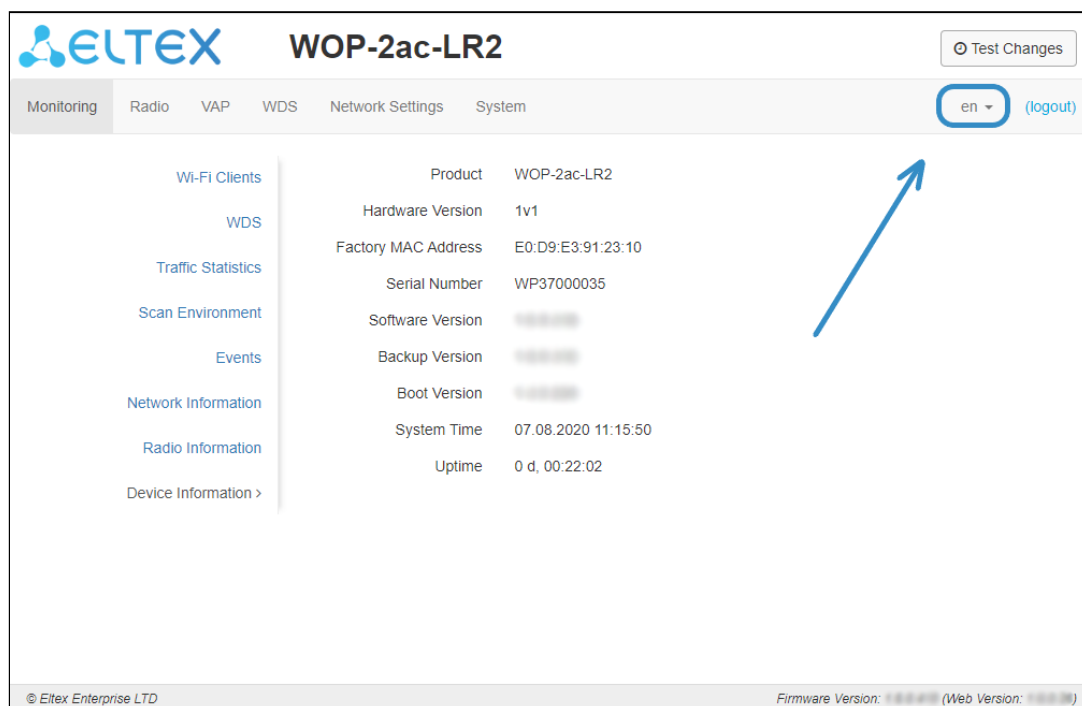
1. Open a web browser (web-page explorer), for example, Firefox, Opera, Chrome.

2. Enter the IP address of the device to the browser address line.

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

If connection is successful, the request form with the user name and password will be displayed on a browser window.

3. Enter Login and Password into corresponding fields.

4. Click the 'Log in' button. Device Web configurator home page will be opened in the browser window.

5. If necessary, you can switch the display language information. Russin and English languages are available for WOP-2ac-LR2.

4.2 Applying configuration and discarding changes

1. Applying configuration

> ✓ **Click the** [✓ Apply] **button to save the configuration into the device flash memory and apply 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 3.

Table 3 – Visual indication of the current status of the setting application process

Image	State description
[⟳ Apply]	After pressing 'Apply', the process of settings saving to device memory is launched. This is indicated by the [⟳] icon on the Apply button.
[✓ Apply]	Successful settings saving and application are indicated by the [✓] icon on the Apply button.

2. Discarding changes

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

The button for discarding changes appears as follows: [✖ Cancel] .
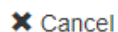
4.3 Test changes mode

The device has a test mode for a test configuration application.

To activate it, press the 'Test changes' button on the top panel of the web interface.

Test mode operating time is 300 seconds (5 minutes). During this time you can navigate through the web configurator tabs and make any changes by applying them on each page using the 'Apply' button.

After checking the required configuration, press the 'Exit from Test Mode' button and select the desired action:

- 'Save and exit' – pressing this button will exit the test mode and save to the non-volatile memory all configuration changes that were made and applied in this mode. It will be impossible to undo changes made in the test mode.
- 'Cancel and exit' – pressing will exit the test mode and cancel all changes made in this mode. The configuration in effect on the device before the test mode is activated will be restored.
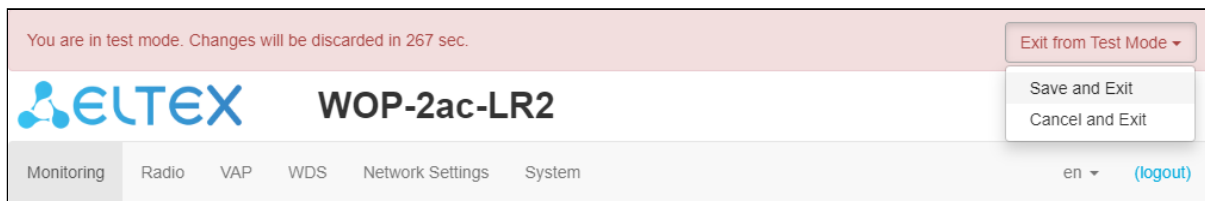
If the administrator does not exit the test mode within 300 seconds, this will happen automatically along with a rollback of all changes that have been made in this mode. After the specified time, the configuration will be restored even if access to the device is lost as a result of the changes made.

4.4 Main elements of the web interface

Navigation elements of the web interface are shown on the figure below.
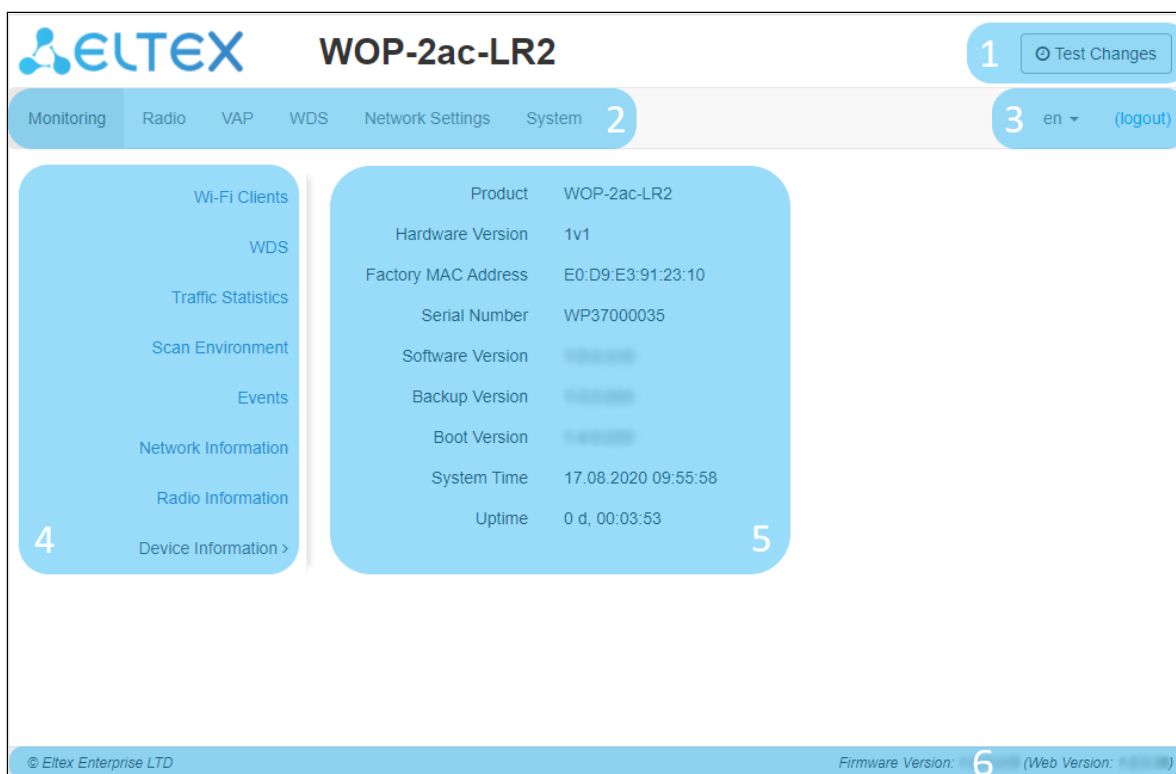
User interface window is divided into five general areas:
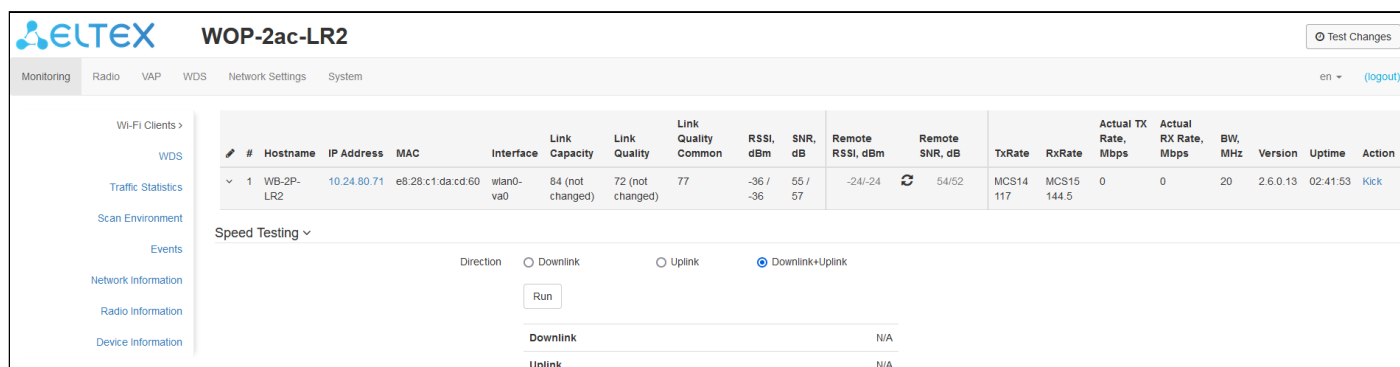
1. 'Test mode' button – start the configuration testing mode.
2. Menu tabs categorize the submenu tabs: **Monitoring**, **Radio**, **VAP, WDS, Network Settings, System**.
3. Interface language selection and Logout button designed to to end a session in the web interface under a given user.
4. Submenu tabs allow you to control settings field.
5. Device configuration field displays data and configuration.
6. Information field displays current firmware version.

4.5 The 'Monitoring' menu

In the 'Monitoring' menu you can view the current system state.

4.5.1 The 'Wi-Fi Clients' submenu

The 'Wi-Fi clients' submenu displays information about the status of connected Wi-Fi clients, traffic statistics and link speed testing.

	#	Hostname	IP Address	MAC	Interface	Link Capacity	Link Quality	Link Quality Common	RSSI, dBm	SNR, dB	Remote RSSI, dBm	Remote SNR, dB		TxRate	RxRate	Actual TX Rate, Mbps	Actual RX Rate, Mbps	BW, MHz	Version	Uptime	Action
✎																					
⌄	1	WB-2P-LR2	10.24.80.71	e8:28:c1:da:cd:60	wlan0-va0	84 (not changed)	72 (not changed)	77	-36 / -36	55 / 57	-24/-24 ⟳	54/52		MCS14 117	MCS15 144.5	0	0	20	2.6.0.13	02:41:53	Kick

Speed Testing ⌄

Direction	○ Downlink	○ Uplink	◉ Downlink+Uplink
	Run		

Downlink	N/A
Uplink	N/A

> ✅ For ease of monitoring, there is an option to select the parameters to display. To do this, click on the ✎ icon. If you click the 'By Defaults' button, the default settings will be set.

- *#* − number of the connected device in the list;
- *Hostname* − network name of the device;
- *IP Address* − IP address of the connected device;
- *MAC* − MAC address of the connected device;
- *Interface* − WOP-2ac-LR2 interface for interaction with the connected device;
- *Link Capacity* − parameter that reflects the efficiency of modulation on the transmission used by an access point. It is calculated based on the number of packets transmitted to the client on each modulation, and the reduction factors. The maximum value is 100% (means that all packets are transmitted to the client at maximum modulation for the maximum nss type supported by the client). The minimum value is 2% (in the case when the packets are transmitted on the modulation nss1mcs0 for a client with MIMO 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 retransmitted 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 all the time the client is connected;
- *RSSI* − received signal level, dBm;
- *SNR* − signal/noise ratio, dB;
- *Remote RSSI* − output of the received signal level from the subscriber station, dBm;
- *Remote SNR* − output of the signal/noise ratio level from the subscriber station, dB;
- *TxRate* − channel data rate of transmission, Mbps;
- *RxRate* − channel data rate of receiving, Mbps;
- *Actual TX Rate* − average data transfer rate for the last 10 seconds, Mbps;
- *Actual RX Rate* − average data reception rate for the last 10 seconds, Mbps;
- *BW* − radio channel bandwidth, MHz;

- *Version* − firmware version of the WB-2P-LR2 subscriber station. Subscriber station should have the firmware version 2.4.1 and higher;
- *Uptime* − Wi-Fi client connection time;
- *Action* − when clicking on the 'Kick' button, the Wi-Fi connection with the subscriber station will be broken. Subscriber station will reconnect.

> ✅ The **Remote RSSI** and **Remote SNR** values are not updated in real time. To request the current values,
>
> click ⟳ , after which the information in the fields will be updated within 10 seconds.

The 'Speed Testing' subsection is designed to test the speed of the link in the direction from the base station to the subscriber station and back:

- *Downlink* − speed test will be performed in the direction from the base station to the subscriber station;
- *Uplink* − speed test will be performed in the direction from the subscriber station to the base station;
- *Downlink+Uplink* − speed test will be performed alternately in each direction.

The test is performed with TCP traffic and lasts 10 seconds for one direction. The test can only be run to one subscriber station at a time. Subscriber station must have firmware version 2.4.4 or higher.

To run the test, select the direction and click the 'Run' button. After completing the test, the result will be displayed in the appropriate field.

By default, VLAN 7 and subnet 192.0.4.0/24 are used for the test. If the network already uses this subnet and VLAN, you should change the settings for the test so that they do not overlap with existing networks. This can be done through the CLI. The process is described in more detail in section 'Speed Testing'.

The 'Advanced Traffic Statistics' subsection contains information about the amount of transmitted and received traffic, errors and retries, the current speed and packet statistics by modulation.

Advanced Traffic Statistics

Total TX / RX, bytes	12 496 505 / 19 083 028	Fails, packets 0
Total TX / RX, packets	12 604 / 16 059	TX Period Retry, packets 0
Data TX / RX, bytes	12 168 393 / 18 664 923	TX Retry Count, packets 7 322
Data TX / RX, packets	12 589 / 16 023	Actual TX / RX Rate, kbps 0 / 0

Rate	TX Packets		RX Packets	
DSSS1	17	0%	51	0%
CCK5	0	0%	2	0%
MCS0	0	0%	32	0%
MCS1	0	0%	56	0%
MCS2	0	0%	1012	6%
MCS3	0	0%	394	2%
MCS4	3984	32%	2197	14%
MCS5	6	0%	1898	12%
MCS6	1	0%	2446	15%
MCS7	0	0%	2520	16%
MCS8	0	0%	261	2%
MCS9	0	0%	1113	7%
MCS10	6386	51%	196	1%
MCS11	1402	11%	3880	24%
MCS12	808	6%	0	0%

- *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 to the connected device;
- *TX Period Retry, packets* − the number of retransmissions to the connected device in the last 10 seconds;
- *TX Retry Count, packets* − the number of retransmissions to the connected device during all the time of connection;
- *Actual TX / RX Rate, kbps* − average data transfer rate for the last 10 seconds.

4.5.2   The 'WDS' submenu

The 'WDS' submenu displays information about the status of WOP-2ac-LR2 connected via WDS.

✏	#	Hostname	IP Address	MAC	Interface	Link Capacity	Link Quality	Link Quality Common	RSSI, dBm	SNR, dB	Remote RSSI, dBm	Remote SNR, dB		TxRate	RxRate	TX BW, MHz	RX BW, MHz	Uptime
⌄	1	WOP-2ac-LR2	10.24.80.92	e8:28:c1:da:cd:60	wlan0	44	80	84	-24 / -24	61 / 70	-36/-42	⟳	47/34	MCS15 144.5	MCS11 52	20	20	00:00:25

Total TX / RX, bytes	14 354 / 2 911	Fails, packets	0
Total TX / RX, packets	97 / 23	TX Period Retry, packets	4
Data TX / RX, bytes	10 927 / 1 176	TX Retry Count, packets	7
Data TX / RX, packets	85 / 11	Actual TX / RX Rate, kbps	3 / 0

Rate	TX Packets		RX Packets	
DSSS1	12	12%	11	50%
OFDM6	7	7%	0	0%
OFDM54	2	2%	0	0%
MCS0	4	4%	0	0%
MCS1	4	4%	0	0%
MCS2	6	6%	0	0%
MCS3	1	1%	0	0%
MCS4	11	11%	9	41%
MCS5	9	9%	0	0%
MCS9	6	6%	0	0%
MCS10	4	4%	0	0%
MCS11	4	4%	2	9%
MCS12	13	13%	0	0%
MCS13	7	7%	0	0%
MCS14	2	2%	0	0%
MCS15	5	5%	0	0%

> ✅ For ease of monitoring, there is an option to select the parameters to display. To do this, click on the ✏ icon. If you click the 'By Defaults' button, the default settings will be set.

- *#* − number of the connected device in the list;
- *IP address* − IP address of the connected device;
- *Hostname* − network name of the device;
- *MAC address* − MAC address of the connected device;
- *Interface* − WOP-2ac-LR2 interface of interaction with a 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;
- *Remote RSSI* − output of the received signal level from the subscriber station, dBm;
- *Remote SNR* − output of the signal/noise ratio level from the subscriber station, dB;
- *TxRate* − channel data rate of transmission, Mbps;
- *RxRate* − channel data rate of receiving, Mbps;
- *TxBW* − transmission bandwidth, MHz;
- *RxBW* − receive bandwidth, MHz;
- *Uptime* − connection uptime.
- *Total TX/RX, bytes* − the number of bytes sent/received on the connected device;
- *Total TX/RX, packets* − the number of packets sent/received on the connected device;
- *Data TX/RX, bytes* − the number of data bytes sent/received on the connected device;
- *Data TX/RX, packets* − the number of data packets sent/received on the connected device;
- *Fails, packets* − the number of packets sent with errors on the connected device;
- *TX Period Retry, packets* − the number of retries of transmission to the connected device in the last 10 s;
- *TX Retry Count, packets* − the number of retries of transmission to the connected device during the entire connection;
- *Actual TX/RX Rate, Kbps* − the current traffic transmission rate at the moment.

> ✅ The **Remote RSSI** and **Remote SNR** values are not updated in real time. To request the current values,
> click ⟳ , after which the information in the fields will be updated within 10 seconds.

4.5.3 The 'Traffic Statistics' submenu

The 'Traffic Statistics' section displays the diagrams of the speed of the traffic transmission/reception for last 3 minutes, as well as information on the amount of transmitted/received traffic since the access point was turned on.
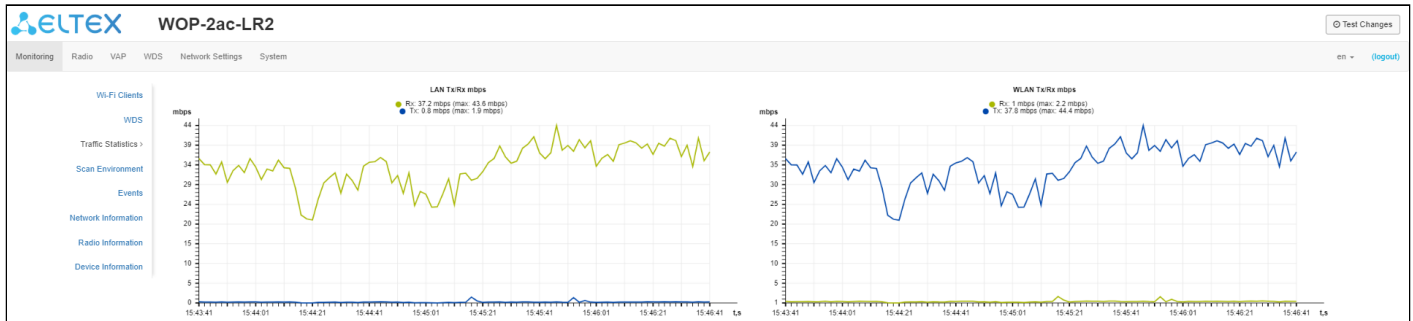
The LAN Tx/Rx diagram shows the speed of the traffic transmission/reception via the access point's Ethernet interface in last 3 minutes. The diagram is automatically updated every 2 seconds.

The WLAN Tx/Rx diagram shows the speed of the traffic transmission/reception via the access point's Radio interfaces in last 3 minutes. The diagram is automatically updated every 2 seconds.

'Transmit' table description:

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

Transmit ⌄				
Interface	Total Packets	Total Bytes	Total Drop	Errors
LAN	691	1084814	0	0
WLAN	0	0	0	0
wlan0-va0	0	0	0	0
wlan0-va1	0	0	0	0
wlan0-va2	0	0	0	0
wlan0-va3	0	0	0	0
wlan0-wds0	0	0	0	0
wlan0-wds1	0	0	0	0
wlan0-wds2	0	0	0	0
wlan0-wds3	0	0	0	0
wlan0-wds4	0	0	0	0
wlan0-wds5	0	0	0	0
wlan0-wds6	0	0	0	0
wlan0-wds7	0	0	0	0
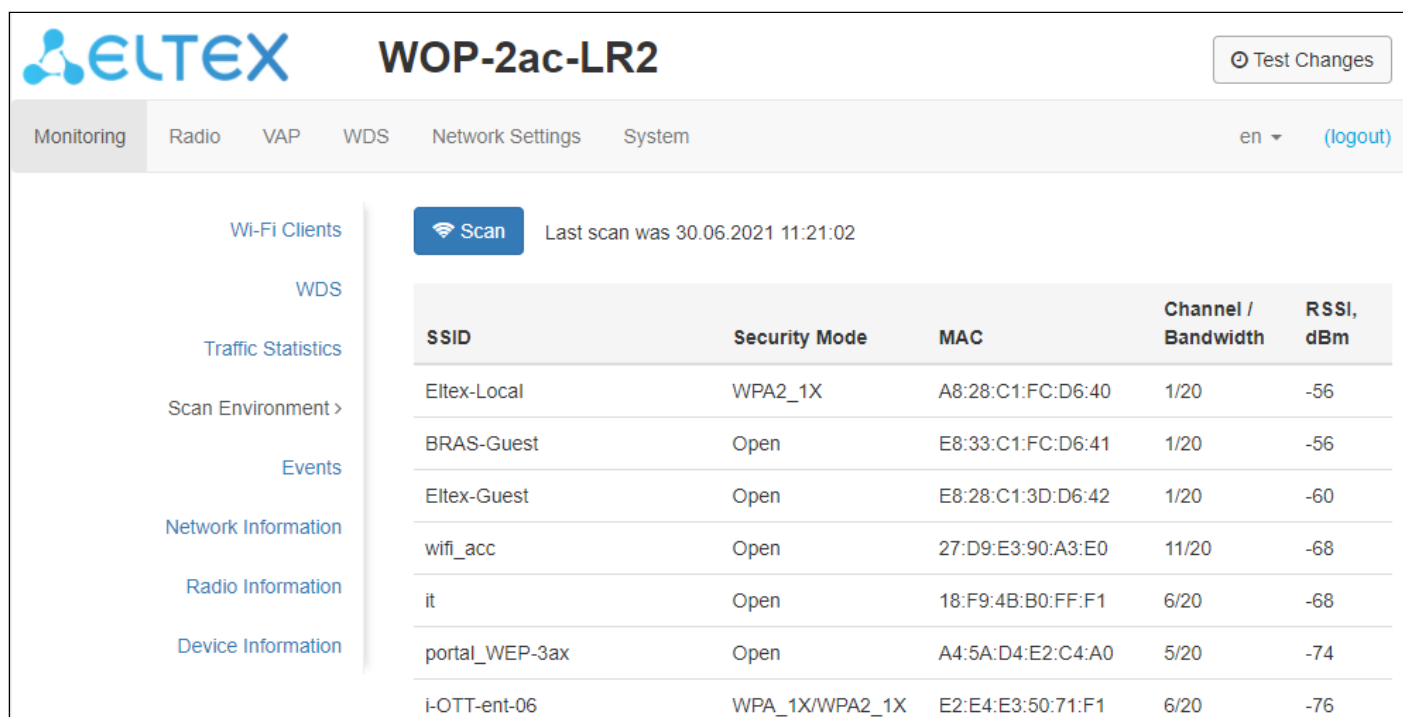
'Receive' table description:

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

Receive ⌄				
Interface	Total Packets	Total Bytes	Total Drop	Errors
LAN	160685	34180986	5538	0
WLAN	6327	3073059	0	0
wlan0-va0	6327	3073059	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
wlan0-wds3	0	0	0	0
wlan0-wds4	0	0	0	0
wlan0-wds5	0	0	0	0
wlan0-wds6	0	0	0	0
wlan0-wds7	0	0	0	0

4.5.4 The 'Scan Environment' submenu

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

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:

- *SSID* – SSID of the detected access point;
- *Security Mode* – security mode of the detected access point;
- *MAC* – MAC address of the detected access point;
- *Channel/Bandwidth* – radio channel on which the detected access point operates;
- *RSSI* – the level with which the device receives the signal of the detected access point, dBm.

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

4.5.5 The 'Events' submenu

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

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

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.

4.5.6   The 'Network Information' submenu

In the 'Network Information' submenu you can view common network settings of the device.

WAN Status:

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

Ethernet:

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

SFP

- *SFP-module Status* – indicates presence/absence of SFP module;
- *Link Status* – optical interface operation status;
- *Tx Fault* – transceiver failure indication;
- *LOS* – signal loss;
- *Speed* – data transfer rate;

- *Temperature* – current temperature of the SFP module;
- *Voltage* – SFP module supply voltage;
- *Current* – SFP module laser bias current;
- *Emission power* – transceiver output power;
- *Receiver power* – receiver input power.

ARP

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

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

Routes:

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

4.5.7 The 'Radio Information' submenu

In the 'Radio Information' submenu the current status of WOP-2ac-LR2 radio interface is displayed.
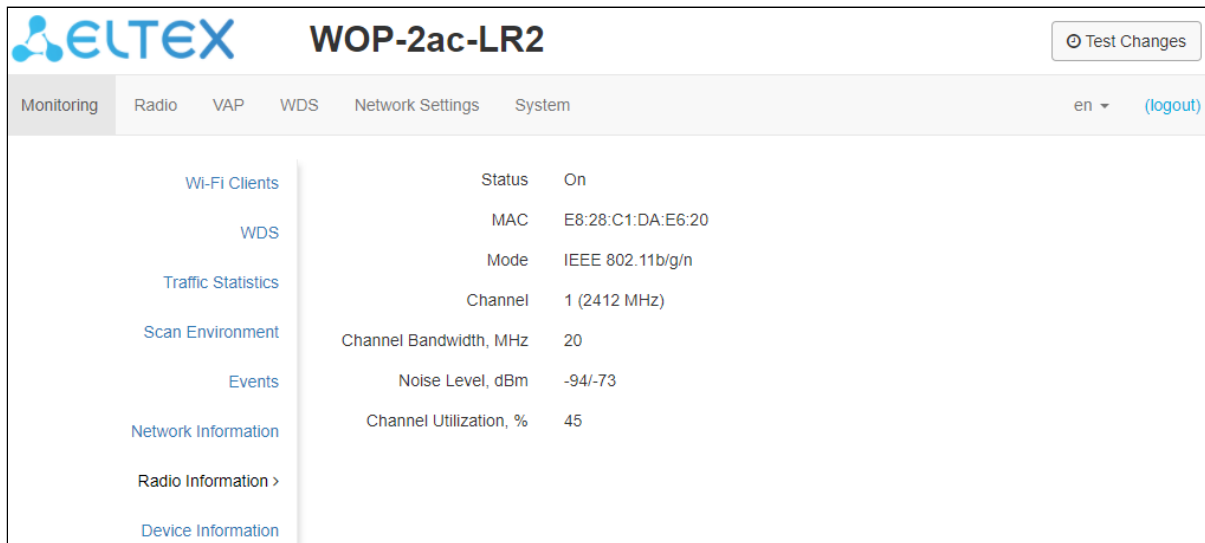
The access point radio interfaces can be in two states: 'On' and 'Off'. The Radio status depends on whether the radio interface has virtual access points (VAPs) or wireless bridges (WDS) enabled. In case there is at least one active VAP or configured WDS on the radio interface, Radio will be in the 'On' 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, MHz;
- *Noise Level* – level of the noise in the radio channel, dBm;
- *Channel Utilization* – channel occupancy information expressed as percentage.
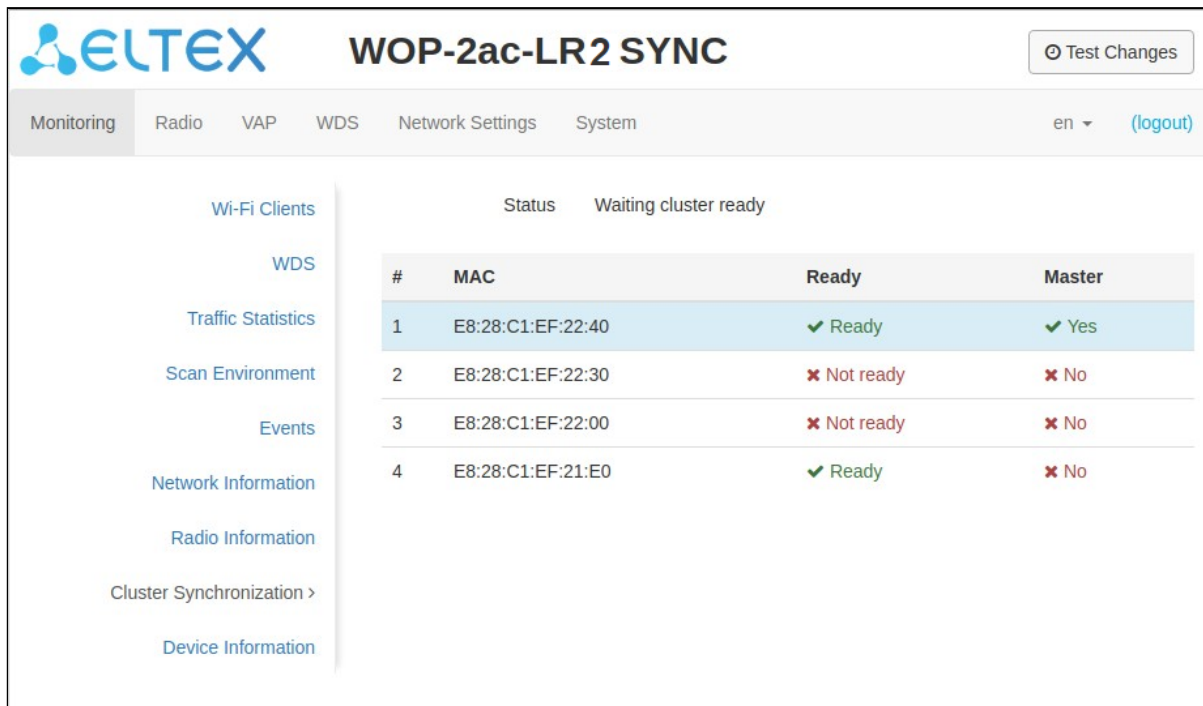
4.5.8   The 'Cluster Synchronization' submenu

This submenu contains information about the status of the inter-sectoral synchronization (ISS) and all cluster members.

> ✅ **The submenu is only available for WOP-2ac-LR2 SYNC devices.**

Possible status values:

- *Running* – transmission synchronization process is started between the BSs;
- *Waiting cluster ready* – the process of waiting for all cluster members to be ready to start synchronization;
- *Disabled* – ISS is disabled in the base station settings.
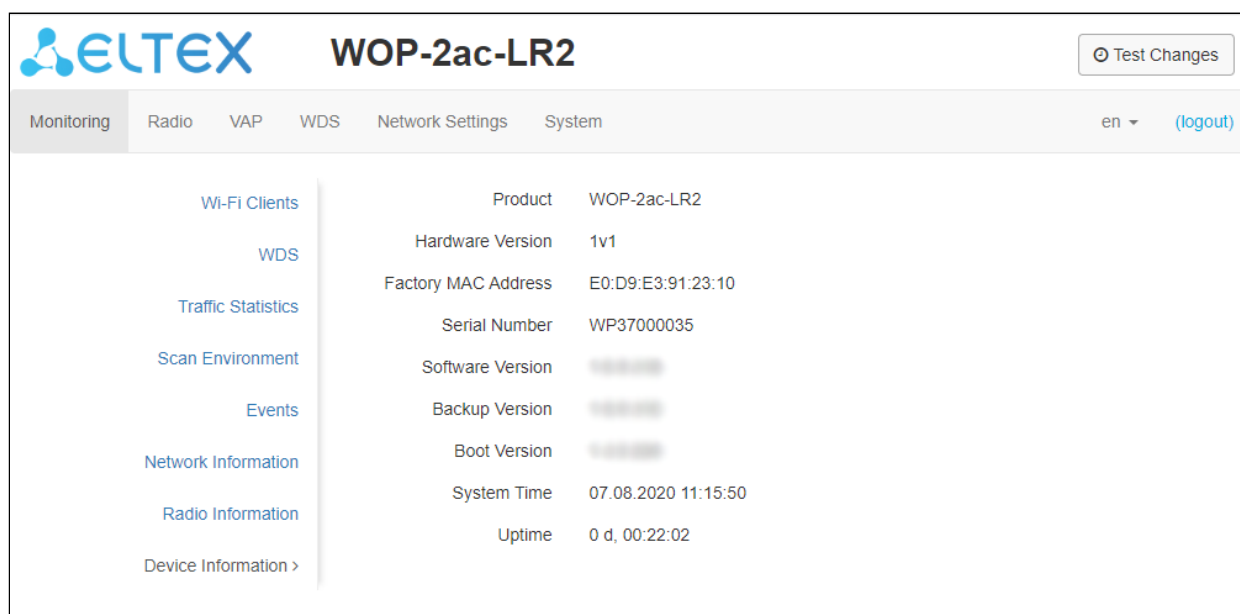
Information on cluster members:

- *#* – number in the list;
- *MAC* – MAC addresses of base stations included in a given ISS cluster;
- *Ready* – readiness state of the cluster member. Possible states:
    - *Ready* – this BS has communication with all other cluster members and is ready to start the synchronization process;
    - *Not ready* – this BS has no connection with at least one other cluster member, which is specified in its configuration on the Radio/Synchronization page.
- *Master* – flag defining the master in the ISS cluster.

The line with the information about the specified BS is highlighted in blue.

4.5.9   The 'Device Information' submenu

The 'Device Information' submenu displays main WOP-2ac-LR2 parameters.

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

4.6 The 'Radio' menu

In the 'Radio' menu you can configure the wireless interface

4.6.1 The 'Radio' submenu

In the 'Radio' submenu, you can configure the device's radio interface.

- *Mode* – select interface operation mode:
    - IEEE 802.11b/g
    - IEEE 802.11b/g/n
    - IEEE 802.11n
- *Channel* – select channel for data transmission;
- *Channel Bandwidth, MHz* – channel bandwidth, on which the base station operates. The parameter may take values of 5, 10, 20 and 40 MHz. If the base station has 5 or 10 MHz bandwidth, you should select the same bandwidth on the user station;
- *Fixed center frequency* – when the flag is checked, all traffic (data and management packets) will be transmitted on the specified center channel frequency with a given bandwidth (40 MHz). The function is proprietary, the transmission is not carried out according to IEEE 802.11 standards, where it is supposed to use different center frequencies for data traffic and management with 40 MHz bandwidth;
- *Tx Power (dBm)* – transmitting Wi-Fi signal power adjustment, dBm;
- *Fixed Transmit Rate* – fixed wireless data transmission rate which is defined by IEEE 802.11b/g/n standards;
- *ACK Timeout, µs* – time for delivery confirmation from the subscriber.
- *Polling* – when checked the option is enabled, otherwise – disabled. Polling is one of the variants of TDM access to the medium (time division). Characterized by a constant customer survey by the BS:
    - *MAX TX Duration, ms* – a time indicating how long the subscriber station can transmit traffic;
    - *Management packet modulation* – fixed rate for management packets.

In the 'Advanced' submenu, you can configure advanced device's radio interface parameters.

- *OBSS Coexistence* – automatic channel bandwidth reduction when the air is loaded. When the flag is set, the mode is enabled;
- *Short Guard Interval* – support for Short Guard interval. Access point transmits data using 400 ns Guard interval (instead of 800 ns) to clients which also support Short GI;
- *STBC* – Soace-Time Block Coding method dedicated to improve data transmission reliability. The field is available only if the selected mode of operation of the radio interface includes 802.11n. When checked, the device transmits one data flow through several antennas. When unchecked, the device does not transmit one data flow through several antennas.
- *Beacon Interval, ms* – beacon frames transmission period. The frames are sent to detect access points. The parameter takes values from 20 to 2000 ms, by default – 100 ms;
- *Fragmentation Threshold* – frame fragmentation threshold, bytes. The parameter takes values 256-2346, by default – 2346;
- *RTS Threshold* – after what quantity of bytes the Request to Send will be sent. Decreasing of the parameter's value might improve access point operation when there are a lot of clients connected. However, decreasing of the parameter's value will reduce general bandwidth of wireless network. The parameter takes values from 0 to 2347, by default – 2347;
- *Frame Aggregation* – enable support for AMPDU/AMSDU;
- *Short Preamble* – use of the packet short preamble;
- *Broadcast/Multicast Rate Limiting, p/s* – when the flag is set, transmission of broadcast / multicast traffic over the wireless network is restricted. Specify the limit for broadcast traffic in the popup window (p/s).

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

4.6.2 The 'QoS' submenu

In the 'QoS' submenu, you may configure Quality of Service functions.

- *WMM* – WMM support activation (Wi-Fi Multimedia);
- *Enable QoS* – when the flag is set, EDCA parameters configuration is available;
- *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 (1p: cs1, cs2 priorities);
    - *Data 2 (Best Effort)* – middle priority queue, middle bandwidth and delay. Most of the traditional IP data is sent to this queue (802.1p: cs0, cs3 priorities);
    - *Data 1 (Video)* – high priority queue, minimal delay. In this queue, time-sensitive video data is automatically processed (802.1p: cs4, cs5 priorities);
    - *Data 0 (Voice)* – high priority queue, minimal delay. In this queue, time sensitive data is automatically processed, such as: VoIP, streaming video (802.1p: cs6, cs7 priorities).
  - *AIFS* – Arbitration Inter-Frame Spacing, defines the waiting time of data frames, measured in slots, takes values (1-255);
  - *cwMin* – the initial timeout value before resending a frame, specified in milliseconds, takes the values 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023. The value of cwMin cannot exceed the value of cwMax;

- *cwMax* – the maximum timeout value before resending a frame, specified in milliseconds, takes the values 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023. The value of cwMax must exceed the value of cwMin;
- *TXOP Limit* – this parameter is used only for data transmitted from the client station to the access point. The transmission capability is the time interval, in milliseconds, when the client WME station has the rights to initiate data transmission over the wireless medium to the access point, the maximum value is 65535 milliseconds;
- *Station EDCA parameters* – table of client station parameter settings (traffic is transmitted from the client station to the access point). For description of table fields, see above.

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

4.6.3 The 'Synchronization' submenu

> ✓ **This menu is available for WOP-2ac-LR2 SYNC only.**

Contains settings of inter-sectoral synchronization (ISS) for base stations.

- *Enable* – when checked, ISS mechanism is enabled, otherwise – disabled;
- *Cluster ID* – base station cluster ID. By default – 0. Used to organize several clusters within one L2 segment to identify control packets of BS ISS included in one cluster;
- *MAC address 1..3* – MAC addresses of other base stations included in the given ISS cluster.

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

4.7 The 'VAP' menu

In the 'VAP' menu, you configure virtual Wi-Fi access points (VAP).

4.7.1 The 'Summary' submenu

The 'Summary' submenu displays the settings of all VAPs. You can see the settings of each virtual access point in sections VAP0..3.

- *VAP0..3* – the sequence number of the virtual access point;
- *Enabled* – when checked, the virtual access point is enabled, otherwise it is disabled;
- *Security mode* – the type of data encryption used on the virtual access point;
- *VLAN ID* – VLAN number from which the tag will be removed when transmitting Wi-Fi traffic to clients connected to this VAP. When traffic flows in the opposite direction, untagged traffic from clients will be tagged with VLAN ID (when VLAN Trunk mode is disabled);
- *SSID* – virtual wireless network name;
- *Broadcast SSID* – when checked, SSID broadcasting is on, otherwise it is disabled;
- *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.

4.7.2 The 'VAP' submenu

Common Settings

- *Enabled* – when checked, the virtual access point is enabled, otherwise it is disabled;
- *VLAN ID* – VLAN number from which the tag will be removed when transmitting Wi-Fi traffic to clients connected to this VAP. When traffic flows in the opposite direction, untagged traffic from clients will be tagged with VLAN ID (when VLAN Trunk mode is disabled);
- *SSID* – virtual wireless network name;
- *Broadcast SSID* – when checked, SSID broadcasting is on, otherwise it is disabled;
- *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;
- *Priority* – prioritization method. Specifies the field on the basis of which traffic transmitted to the radio interface will be allocated to the WMM queues:
    - *DSCP* – will analyze the priority from the DSCP field of the IP packet header; if the DSCP value in tagged packets is 0, then the priority from the CoS field (802.1p) will be analyzed;
    - *802.1p* – will analyze the priority from the CoS (Class of Service) field of the tagged packets; if the priority is overridden by VLAN mapping rules, the priority set for transmissions to the radio channel will be analyzed.
- *Maximum Stations* – the maximum number of clients connected to the virtual network;
- *Security Mode* – wireless access security mode:
    - *Off* – do not use encryption for data transfer. The access point is available for any subscriber to connect;
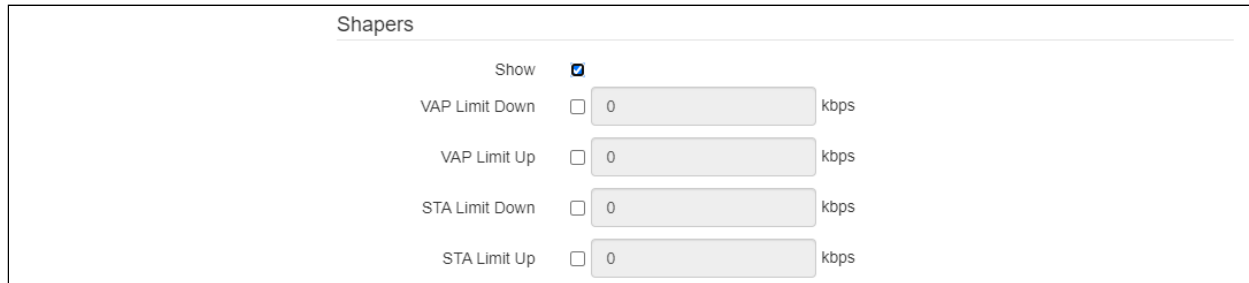
- *WPA, WPA2, WPA/WPA2* – encryption methods, if you select one of the methods, the following setting will be available:
  - *WPA Key* – key/password required to connect to the virtual access point. The length of the key makes from 8 to 63 characters;
- *WPA-Enterprise, WPA2-Enterprise, WPA/WPA2-Enterprise* – wireless channel encryption mode, in which the client is authorized on the centralized RADIUS server. To configure this security mode, you must specify the parameters of the RADIUS server. You also need to specify a key for the RADIUS server. If you select one of the methods, the RADIUS server parameters configuration 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;
  - *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.
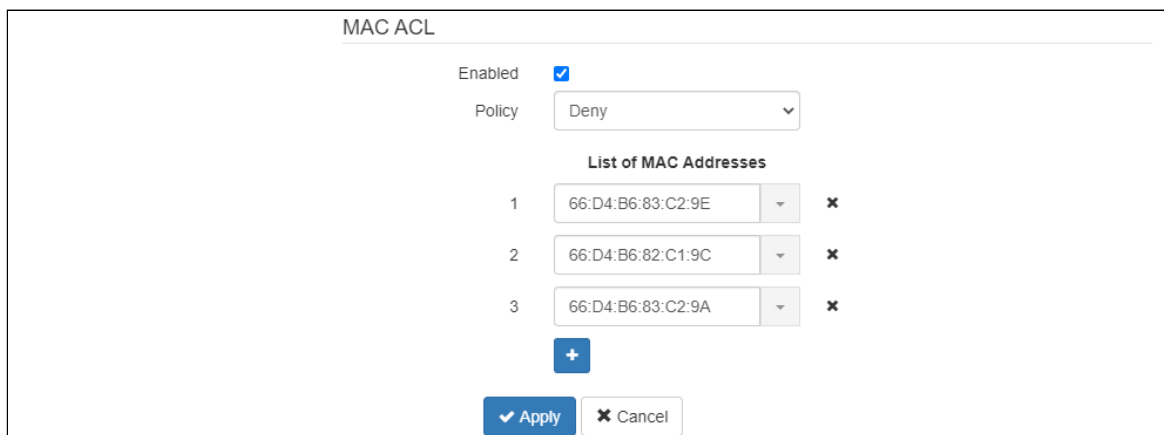
Shapers

- *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.

MAC ACL

This subsection configures lists of MAC addresses of clients that, depending on the access policy selected, are allowed or denied to connect to this VAP.

- *Enabled* – when checked, the selected access policy will work;
- *Policy* – access policy. Possible values:
    - *Deny* – clients whose MAC addresses are listed will not be allowed to connect to this VAP. Everyone else will be allowed access to this VAP;
    - *Allow* – clients whose MAC addresses are listed will be allowed to connect to this VAP. Everyone else will be denied access.
- *List of MAC Addresses* – list of MAC addresses of clients that are allowed or denied access to this VAP. May contain up to 128 addresses.

To add the address to the list click the [+] button and in the displayed field, enter the MAC address. To delete the address from the list, click the [✖] button in the corresponding line.

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

By default, up to 10 addresses are displayed in the list. To see the full list if it contains more than 10 addresses, click 'Show all'.

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

4.8 The 'WDS' menu

In the 'WDS' menu, you configure wireless bridges between WOP-2ac-LR2.

> ✔ **When configuring a WDS connection, it is necessary that on the devices that will be connected via WDS, the same channel and channel width are selected in the radio interface settings.**

4.8.1 The 'WDS' submenu

- *Enabled* – when the flag is set, the wireless bridge mode is enabled; otherwise, it is disabled;
- *Security* – wireless network access security mode:
    - *Off* – do not use encryption for data transfer.
    - *WPA2* – encryption method for which the following setting is available:

- *WPA Key* – key/password required to connect to the opposite access point. The key length is from 8 to 63 characters.
- *Link X (where X=0..7)* − enable wireless bridge link;
- *MAC* − MAC address of the opposite device to which the wireless bridge is configured;
- *Fixed Transmit Rate*− fixed wireless data transmission rate which is defined by IEEE 802.11b/g/n standards. For each link is selected individually.

To apply the new configuration and save the settings to the non-volatile memory, click 'Apply'. To cancel the changes click the 'Cancel' button.

4.9 The 'Network Settings' menu

4.9.1 The 'System Configuration' submenu

- *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);
- *Management VLAN*:
    - *Disabled*− Management VLAN is not used;
    - *Terminating*− the mode in which the management VLAN is terminated at the access point; in this case, clients connected via the radio interface do not have access to this VLAN;
    - *Forwarding*− the mode in which the management VLAN is also transmitted to the radio interface (with the appropriate VAP configuration).
- *VLAN ID* − the VLAN ID used to access the device, takes values 1-4094;
- *Protocol* − select protocol for connection of the device via Ethernet interface to service provider network:

- *DHCP*– operation mode, when IP address, subnet mask, DNS server address, defualt gateway and other parameters required for operation are obtained from DHCP server automatically;
- *Static* – operation mode where IP address and all the necessary parameters for WAN interface are assigned statically. If 'Static' is selected, the following parameters will be available to set:
    - *Static IP* – device WAN interface IP address in the provider network;
    - *Netmask* – external subnet mask;
    - *Gateway* – address, to which the packet is sent, if the route in routing table is not found for it;
- *Primary DNS Server, Secondary DNS Server* – IP address of DNS servers. If DNS servers' addresses are not allocated automatically via DHCP, set them manually.
- *Local Management via Ethernet[1]* – enables the device accessibility without tag via Ethernet.
    - *Enabled* – activates the device accessibility without tag via Ethernet;
    - *Static IP* – IP address of the Ethernet interface in local network (by deafult 192.0.3.1);
    - *Netmask* – subnet mask.

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

---

[1] The setting is available only in Terminating and Forwarding modes.

4.9.2 The 'Access' submenu

In the 'Access' submenu, you can configure access to the device via the web interface, Telnet, SSH, NETCONF and SNMP.

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

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

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

WOP-2ac-LR2 software allows monitoring of the device status and its sensors via SNMP. The device supports SNMPv1, SNMPv2.

SNMP	☑
roCommunity	public
rwCommunity	private
TrapSink	
Trap2Sink	
InformSink	
Sys Name	WOP-2ac-LR2
Sys Contact	Contact
Sys Location	Russia
Trap Community	trap

To change the SNMP agent parameters, check the box next to 'SNMP'. After this the following parameters will become available.

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

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

- eltexLtd.1.127.1 – monitoring of BS parameters and connected APs;
- eltexLtd.1.127.3 – BS management (reboot);

where eltexLtd – 1.3.6.1.4.1.35265 is Eltex Enterprise identifier.

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

4.10   The 'System' menu

In the system submenu, you may configure system parameters: time, syslog as well as password change, configuration upload/download, firmware update and device reboot can be performed.

4.10.1   The 'Device Firmware Upgrade' submenu

The 'Device Firmware Upgrade' submenu is intended to upgrade the device firmware.

- *Active Version* – installed firmware version, which is operating at the moment;
- *Backup Version* – installed firmware version which can be used in case of problems with the current active firmware version;
    - *Set Active* – a button that allows 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 'Choose file' button in the *Firmware Image* field and specify the path to the firmware file in .tar.gz format.
To start the upgrade process, click the 'Start Upgrading' button. The process may take several minutes (its current status will be shown on the page). The device will be automatically rebooted when the upgrade is completed.

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

4.10.2 The 'Configuration' submenu

In the 'Configuration' submenu current configuration can be saved and restored.
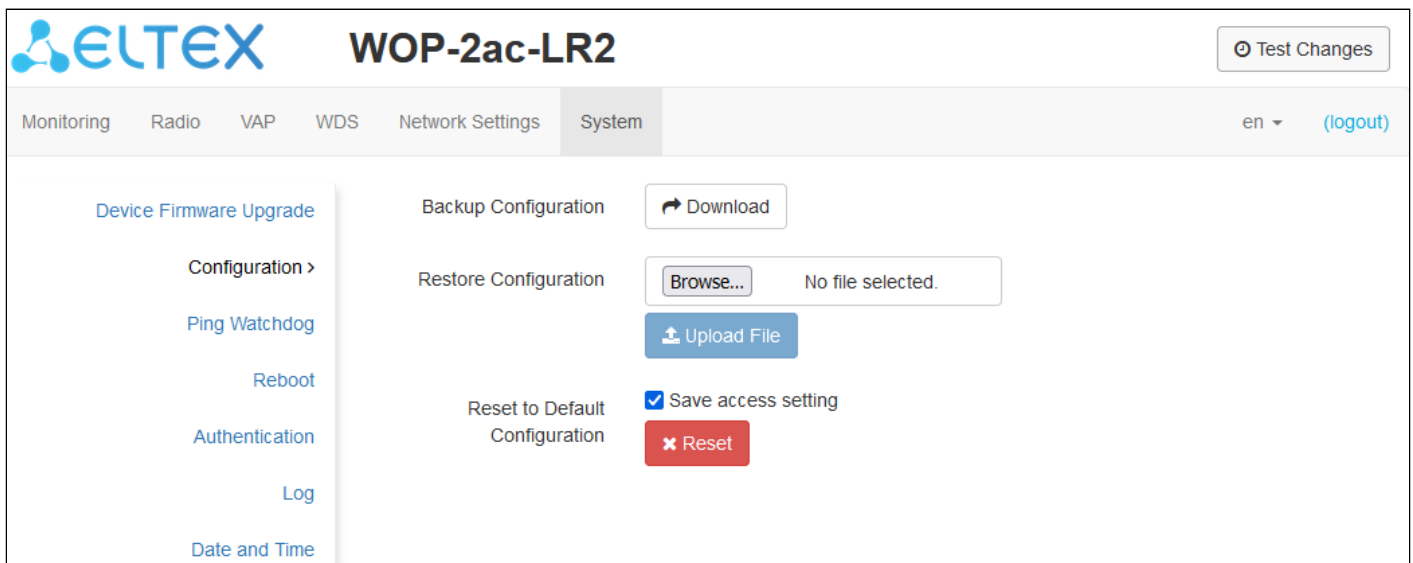
Backup Configuration

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

Restore Configuration

To upload the configuration file saved on the local computer, use the *Restore Configuration* item. To upload the device configuration, click the 'Choose file' 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.

> ✅ **Note that all the passwords of configuration are encrypted with a key depending on device MAC address. Before loading a configuration from one device to another, you should change all passwords.**

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:

```
"authentication":{
  "admin-password":"encrypted:7068747570617169"
},
changes to
"authentication":{
  "admin-password":"password"
},
```

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.

4.10.3 The 'Ping Watchdog' submenu

The 'Ping Watchdog' feature allows to detect disconnection issues and to reboot the device or its interfaces without user intervention. Rebooting the interface also reboots the DHCP client on the current WAN interface.

- *Enabled* – when the flag is checked, Ping Watchdog is enabled, disabled otherwise;
- *Action*:
    - *Restart Ethernet Interface* – in case of specified Ping Server unavailability, the Ethernet interface restart will occur;
    - *Restart Wireless Interface* – in case of specified Ping Server unavailability, the Wireless interface restart will occur;
    - *Reboot device* – in case of specified Ping Server unavailability, the device reboot will occur.
- *Ping Server* – IP address or domain hostname where ICMP requests are sent;
- *Startup Delay* – time in seconds after starting the device or after previous triggering during which the Ping Watchdog does not operate. Possible values from 60 to 86400 inclusive.
- *ICMP Echo-Request Period* – time in seconds after which ICMP echo request will be sent after receiving ICMP echo reply or after making decision that previous ICMP echo request has failed. Possible values from 1 to 86400 inclusive.
- *ICMP Echo-Reply Timeout* – time in seconds during which ICMP echo reply to ICMP echo request is expected. If ICMP echo reply was not received when the time is out, then ICMP echo request is considered as a failure. Possible values from 1 to 10 inclusive.
- *Maximum Failed Checks* – maximum number of failed ICMP echo requests. If number of failed ICMP echo requests reaches specified number, a specified action is performed. Possible values from 1 to 86400 inclusive.

4.10.4 The 'Reboot' submenu

To reboot the device, click on the 'Reboot' button. The device reboot process takes about 1 minute.
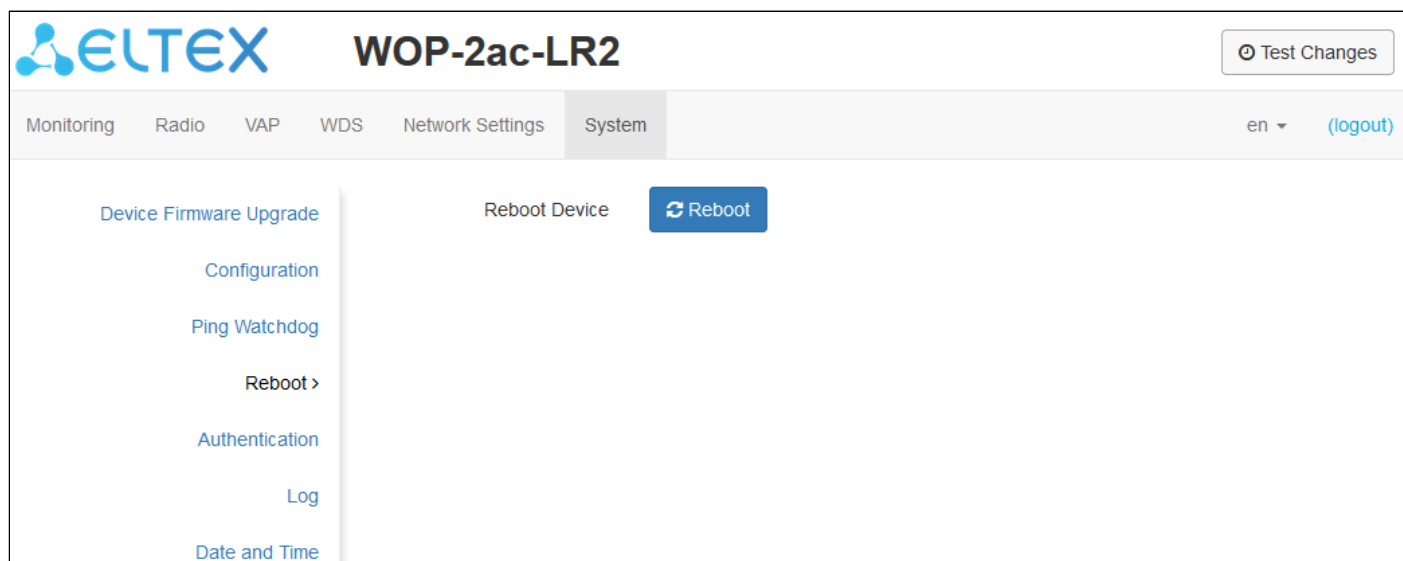
4.10.5 The 'Authentication' submenu

The 'Authentication' submenu is used to configure user authentication.

> ✅ **Factory account to access the device: login: admin, password: password.**

It is also possible to create additional accounts with the roles of administrator or viewer (configuration is only available through the CLI). Accounts with the role of administrator have full access to the device: reading and writing any settings, full monitoring of the device status. Accounts with the viewer role have only monitoring access.

The 'Local Password' section is used to change the factory default password for the admin account. This password is stored on the access point. To change the password, enter the new password first in the 'Password' field, then in the 'Confirm Password' field and click 'Apply' in this section to save the new password.

The 'RADIUS Authentication' section configures access to the RADIUS server that will be used to authenticate and authorize the AP user.

- *RADIUS Authentication* – when this flag is checked, authentication will be performed by the account on the RADIUS server;
- *Address of RADIUS Server* – RADIUS server IP address;
- *Port of RADIUS Server* – RADIUS server port, which is used for authentication and authorization;
- *Password of RADIUS Server* – RADIUS server key, which is used for authentication and authorization.

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

When authenticating via RADIUS server, you should create a local account, which is the same as the account on the RADIUS server. The configuration is performed through the CLI. For details see section 'Additional users creation'.

> ✅ **If RADIUS authentication is enabled, but the server is unavailable, authentication will be performed using the local account.**

4.10.6 The 'Log' submenu

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

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

4.10.7 The 'Date and Time' submenu

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

Manual

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

NTP Server

- *Date and Time device* – date and time set on the device;
- *NTP Server* – time synchronization server IP address/domain name. You can specify an address or select from the list;
- *Time Zone* – allows to set the time zone according to the nearest city for your region from the list.

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

5 Managing the device using the command line

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

5.1 Connection to the device

By default, WOP-2ac-LR2 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-2ac-LR2 factory default IP address: **192.168.1.10**, subnet mask: **255.255.255.0**.

Connection to the device is performed via SSH/Telnet:

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

5.2 Network parameters configuration

Configuration of access point static network parameters

WOP-2ac-LR2(root):/# **configure**
WOP-2ac-LR2(config):/# **interface**
WOP-2ac-LR2(config):/interface# **br0**
WOP-2ac-LR2(config):/interface/br0# **common**
WOP-2ac-LR2(config):/interface/br0/common# **static-ip X.X.X.X** (where X.X.X.X - WOP-2ac-LR2 IP address)
WOP-2ac-LR2(config):/interface/br0/common# **netmask X.X.X.X** (where X.X.X.X - Subnet mask)
WOP-2ac-LR2(config):/interface/br0/common# **dns-server-1 X.X.X.X** (where X.X.X.X - IP address of the dns server №1)
WOP-2ac-LR2(config):/interface/br0/common# **dns-server-2 X.X.X.X** (where X.X.X.X - IP address of the dns server №2)
WOP-2ac-LR2(config):/interface/br0/common# **protocol static-ip** (Change operation mode from DHCP to Static-IP)
WOP-2ac-LR2(config):/interface/br0/common# **save** (Save configuration)

<u>Adding static route:</u>

WOP-2ac-LR2(config):/interface/br0/common# **exit**
WOP-2ac-LR2(config):/interface/br0# **exit**
WOP-2ac-LR2(config):/interface# **exit**
WOP-2ac-LR2(config):/# **route**
WOP-2ac-LR2(config):/route# **default**
WOP-2ac-LR2(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-2ac-LR2(config):/route/default# **netmask X.X.X.X** (where X.X.X.X - destination network mask, for default route - 0.0.0.0)
WOP-2ac-LR2(config):/route/default# **gateway X.X.X.X** (where X.X.X.X - gateway IP address)
WOP-2ac-LR2(config):/interface/br0/common# **save** (Save configuration)

Configuration of reception of the network parameters via DHCP

WOP-2ac-LR2(root):/# **configure**
WOP-2ac-LR2(config):/# **interface**
WOP-2ac-LR2(config):/interface# **br0**
WOP-2ac-LR2(config):/interface/br0# **common**
WOP-2ac-LR2(config):/interface/br0/common# **protocol dhcp** (Changing the operating mode from Static-IP to DHCP)
WOP-2ac-LR2(config):/interface/br0/common# **save** (Save configuration)

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

Non-tagged access

Obtain network parameters via DHCP:

WOP-2ac-LR2(root):/# **set-management-vlan-mode off protocol dhcp**

Static parameters:

WOP-2ac-LR2(root):/# **set-management-vlan-mode off protocol static-ip ip-addr X.X.X.X netmask Y.Y.Y.Y gateway Z.Z.Z.Z** (where X.X.X.X - static IP address, Y.Y.Y.Y - subnet mask, Z.Z.Z.Z - gateway)

Access via management VLAN in Terminating mode

Obtain network parameters via DHCP:

WOP-2ac-LR2(root):/# **set-management-vlan-mode terminating vlan-id X protocol dhcp** (where X - VLAN ID used for device access. Possible values: 1-4094)

Static parameters:

WOP-2ac-LR2(root):/# **set-management-vlan-mode terminating vlan-id X protocol static-ip ip-addr X.X.X.X netmask Y.Y.Y.Y gateway Z.Z.Z.Z** (where X - VLAN ID used for device access. Possible values: 1-4094, X.X.X.X - static IP address; Y.Y.Y.Y - subnet mask; Z.Z.Z.Z - gateway)

Access via management VLAN in Forwarding mode

Obtain network parameters via DHCP:

WOP-2ac-LR2(root):/# **set-management-vlan-mode forwarding vlan-id X protocol dhcp** (where X - VLAN ID used for device access. Possible values: 1-4094)

Static parameters:

WOP-2ac-LR2(root):/# **set-management-vlan-mode forwarding vlan-id X protocol static-ip ip-addr X.X.X.X netmask Y.Y.Y.Y gateway Z.Z.Z.Z** (where X - VLAN ID used for device access. Possible values: 1-4094, X.X.X.X - static IP address; Y.Y.Y.Y - subnet mask; Z.Z.Z.Z - gateway)

Finishing and saving configuration

WOP-2ac-LR2(root):/# **save** (Save configuration)

5.3 Virtual Wi-Fi access points (VAP) configuration

The table shows the commands for configuring VAP security modes.

Table 4 – 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.

5.3.1 Configuration of VAP without encryption

Creation of VAP without encryption

```
WOP-2ac-LR2(root):/# configure
WOP-2ac-LR2(config):/# interface
WOP-2ac-LR2(config):/interface# wlan0-va0
WOP-2ac-LR2(config):/interface/wlan0-va0# vap
WOP-2ac-LR2(config):/interface/wlan0-va0/vap# ssid 'SSID_WOP-2ac-LR2_open' (Change SSID name)
WOP-2ac-LR2(config):/interface/wlan0-va0/vap# security-mode off (Encryption mode off - Without password)
WOP-2ac-LR2(config):/interface/wlan0-va0/vap# exit
WOP-2ac-LR2(config):/interface/wlan0-va0# common
WOP-2ac-LR2(config):/interface/wlan0-va0/common# enabled true (Enable VAP)
WOP-2ac-LR2(config):/interface/wlan0-va0/common# save
```

5.3.2   Configuration of VAP with WPA-Personal security mode

Creation of VAP with WPA-Personal security mode

WOP-2ac-LR2(root):/# **configure**
WOP-2ac-LR2(config):/# **interface**
WOP-2ac-LR2(config):/interface# **wlan0-va0**
WOP-2ac-LR2(config):/interface/wlan0-va0# **vap**
WOP-2ac-LR2(config):/interface/wlan0-va0/vap# **ssid 'SSID_WOP-2ac-LR2_Wpa2'** (Change SSID name)
WOP-2ac-LR2(config):/interface/wlan0-va0/vap# **security-mode WPA_WPA2** (Encryption mode - WPA/ WPA2)
WOP-2ac-LR2(config):/interface/wlan0-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-2ac-LR2(config):/interface/wlan0-va0/vap# **exit**
WOP-2ac-LR2(config):/interface/wlan0-va0# **common**
WOP-2ac-LR2(config):/interface/wlan0-va0/common# **enabled true** (Enable VAP)
WOP-2ac-LR2(config):/interface/wlan0-va0/common# **save**

5.3.3   Configuration of VAP with Enterprise authorization

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

WOP-2ac-LR2(root):/# **configure**
WOP-2ac-LR2(config):/# **interface**
WOP-2ac-LR2(config):/interface# **wlan0-va0**
WOP-2ac-LR2(config):/interface/wlan0-va0# **vap**
WOP-2ac-LR2(config):/interface/wlan0-va0/vap# **ssid 'SSID_WOP-2ac-LR2_enterprise'** (Change SSID name)
WOP-2ac-LR2(config):/interface/wlan0-va0/vap# **security-mode WPA_WPA2_1X** (Encryption mode - WPA/WPA2-Enterprise)
WOP-2ac-LR2(config):/interface/wlan0-va0/vap# **radius**
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/radius# **domain root** (where root - User domain)
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/radius# **auth-address X.X.X.X** (where X.X.X.X - RADIUS server IP address)
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/radius# **auth-port X** (where X - RADIUS server port, used for authentication and authorization. By default: 1812)
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/radius# **auth-password secret** (where secret - Password for RADIUS server, used for authentication and authorization)
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/radius# **acct-enable true** (Enable the sending of 'Accounting' messages to the RADIUS server. By default: false)
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/radius# **acct-address X.X.X.X** (where X.X.X.X - RADIUS server IP address, used for accounting)
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/radius# **acct-port X** (where X - RADIUS server port, that used for accounting. By default: 1813)
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/radius# **acct-password secret** (where secret - password for RADIUS server used for accounting)
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/radius# **acct-periodic true** (Enable the sending of 'Accounting' messages to the RADIUS server. By default: false)
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/radius# **acct-interval 600** (Interval of sending of 'Accounting' messages to the RADIUS server)
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/radius# **exit**
WOP-2ac-LR2(config):/interface/wlan0-va0/vap# **exit**
WOP-2ac-LR2(config):/interface/wlan0-va0# **common**
WOP-2ac-LR2(config):/interface/wlan0-va0/common# **enabled true** (Enable VAP)
WOP-2ac-LR2(config):/interface/wlan0-va0/common# **save**

5.3.4   Advanced VAP settings

Assigning VLAN-ID on VAP

WOP-2ac-LR2(config):/interface/wlan0-va0/vap# **vlan-id X** (where X - number of VLAN-ID on VAP)

Enabling VLAN trunk on VAP

WOP-2ac-LR2(config):/interface/wlan0-va0/vap# **vlan-trunk true** (Enabling VLAN trunk on VAP. To disable, enter **false**)

Enabling General VLAN on VAP

WOP-2ac-LR2(config):/interface/wlan0-va0/vap# **general-vlan-mode true** (Enabling General VLAN on SSID. To disable, enter **false**)
WOP-2ac-LR2(config):/interface/wlan0-va0/vap# **general-vlan-id X** (where X – General VLAN number)

Enabling hidden SSID

WOP-2ac-LR2(config):/interface/wlan0-va0/vap# **hidden true** (Enabling hidden SSID. To disable, enter **false**)

Client limitation on VAP

WOP-2ac-LR2(config):/interface/wlan0-va0/vap# **sta-limit X** (where X - the maximum allowable number of clients connected to the virtual network)

Enabling client isolation on VAP

WOP-2ac-LR2(config):/interface/wlan0-va0/vap# **station-isolation true** (Enable traffic isolation between clients within a single VAP. To disable, enter **false**)

Shaper configuration

WOP-2ac-LR2(config):/interface/wlan0-va0/vap# **shaper-per-sta-rx** (Configuration of the shaper in the direction from the clients (each individually) connected to this VAP of the access point)
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/shaper-per-sta-rx# **value X** (where X - maximum data rate in Kbps)
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/shaper-per-sta-rx# **mode kbps** (Enabling shaper. To disable, enter **off**)
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/shaper-per-sta-rx# **exit**

WOP-2ac-LR2(config):/interface/wlan0-va0/vap# **shaper-per-sta-tx** (Configuration of the shaper in the direction to the clients (each individually) connected to this VAP of the access point)
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/shaper-per-sta-tx# **value X** (where X - maximum data rate in Kbps)
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/shaper-per-sta-tx# **mode kbps** (Enabling shaper. To disable, enter **off**)
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/shaper-per-sta-tx# **exit**

WOP-2ac-LR2(config):/interface/wlan0-va0/vap# **shaper-per-vap-rx** (Configuration of the shaper in the direction from the clients (summary) connected to this VAP of the access point)
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/shaper-per-vap-rx# **value X** (where X - maximum data rate in Kbps)
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/shaper-per-vap-rx# **mode kbps** (Enabling shaper. To disable, enter **off**)
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/shaper-per-vap-rx# **exit**

WOP-2ac-LR2(config):/interface/wlan0-va0/vap# **shaper-per-vap-tx** (Configuration of the shaper in the direction to the clients (summary) connected to this VAP of the access point)
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/shaper-per-vap-tx# **value X** (where X - maximum data rate in Kbps)
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/shaper-per-vap-tx# **mode kbps** (Enabling shaper. To disable, enter **off**)
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/shaper-per-vap-tx# **exit**

Select prioritization method

WOP-2ac-LR2(config):/interface/wlan0-va0/vap# **priority-by-dscp false** (Priority analysis from the CoS (Class of Service) field of tagged packets. Default value: **true**. In this case the priority from the DSCP field of the IP packet header is analyzed)

Configuration of access control via MAC

WOP-2ac-LR2(config):/interface/wlan0-va0/vap# **acl**
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/acl# **mac**
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/acl/mac# **add XX:XX:XX:XX:XX:XX** (where
XX:XX:XX:XX:XX:XX - MAC address of the device, which should be allowed/forbidden to access. To
remove an address from the list, use the **del** command)
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/acl/mac# **exit**
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/acl# **policy allow** (Selects the policy that only those
clients whose MAC addresses are contained in the list will be allowed to connect to this VAP. Default
value: **deny** - policy that will deny connection to this VAP to clients whose MAC addresses are contained
in the list)
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/acl# **enable true** (Enable selected access policy. To
disable, enter **false**)

VLAN mapping

WOP-2ac-LR2(config):/interface/wlan0-va0/vap# **vlan-mapping**
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/vlan-mapping# **rule**
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/vlan-mapping/rule# **add name1** (where "name1" - mapping rule name. To
remove the rule use the **del** command)
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/vlan-mapping/rule# **name1**
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/vlan-mapping/rule/name1# **eth-vlan-id X** (where X - VLAN ID in Ethernet)
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/vlan-mapping/rule/name1# **eth-priority X** (where X - 802.1P priority when
transmitting in Ethernet. Possible values: 0-7, auto. If priority is auto or not specified in this option - the original will be
used)
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/vlan-mapping/rule/name1# **wlan-vlan-id X** (where X - VLAN ID in WLAN)
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/vlan-mapping/rule/name1# **wlan-priority X** (where X - 802.1P priority
when transmitting in WLAN. Possible values: 0-7, auto. If priority is auto or not specified in this option - the original will be
used)
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/vlan-mapping/rule/name1# **exit**
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/vlan-mapping/rule# **exit**
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/vlan-mapping# **enable true** (Enabling vlan-mapping. To disable,
enter **false**)

Limiting the number of multicast groups for a client

General limitation of the number of groups for each client connected to a given VAP

WOP-2ac-LR2(config):/interface/wlan0-va0/vap# **multicast-group-limits**
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/multicast-group-limits# **default-limit X** (where X - maximum number of multicast groups that the client can subscribe to. Possible values: 1-64. Default: 64)
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/multicast-group-limits# **enable true** (Enable multicast-group-limits. To disable, enter **false**)

Individual limitation of the number of groups for a particular client

WOP-2ac-LR2(config):/interface/wlan1-va0/vap# **multicast-group-limits**
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/multicast-group-limits# **mac**
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/multicast-group-limits/mac#
add XX:XX:XX:XX:XX:XX (where XX:XX:XX:XX:XX:XX - MAC address of the device, for which limiting is set. To remove use the **del** command)
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/multicast-group-limits/mac# **XX:XX:XX:XX:XX:XX** (where XX:XX:XX:XX:XX:XX - MAC address of the device, for which limiting is set)
WOP-2ac-LR2(config):/interface/wlan0-va0/vap/multicast-group-limits/mac/XX:XX:XX:XX:XX:XX# **limit X** (where X - maximum number of multicast groups that the client can subscribe to. Possible values: 1-64)
WOP-2ac-LR2(config):/interface/wlan1-va0/vap/multicast-group-limits/mac/XX:XX:XX:XX:XX:XX# **exit**
WOP-2ac-LR2(config):/interface/wlan1-va0/vap/multicast-group-limits/mac# **exit**
WOP-2ac-LR2(config):/interface/wlan1-va0/vap/multicast-group-limits# **enable true** (Enable multicast-group-limits. To disable enter **false**)

For all clients for which no individual limit is specified – the general limit on the number of groups set in the 'default-limit' will be applied.

BPDU packet filtering

Configuring BPDU packet filtering for a specific VAP

WOP-2ac-LR2(config):/interface/wlan0-va0# **common**
WOP-2ac-LR2(config):/interface/wlan0-va0/common# **bpdu-filter true** (Enable BPDU packet filtering on the current VAP. To disable enter **false**)

Configuring BPDU packet filtering for the eth0 interface

WOP-2ac-LR2(config):/interface/eth0# **common**
WOP-2ac-LR2(config):/interface/eth0/common# **bpdu-filter true** (Enable BPDU packet filtering on the eth0 interface. To disable enter **false**)

5.4 Radio configuration

To set the channel and change the power, use the following commands:

Change of operation channel, bandwidth and radio interface power

WOP-2ac-LR2(root):/# **configure**
WOP-2ac-LR2(config):/# **interface**
WOP-2ac-LR2(config):/interface# **wlan0**
WOP-2ac-LR2(config):/interface/wlan0# **wlan**
WOP-2ac-LR2(config):/interface/wlan0/wlan# **radio**
WOP-2ac-LR2(config):/interface/wlan0/wlan/radio# **tx-power X** (where X - power level in dBm)
WOP-2ac-LR2(config):/interface/wlan0/wlan/radio# **channel X** (where X - number of static channel, on which the point will operate)
WOP-2ac-LR2(config):/interface/wlan0/wlan/radio# **bandwidth X** (where X - channel bandwidth)

5.4.1 Advanced Radio settings

Changing the operating mode of the radio interface

WOP-2ac-LR2(config):/interface/wlan0/wlan/radio# **work-mode X** (where X - radio interface operation mode according to IEEE 802.11. Possible values: bg, bgn, n)

Enabling fixed central frequency

WOP-2ac-LR2(config):/interface/wlan0/wlan/radio# **center-frequency true** (Enabling fixed central frequency. To disable enter **false**)

Changing the primary channel

WOP-2ac-LR2(config):/interface/wlan0/wlan/radio# **control-sideband lower** (Parameter may take values: lower, upper. By default: **lower**)

Enabling the use of Short Guard Interval

WOP-2ac-LR2(config):/interface/wlan0/wlan/radio# **sgi true** (Enabling the use of a Short Guard Interval for data transmission of 400 ns instead of 800 ns. To disable, enter **false**)

Enabling STBC

WOP-2ac-LR2(config):/interface/wlan0/wlan/radio# **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-2ac-LR2(config):/interface/wlan0/wlan/radio# **aggregation true** (Enabling aggregation on Radio - support for AMPDU/AMSDU. To disable, enter **false**)

Enabling the short preamble

WOP-2ac-LR2(config):/interface/wlan0/wlan/radio# **short-preamble true** (Enabling the short packet preamble. To disable, enter **false**)

Polling configuration

WOP-2ac-LR2(config):/interface/wlan0/wlan/radio# **polling**
WOP-2ac-LR2(config):/interface/wlan0/wlan/radio/polling# **enable true** (Enabling polling. To disable enter **false**)
WOP-2ac-LR2(config):/interface/wlan0/wlan/radio/polling# **tx-duration X** (where X - maximum possible time of traffic transfer by the subscriber's station in ms. Possible values: 1-100. Default: 10)
WOP-2ac-LR2(config):/interface/wlan0/wlan/radio/polling# **tx-modulation X** (The baud rate for control packets. Possible values: 6, 9, 12,18, 24, 36, 48, 54. Default: 24)

Enabling fixed channel rate

WOP-2ac-LR2(config):/interface/wlan0/wlan/radio# **fixed-rate X** (where X - the name of the modulation in uppercase letters without spaces, for example - OFDM54, MCS15. Allowed values are determined by the mode of the radio interface and channel bandwidth)
WOP-2ac-LR2(config):/interface/wlan0/wlan/radio# **enable-fixed-rate true** (Enable fixed channel rate. To disable, enter **false**)

Channel rate limiting

WOP-2ac-LR2(config):/interface/wlan0/wlan/radio# **maximal-rate-legacy X** (where X - the name of the modulation in uppercase letters without spaces. The parameter is used when connecting clients in IEEE 802.11g mode)
WOP-2ac-LR2(config):/interface/wlan0/wlan/radio# **maximal-rate-ht X** (where X - the name of the modulation in uppercase letters without spaces. The parameter is used when connecting clients in IEEE 802.11n mode)
WOP-2ac-LR2(config):/interface/wlan0/wlan/radio# **enable-maximal-rate true** (Enable channel rate limiting. To disable, enter **false**)

Enabling Broadcast/Multicast shaper

WOP-2ac-LR2(config):/interface/wlan0/wlan/radio# **tx-broadcast-limit X** (where X - Restricting broadcast/multicast traffic over the wireless network, specify a limit for broadcast traffic per packet/s)

ACK timeout configuration

WOP-2ac-LR2(config):/interface/wlan0/wlan/radio# **ack-timeout X** (where X - ACK timeout. Possible values: 1-255. By default: 64)

Enabling QoS and parameter changes

WOP-2ac-LR2(config):/interface/wlan0/wlan/radio# **qos**
WOP-2ac-LR2(config):/interface/wlan0/wlan/radio/qos# **enable true** (When enabled the EDCA parameters that set in configuration are applied. To disable enter **false**)
WOP-2ac-LR2(config):/interface/wlan0/wlan/radio/qos# **edca-ap** (Configuring the access point's QoS parameters (traffic is transmitted from the access point to the client))
WOP-2ac-LR2(config):/interface/wlan0/wlan/radio/qos/edca-ap# **bk** (Configure EDCA parameters for low-priority high-bandwidth queues (802.1p priorities: cs1, cs2))
WOP-2ac-LR2(config):/interface/wlan0/wlan/radio/qos/edca-ap/bk# **aifs X** (where X - the time frame(s) of data measured in slots. Takes the values: 1-255)
WOP-2ac-LR2(config):/interface/wlan0/wlan/radio/qos/edca-ap/bk# **cwmin X** (where 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-2ac-LR2(config):/interface/wlan0/wlan/radio/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-2ac-LR2(config):/interface/wlan0/wlan/radio/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-2ac-LR2(config):/interface/wlan0/wlan/radio/qos/edca-ap/bk# **exit**
WOP-2ac-LR2(config):/interface/wlan0/wlan/radio/qos/edca-ap# **exit**
WOP-2ac-LR2(config):/interface/wlan0/wlan/radio/qos# **edca-sta** (Configuring the client station QoS parameters (traffic is transmitted from the client station to the access point))

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

5.5 WDS configuration

> ✅ **When configuring a WDS connection, it is necessary that the same channel and channel width be selected on the devices to be connected via WDS in the radio interface settings (see Radio settings above).**

WDS configuration

WOP-2ac-LR2(root):/# **configure**
WOP-2ac-LR2(config):/# **interface**
WOP-2ac-LR2(config):/interface# **wlan0-wds0** (Select WDS link. Possible values: wlan0-wds0 - wlan0-wds7)
WOP-2ac-LR2(config):/interface/wlan0-wds0# **wds**
WOP-2ac-LR2(config):/interface/wlan0-wds0/wds# **mac-addr XX:XX:XX:XX:XX:XX** (Oncoming access point MAC address)
WOP-2ac-LR2(config):/interface/wlan0-wds0/wds# **exit**
WOP-2ac-LR2(config):/interface/wlan0-wds0# **common**
WOP-2ac-LR2(config):/interface/wlan0-wds0/common# **enabled true** (Enabling WDS link. To disable, enter **false**)
WOP-2ac-LR2(config):/interface/wlan0-wds0/common# **exit**
WOP-2ac-LR2(config):/interface/wlan0-wds0# **exit**
WOP-2ac-LR2(config):/interface# **wlan0**
WOP-2ac-LR2(config):/interface/wlan0# **wlan**
WOP-2ac-LR2(config):/interface/wlan0/wlan# **wds**
WOP-2ac-LR2(config):/interface/wlan0/wlan/wds# **security-mode WPA2** (Select WPA2 security mode. Possible value: off - without password)
WOP-2ac-LR2(config):/interface/wlan0/wlan/wds# **key-wpa password123** (The key/password required to connect to the counter AP. The key must be between 8 and 63 characters long)
WOP-2ac-LR2(config):/interface/wlan0/wlan/wds# **enabled true** (Enabling WDS. To disable, enter **false**)
WOP-2ac-LR2(config):/interface/wlan0/wlan/wds# **save**

Configuration of the **counter BS** is carried out in the same way.

Enabling large packet transmission in WDS

WOP-2ac-LR2(root):/# **configure**
WOP-2ac-LR2(config):/# **interface**
WOP-2ac-LR2(config):/interface# **eth0**
WOP-2ac-LR2(config):/interface/eth0# **eth**
WOP-2ac-LR2(config):/interface/eth0/eth# **jumbo-support true** (Enabling large packet transmission. To disable, enter **false**)
WOP-2ac-LR2(config):/interface/eth0/eth# **exit**
WOP-2ac-LR2(config):/interface/eth0# **exit**
WOP-2ac-LR2(config):/interface# **exit**

<u>**Increase MTU on interfaces:**</u>

WOP-2ac-LR2(config):/interface# **eth0**
WOP-2ac-LR2(config):/interface/eth0# **common**
WOP-2ac-LR2(config):/interface/eth0/common# **mtu X** (where X - MTU value. Maximum value is 2400)
WOP-2ac-LR2(config):/interface/eth0/common# **exit**
WOP-2ac-LR2(config):/interface/eth0# **exit**
WOP-2ac-LR2(config):/interface# **wlan0-wds0**
WOP-2ac-LR2(config):/interface/wlan0-wds0# **common**
WOP-2ac-LR2(config):/interface/wlan0-wds0/common# **mtu X** (where X - MTU value. Maximum value is 2400)
WOP-2ac-LR2(config):/interface/wlan0-wds0/common# **save**

5.6 System settings

5.6.1 Device firmware update

Device firmware update via tftp

WOP-2ac-LR2(root):/# **firmware upload tftp <tftp server IP address> <Firmware file name>** (Example: firmware upload tftp 192.168.1.15 WOP-2ac-LR2-1.7.0_build_358.tar.gz)
WOP-2ac-LR2(root):/# **firmware upgrade**

Device firmware update via http

WOP-2ac-LR2(root):/# **firmware upload http <URL to download firmware>** (Example: firmware upload http https://eltex-co.ru/upload/iblock/c41/WOP-2ac-LR2-1.7.0_build_358.tar.gz)
WOP-2ac-LR2(root):/# **firmware upgrade**

Switching to a backup version of the access point firmware

WOP-2ac-LR2(root):/# **firmware switch**

5.6.2 Device configuration management

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

WOP-2ac-LR2(root):/# **manage-config reset-to-default**

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

WOP-2ac-LR2(root):/# **manage-config reset-to-default-without-management**

Download the device configuration file to tftp server

WOP-2ac-LR2(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-2ac-LR2(root):/# **manage-config upload tftp <tftp server IP address> <Configuration file name>**
(Example: manage-config upload tftp 192.168.1.15 config.json)
WOP-2ac-LR2(root):/# **manage-config apply** (Apply configuration to the access point)

5.6.3 Device reboot

The command for rebooting the device.

WOP-2ac-LR2(root):/# **reboot**

5.6.4 Authentication mode configuration

The device has a factory admin account with 'password' password. This account can't be deleted. You can change the password with the following commands.

Changing the password for the admin account

WOP-2ac-LR2(root):/# **configure**
WOP-2ac-LR2(config):/# **authentication**
WOP-2ac-LR2(config):/authentication# **admin-password <New password for admin>** (1 to 64 characters, including Latin letters and numbers)
WOP-2ac-LR2(config):/authentication# **save**

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

> ✅ One of two roles must be assigned to new users:
> **admin** – a user with this role will have full access to the configuration and monitoring of the BS;
> **viewer** – a user with this role will only have access to monitoring the BS.

The following commands are used to create additional users:

Adding new users

WOP-2ac-LR2(root):/# **configure**
WOP-2ac-LR2(config):/# **authentication**
WOP-2ac-LR2(config):/authentication# **user**
WOP-2ac-LR2(config):/authentication/user# **add userX** (where "userX" - name of the new user. To delete use the **del** command)
WOP-2ac-LR2(config):/authentication/user# **userX**
WOP-2ac-LR2(config):/authentication/user/userX# **login userX** (where "userX" - name of the created user)
WOP-2ac-LR2(config):/authentication/user/userX# **password <Password for the userX user>** (1 to 64 characters, including Latin letters and numbers)
WOP-2ac-LR2(config):/authentication/user/userX# **role admin** (Configuration rights assigned to user. Possible value: viewer - only monitoring will be available for this user)
WOP-2ac-LR2(config):/authentication/user/userX# **save**

To authenticate via RADIUS server, you should configure its access parameters.

Configuring RADIUS server access settings

WOP-2ac-LR2(root):/# **configure**
WOP-2ac-LR2(config):/# **authentication**
WOP-2ac-LR2(config):/authentication# **radius**
WOP-2ac-LR2(config):/authentication/radius# **auth-address X.X.X.X** (where X.X.X.X - RADIUS server IP address)
WOP-2ac-LR2(config):/authentication/radius# **auth-port X** (where X - port of the RADIUS server, which is used for authentication and authorization. Default: 1812)
WOP-2ac-LR2(config):/authentication/radius# **auth-password secret** (where "secret" - key for RADIUS server, which is used for authentication and authorization)
WOP-2ac-LR2(config):/authentication/radius# **exit**
WOP-2ac-LR2(config):/authentication# **radius-auth true** (Enable RADIUS server authentication mode. To disable enter **false**)
WOP-2ac-LR2(config):/authentication# **save**

> ✅ When authenticating via RADIUS server, you should always create a local account, which is the same as the account on the RADIUS server.
> In this case, in the local account must be specified the role that determines the access rights (admin or viewer).
> If the RADIUS server is unavailable, authentication will be performed using the local account.

5.6.5   DCHP-snooping configuration

Commands for DHCP-snooping configuration

WOP-2ac-LR2(root):/# **configure**
WOP-2ac-LR2(config):/# **dhcp-snooping**
WOP-2ac-LR2(config):/dhcp-snooping# **enable true** (Enable DHCP-snooping. To disable enter **false**)
WOP-2ac-LR2(config):/dhcp-snooping# **vlan** (DHCP-snooping configuration for tagged traffic)
WOP-2ac-LR2(config):/dhcp-snooping/vlan# **add vlan-group** (where 'vlan-group' - VLAN group name, for which DHCP-snooping will operate)
WOP-2ac-LR2(config):/dhcp-snooping/vlan# **vlan-group**
WOP-2ac-LR2(config):/dhcp-snooping/vlan/vlan-group# **vid 'X;Y-Z'** (where X - VLAN number, Y-Z - range of VLANs, which will be in 'vlan-group' and for which DHCP-snooping will operate. VLAN range configuration example: vid '10;100-110')
WOP-2ac-LR2(config):/dhcp-snooping/vlan/vlan-group# **exit**
WOP-2ac-LR2(config):/dhcp-snooping/vlan# **exit**
WOP-2ac-LR2(config):/dhcp-snooping# **untag true** (Enable DHCP-snooping for untagged traffic. To disable enter **false**)

✅   By default, only eth0 is considered a trusted port. For all wlan0-vaX interfaces, dhcp-trusted false. You can change the settings by using the commands below.

Configure a trusted port on a VAP:

Commands for configuring trusted ports

WOP-2ac-LR2(config):/# **interface**
WOP-2ac-LR2(config):/interface# **wlan0-va0**
WOP-2ac-LR2(config):/interface/wlan0-va0# **common**
WOP-2ac-LR2(config):/interface/wlan0-va0/common# **dhcp-trusted true** (Enable trusted port. When set to **true**, the DHCP server that is on the client side of the VAP is allowed to operate. To disable, enter **false**, in which case you will not be able to work with such a DCHP server)

5.6.6 Setting the date and time

Commands to configure NTP server time synchronization

WOP-2ac-LR2(root):/# **configure**
WOP-2ac-LR2(config):/# **date-time**
WOP-2ac-LR2(config):/date-time# **mode ntp** (Enable NTP operation mode. Possible value is manual - set the time manually)
WOP-2ac-LR2(config):/date-time# **ntp**
WOP-2ac-LR2(config):/date-time/ntp# **server <NTP server IP address>** (NTP server configuration)
WOP-2ac-LR2(config):/date-time/ntp# **exit**
WOP-2ac-LR2(config):/date-time# **common**
WOP-2ac-LR2(config):/date-time/common# **timezone 'Asia/Novosibirsk (Novosibirsk)'** (Timezone configuration)
WOP-2ac-LR2(config):/date-time/common# **save**

5.7 Monitoring

5.7.1 Wi-Fi clients

To display the monitoring of connected Wi-Fi clients the following command is used:

---

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

where <mac address of the client 1> ... <mac address of the client N> - MAC addresses of the client devices connected to the access point. To display information for all clients, type all instead of <mac address of the client>;

filter is a special word, after which the monitoring parameters required for output by client/clients are specified;

... <parameter N> - monitoring parameter/parameters required for output by client/clients.

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

WOP-2ac-LR2(root):/# **monitoring associated-clients** <Tab>

```
e0:d9:e3:49:c1:a0
60:ab:67:ba:89:24
all
```

To display the list of monitoring parameters, press the TAB key after **filter**.

WOP-2ac-LR2(root):/# **monitoring associated-clients 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 on all connected clients

WOP-2ac-LR2(root):/# **monitoring associated-clients all**

```
index                     | 0
interface                 | wlan0-va0
state                     | ASSOC AUTH_SUCCESS
hw-addr                   | e0:d9:e3:49:c1:a0
ip-addr                   | 192.168.50.61
hostname                  | WB-2P-LR2
authorized                | true
captive-portal-vap        | false
enterprise-vap            | false
rx-retry-count            | 34
tx-fails                  | 0
tx-period-retry           | 0
tx-retry-count            | 27
noise-1                   | -71
noise-2                   | -86
rssi-1                    | -42
rssi-2                    | -42
snr-1                     | 29
snr-2                     | 44
rssi-from-sta-1           | -46
rssi-from-sta-2           | -46
snr-from-sta-1            | 44
snr-from-sta-2            | 36
tx-rate                   | MCS11 NO SGI 52
rx-rate                   | MCS5 NO SGI 52
rx-bw                     | 20M
rx-bw-all                 | 20M
tx-bw                     | 20M
uptime                    | 00:12:47
multicast-groups-count    | 0
wireless-mode             | n
eltex-serial-number       | WP36000038
eltex-firmware-version    | 2.5.0.165
eltex-board-type          | WB-2P-LR2
perftest-capable          | true
snr-rssi-capable          | true
link-capacity             | 37 (not changed)
link-quality              | 100 (not changed)
link-quality-common       | 67
actual-tx-rate            | 0
actual-rx-rate            | 0
shaped-rx-rate            | 0
actual-tx-pps             | 0
actual-rx-pps             | 0
shaped-rx-pps             | 0
polling-max-resp-delay    | 0
name                      | 0

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

```
Total Packets:        | 83              | 127            |
TX success:           | 100             |                |
Total Bytes:          | 18529           | 21472          |
Data Packets:         | 75              | 89             |
Data Bytes:           | 16213           | 17609          |
Mgmt Packets:         | 8               | 38             |
Mgmt Bytes:           | 366             | 821            |
-------------------------------------------------------------------
```

```
Rate                Transmitted              Received
-------------------------------------------------------------------
dsss1          | 10        |  12%|          40 |  31%|
ofdm6          | 0         |   0%|           1 |   0%|
mcs3           | 0         |   0%|          21 |  16%|
mcs4           | 1         |   1%|          12 |   9%|
mcs5           | 48        |  57%|          34 |  26%|
mcs6           | 13        |  15%|          18 |  14%|
mcs11          | 1         |   1%|           0 |   0%|
mcs12          | 10        |  12%|           0 |   0%|
-------------------------------------------------------------------
```

```
Multicast groups: none

index                   | 1
interface               | wlan0-va0
state                   | ASSOC SLEEP AUTH_SUCCESS
hw-addr                 | 60:ab:67:ba:89:24
ip-addr                 | 192.168.50.77
hostname                | Test
authorized              | true
captive-portal-vap      | false
enterprise-vap          | false
rx-retry-count          | 18
tx-fails                | 0
tx-period-retry         | 0
tx-retry-count          | 0
noise-1                 | -75
noise-2                 | -89
rssi-1                  | -49
rssi-2                  | -34
snr-1                   | 26
snr-2                   | 55
rssi-from-sta-1         | N/A
rssi-from-sta-2         | N/A
snr-from-sta-1          | N/A
snr-from-sta-2          | N/A
tx-rate                 | MCS5 NO SGI 52
rx-rate                 | MCS7 NO SGI 65
rx-bw                   | 20M
rx-bw-all               | 20M
tx-bw                   | 20M
uptime                  | 00:00:05
multicast-groups-count  | 1
wireless-mode           | n
perftest-capable        | false
snr-rssi-capable        | false
link-capacity           | 0
link-quality            | 0
```

```
link-quality-common      | 100
actual-tx-rate           | 0
actual-rx-rate           | 1
shaped-rx-rate           | 0
actual-tx-pps            | 0
actual-rx-pps            | 1
shaped-rx-pps            | 0
polling-max-resp-delay   | 0
name                     | 1
```

Rate	Transmitted	Received	
Total Packets:	5	70	
TX success:	100		
Total Bytes:	573	6640	
Data Packets:	2	24	
Data Bytes:	316	4768	
Mgmt Packets:	3	46	
Mgmt Bytes:	205	192	

Rate	Transmitted		Received	
dsss1	5	100%	9	13%
ofdm24	0	0%	41	59%
mcs0	0	0%	1	1%
mcs2	0	0%	1	1%
mcs3	0	0%	2	2%
mcs4	0	0%	4	5%
mcs5	0	0%	3	4%
mcs7	0	0%	8	11%

Multicast groups		Clients	
MAC	IP	Count	IP
0 01:00:5E:00:00:FB	xxx.0.0.251	1	192.168.41.97(295)

Output of information on specific client(s)

WOP-2ac-LR2(root):/# **monitoring associated-clients e0:d9:e3:49:c1:a0** (it is possible to specifiy several MAC addresses, e.g. **monitoring associated-clients e0:d9:e3:93:f9:e0 e0:d9:e3:7a:88:20**)

```
index                     | 0
interface                 | wlan0-va0
state                     | ASSOC AUTH_SUCCESS
hw-addr                   | e0:d9:e3:49:c1:a0
ip-addr                   | 192.168.50.61
hostname                  | WB-2P-LR2
authorized                | true
captive-portal-vap        | false
enterprise-vap            | false
rx-retry-count            | 36
tx-fails                  | 0
tx-period-retry           | 0
tx-retry-count            | 27
noise-1                   | -99
noise-2                   | -90
rssi-1                    | -42
rssi-2                    | -27
snr-1                     | 57
snr-2                     | 63
rssi-from-sta-1           | -46
rssi-from-sta-2           | -46
snr-from-sta-1            | 44
snr-from-sta-2            | 36
tx-rate                   | MCS5 NO SGI 52
rx-rate                   | MCS6 NO SGI 58.5
rx-bw                     | 20M
rx-bw-all                 | 20M
tx-bw                     | 20M
uptime                    | 00:15:08
multicast-groups-count    | 0
wireless-mode             | n
eltex-serial-number       | WP36000038
eltex-firmware-version    | 2.5.0.165
eltex-board-type          | WB-2P-LR2
perftest-capable          | true
snr-rssi-capable          | true
link-capacity             | 38 (not changed)
link-quality              | 100 (not changed)
link-quality-common       | 67
actual-tx-rate            | 0
actual-rx-rate            | 0
shaped-rx-rate            | 0
actual-tx-pps             | 0
actual-rx-pps             | 0
shaped-rx-pps             | 0
polling-max-resp-delay    | 0
name                      | 0

  Rate              Transmitted           Received
```

```
------------------------------------------------------------------
Total Packets:        | 94                  | 138                 |
TX success:           | 100                 |                     |
Total Bytes:          | 21924               | 23851               |
Data Packets:         | 86                  | 95                  |
Data Bytes:           | 19322               | 19702               |
Mgmt Packets:         | 8                   | 43                  |
Mgmt Bytes:           | 366                 | 821                 |
------------------------------------------------------------------


Rate                  Transmitted          Received
------------------------------------------------------------------
dsss1                 | 10       |    10%|            46 |    33%|
ofdm6                 | 0        |     0%|             1 |     0%|
mcs3                  | 0        |     0%|            21 |    15%|
mcs4                  | 1        |     1%|            12 |     8%|
mcs5                  | 57       |    60%|            34 |    24%|
mcs6                  | 13       |    13%|            23 |    16%|
mcs11                 | 3        |     3%|             0 |     0%|
mcs12                 | 10       |    10%|             0 |     0%|
------------------------------------------------------------------


Multicast groups: none
```

Monitoring parameters filtering

WOP-2ac-LR2(root):/# **monitoring associated-clients e0:d9:e3:49:c1:a0 filter hw-addr ip-addr tx-rate rx-rate uptime** (display a limited number of monitoring parameters for a specific client. It is possible to specify several mac addresses)

```
hw-addr               | e0:d9:e3:49:c1:a0
ip-addr               | 192.168.50.61
tx-rate               | MCS5 NO SGI 52
rx-rate               | MCS4 NO SGI 39
uptime                | 00:17:18
```

WOP-2ac-LR2(root):/# **monitoring associated-clients all filter hw-addr rssi-1 rssi-2 wireless-mode interface** (display a limited number of monitoring parameters for all clients)

```
hw-addr               | e0:d9:e3:49:c1:a0
rssi-1                | -44
rssi-2                | -26
wireless-mode         | n
interface             | wlan0-va0

hw-addr               | 60:ab:67:ba:89:24
rssi-1                | -48
rssi-2                | -38
wireless-mode         | n
interface             | wlan0-va0
```

5.7.2   WDS

For WDS connection monitoring the following command is used:

---

monitoring wds-entries <mac address of the oncoming station 1> ... <mac address of the oncoming station N> **filter** <parameter 1> ... <parameter N>,

where <mac address of the oncoming station 1> ... <mac address of the oncoming station N> - The mac addresses of the oncoming base stations with which the WDS bridges are built. In order to output information for all the counter stations, type **all** instead of <mac address of the oncoming station>;

     filter - a special word, after which the monitoring parameters required for output by one or more oncoming BS are specified;

     <parameter 1> ... <parameter N> - parameter/parameters of monitoring required to output by one or more oncoming BS.

To display the list of BSs with which WDS bridges are built, press the TAB key after **monitoring wds-entries**.

WOP-2ac-LR2(root):/# **monitoring wds-entries** <Tab>

```
e0:d9:e3:49:c2:a0
e8:28:c1:f7:7f:b0
all
```

To display the list of monitoring parameters, press the TAB key after **filter**.

WOP-2ac-LR2(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 on all oncoming BS

WOP-2ac-LR2(root):/# **monitoring wds-entries** (or **monitoring wds-entries all**)

```
index                     | 0
interface                 | wlan0
state                     | WIFI_WDS
hw-addr                   | e0:d9:e3:49:c2:a0
ip-addr                   | 192.168.50.61
hostname                  | WOP-2ac-LR2
authorized                | false
captive-portal-vap        | false
enterprise-vap            | false
rx-retry-count            | 11
tx-fails                  | 20
tx-period-retry           | 11
tx-retry-count            | 361
noise-1                   | -46
noise-2                   | -33
rssi-1                    | -42
rssi-2                    | -33
snr-1                     | 4
snr-2                     | 0
rssi-from-sta-1           | -46
rssi-from-sta-2           | -46
snr-from-sta-1            | 48
snr-from-sta-2            | 49
wds-interface             | wlan0-wds0
tx-rate                   | MCS11 NO SGI 52
rx-rate                   | MCS3 NO SGI 26
rx-bw                     | 20M
rx-bw-all                 | 20M
tx-bw                     | 20M
uptime                    | 00:02:02
multicast-groups-count    | 0
wireless-mode             | n
eltex-firmware-version    | 2.5.0.165
eltex-board-type          | WOP-2ac-LR2
perftest-capable          | true
snr-rssi-capable          | true
link-capacity             | 47
link-quality              | 72
link-quality-common       | 30
actual-tx-rate            | 5
actual-rx-rate            | 0
shaped-rx-rate            | 0
actual-tx-pps             | 7
actual-rx-pps             | 0
shaped-rx-pps             | 0
polling-max-resp-delay    | 0
name                      | 0


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

```
Total Packets:        | 1138               | 45                 |
TX success:           | 96                 |                    |
Total Bytes:          | 153703             | 7190               |
Data Packets:         | 1113               | 24                 |
Data Bytes:           | 115939             | 2842               |
Mgmt Packets:         | 25                 | 21                 |
Mgmt Bytes:           | 2148               | 3580               |
------------------------------------------------------------------------

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

dsss1        | 25         |    2%|        24 |   54%|
mcs3         | 0          |    0%|        12 |   27%|
mcs4         | 246        |   21%|         6 |   13%|
mcs5         | 426        |   37%|         0 |    0%|
mcs6         | 254        |   22%|         0 |    0%|
mcs7         | 49         |    4%|         2 |    4%|
mcs10        | 21         |    1%|         0 |    0%|
mcs11        | 69         |    6%|         0 |    0%|
mcs12        | 47         |    4%|         0 |    0%|
mcs15        | 1          |    0%|         0 |    0%|
------------------------------------------------------------------------

Multicast groups: none

index                  | 1
interface              | wlan0
state                  | WIFI_WDS
hw-addr                | e8:28:c1:f7:7f:b0
ip-addr                | 100.110.0.229
hostname               | WOP-2ac-LR2-SYNC
authorized             | false
captive-portal-vap     | false
enterprise-vap         | false
rx-retry-count         | 237
tx-fails               | 0
tx-period-retry        | 4
tx-retry-count         | 78
noise-1                | -67
noise-2                | -67
rssi-1                 | -50
rssi-2                 | -37
snr-1                  | 17
snr-2                  | 30
rssi-from-sta-1        | -42
rssi-from-sta-2        | -42
snr-from-sta-1         | 49
snr-from-sta-2         | 50
wds-interface          | wlan0-wds1
tx-rate                | MCS11 NO SGI 52
rx-rate                | MCS12 NO SGI 78
rx-bw                  | 20M
rx-bw-all              | 20M
tx-bw                  | 20M
uptime                 | 00:01:47
multicast-groups-count | 0
wireless-mode          | n
eltex-firmware-version | 1.9.0 build 180
```

```
eltex-board-type          | WOP-2ac-LR2 SYNC
perftest-capable          | true
snr-rssi-capable          | true
link-capacity             | 52
link-quality              | 42
link-quality-common       | 42
actual-tx-rate            | 1
actual-rx-rate            | 3
shaped-rx-rate            | 0
actual-tx-pps             | 0
actual-rx-pps             | 6
shaped-rx-pps             | 0
polling-max-resp-delay    | 0
name                      | 1
```

Rate	Transmitted	Received	
Total Packets:	74	1042	
TX success:	100		
Total Bytes:	23710	122338	
Data Packets:	67	1035	
Data Bytes:	21209	88732	
Mgmt Packets:	7	7	
Mgmt Bytes:	357	486	

Rate	Transmitted		Received	
dsss1	7	9%	14	1%
cck5	0	0%	7	0%
ofdm6	1	1%	8	0%
ofdm54	2	2%	0	0%
mcs0	0	0%	6	0%
mcs1	0	0%	10	0%
mcs2	0	0%	24	2%
mcs3	2	2%	62	5%
mcs4	4	5%	87	8%
mcs5	10	13%	326	31%
mcs6	7	9%	26	2%
mcs7	8	10%	0	0%
mcs10	2	2%	129	12%
mcs11	13	17%	224	21%
mcs12	18	24%	117	11%
mcs13	0	0%	1	0%

```
Multicast groups: none
```

Display information one ore more oncoming BS

WOP-2ac-LR2(root):/# **monitoring wds-entries e8:28:c1:f7:7f:b0** (it is possible to specify several MAC addresses, e.g. **monitoring wds-entries e8:28:c1:ef:21:e0 e8:28:c1:ef:22:a0**)

```
index                    | 1
interface                | wlan0
state                    | WIFI_WDS
hw-addr                  | e8:28:c1:f7:7f:b0
ip-addr                  | 100.110.0.229
hostname                 | WOP-2ac-LR2-SYNC
authorized               | false
captive-portal-vap       | false
enterprise-vap           | false
rx-retry-count           | 478
tx-fails                 | 0
tx-period-retry          | 0
tx-retry-count           | 108
noise-1                  | -85
noise-2                  | -72
rssi-1                   | -50
rssi-2                   | -37
snr-1                    | 35
snr-2                    | 35
rssi-from-sta-1          | -40
rssi-from-sta-2          | -40
snr-from-sta-1           | 49
snr-from-sta-2           | 50
wds-interface            | wlan0-wds1
tx-rate                  | MCS6 NO SGI 58.5
rx-rate                  | MCS12 NO SGI 78
rx-bw                    | 20M
rx-bw-all                | 20M
tx-bw                    | 20M
uptime                   | 00:03:13
multicast-groups-count   | 0
wireless-mode            | n
eltex-firmware-version   | 1.9.0 build 180
eltex-board-type         | WOP-2ac-LR2 SYNC
perftest-capable         | true
snr-rssi-capable         | true
link-capacity            | 46
link-quality             | 100
link-quality-common      | 49
actual-tx-rate           | 1
actual-rx-rate           | 4
shaped-rx-rate           | 0
actual-tx-pps            | 1
actual-rx-pps            | 8
shaped-rx-pps            | 0
polling-max-resp-delay   | 0
name                     | 1

Rate              Transmitted           Received
```

```
--------------------------------------------------------------------
Total Packets:      | 142              | 1981                      |
TX success:         | 100              |                           |
Total Bytes:        | 43092            | 253835                    |
Data Packets:       | 135              | 1974                      |
Data Bytes:         | 38415            | 190181                    |
Mgmt Packets:       | 7                | 7                         |
Mgmt Bytes:         | 357              | 486                       |
--------------------------------------------------------------------


Rate                Transmitted          Received
--------------------------------------------------------------------
dsss1               | 7        |     4%|           26 |    1%|
cck5                | 0        |     0%|           11 |    0%|
ofdm6               | 1        |     0%|            8 |    0%|
ofdm54              | 2        |     1%|            0 |    0%|
mcs0                | 0        |     0%|           10 |    0%|
mcs1                | 0        |     0%|           11 |    0%|
mcs2                | 0        |     0%|           31 |    1%|
mcs3                | 2        |     1%|          126 |    6%|
mcs4                | 11       |     7%|          132 |    6%|
mcs5                | 34       |    23%|          456 |   23%|
mcs6                | 12       |     8%|          202 |   10%|
mcs7                | 14       |     9%|           20 |    1%|
mcs10               | 2        |     1%|          143 |    7%|
mcs11               | 30       |    21%|          489 |   24%|
mcs12               | 27       |    19%|          312 |   15%|
mcs13               | 0        |     0%|            3 |    0%|
--------------------------------------------------------------------


Multicast groups: none
```

Monitoring parameters filtering

WOP-2ac-LR2(root):/# **monitoring wds-entries e8:28:c1:f7:7f:b0 filter hw-addr ip-addr tx-rate rx-rate uptime** (display a limited number of monitoring parameters for a particular BS. It is possible to specify several mac addresses)

```
hw-addr                    | e8:28:c1:f7:7f:b0
ip-addr                    | 100.110.0.229
tx-rate                    | MCS6 NO SGI 58.5
rx-rate                    | MCS5 NO SGI 52
uptime                     | 00:03:52
```

WOP-2ac-LR2(root):/# **monitoring wds-entries all filter hw-addr rssi-1 rssi-2 wireless-mode wds-interface eltex-firmware-version** (display a limited number of monitoring parameters for all BS)

```
hw-addr                    | e0:d9:e3:49:c2:a0
rssi-1                     | -42
rssi-2                     | -42
wireless-mode              | n
wds-interface              | wlan0-wds0
eltex-firmware-version     | 1.9.0 build 180

hw-addr                    | e8:28:c1:f7:7f:b0
rssi-1                     | -50
rssi-2                     | -37
wireless-mode              | n
wds-interface              | wlan0-wds1
eltex-firmware-version     | 1.9.0 build 180
```

5.7.3 Speed testing

Speed Testing configuration

WOP-2ac-LR2(root):/# **configure**
WOP-2ac-LR2(config):/# **perftest**
WOP-2ac-LR2(config):/perftest# **server-ip X.X.X.X** (where X.X.X.X - IP address to be assigned to the interface of the subscriber station for the test. Default: 192.0.4.1. It is recommended to configure a subnet that is not used on an existing network)
WOP-2ac-LR2(config):/perftest# **client-ip X.X.X.X** (where X.X.X.X - IP address to be assigned to the interface of the base station for the test. Default: 192.0.4.1. It is recommended to configure a subnet that is not used on an existing network)
WOP-2ac-LR2(config):/perftest# **netmask X.X.X.X** (where X.X.X.X - subnet mask used for the test. Default is 255.255.255.0)
WOP-2ac-LR2(config):/perftest# **vlan-id X** (where X - VLAN ID used for the test. Default: 7. It is recommended to configure VLAN ID that is not used on an existing network)
WOP-2ac-LR2(config):/perftest# **save**

5.7.4 Device info

WOP-2ac-LR2(root):/# **monitoring information**

```
system-time: 19:21:43 17.09.2021
uptime: 1 d 04:19:13
software-version: 1.9.0 build 180
secondary-software-version: 1.9.0 build 180
boot-version: 1.9.0 build 180
memory-usage: 67
memory-free: 30
memory-used: 61
memory-total: 92
cpu: 1.23
is-default-config: false
board-type: WOP-2ac-LR2
hw-platform: WOP-2ac-LR2
factory-wan-mac: E0:D9:E3:91:F4:F0
factory-lan-mac: E0:D9:E3:91:F4:F0
factory-serial-number: WP2A000200
hw-revision: 1.1
session-password-initialized: false
ott-mode: false
last-reboot-reason: reboot by user
test-changes-mode: false
```

5.7.5 Network information

WOP-2ac-LR2(root):/# **monitoring wan-status**

```
interface: br0
protocol: dhcp
ip-address: 100.110.0.248
mac: e8:28:c1:c3:f7:b0
mask: 255.255.255.0
gateway: 100.110.0.1
DNS-1: 100.110.0.250
DNS-2: 170.17.0.100
rx-bytes: 11187477
rx-packets: 53202
tx-bytes: 6238687
tx-packets: 9886
```

WOP-2ac-LR2(root):/# **monitoring ethernet**

```
link: up
speed: 1000
duplex: enabled
rx-bytes: 11268823
rx-packets: 54218
tx-bytes: 6239221
tx-packets: 9894
```

WOP-2ac-LR2(root):/# **monitoring arp**

```
#        ip              mac
---------------------------------------------
0        100.110.0.252   9c:5c:6e:83:e5:5d
1        100.110.0.191   a8:f9:4b:aa:3f:21
```

WOP-2ac-LR2(root):/# **monitoring route**

```
Destination      Gateway         Mask            Flags     Interface
--------------------------------------------------------------------
0.0.0.0          100.110.0.1     0.0.0.0         UG        br0
100.110.0.0      0.0.0.0         255.255.255.0   U         br0
```

5.7.6 Wireless interfaces

WOP-2ac-LR2(root):/# **monitoring radio**

```
hwaddr: E8:28:C1:xx:xx:xx
status: on
noise-1: -77
noise-2: -77
utilization: 49
channel: 1
thermal: 37
bandwidth: 20
frequency: 2412
```

5.7.7 Information on ISS state

WOP-2ac-LR2-SYNC(root):/# **monitoring cluster-synchronization**

```
WOP-2ac-LR2-SYNC(root):/# monitoring cluster-synchronization
status | running

MAC                Ready    Master  Slot  Delay  Me
--------------------------------------------------------
e8:28:c1:ef:22:40 | true  | true  | 5    | 0    | false |
e8:28:c1:ef:22:30 | true  | false | 5    | 0    | true  |
e8:28:c1:ef:22:00 | true  | false | 5    | 0    | false |
--------------------------------------------------------
PTP info:
port-state         | SLAVE
servo-state        | SERVO_LOCKED_STABLE
master-offset      | 223
path-delay         | 3376
```

5.7.8 Event logging

WOP-2ac-LR2(root):/# **monitoring events**

```
Jan 1 03:00:21 WOP-2ac-LR2 daemon.info networkd[1034]: DHCP-client: Interface br0 obtained
lease on 100.110.0.222.
Dec 10 08:40:39 WOP-2ac-LR2 daemon.info monitord[1119]: event: 'authenticated' mac:
E0:D9:E3:49:C1:A0 ssid: 'test' interface: wlan0-va0 channel: 1 rssi: -60 location: 'root'
 reason: 0
Dec 10 08:43:14 WOP-2ac-LR2 daemon.info monitord[1119]: event: 'deauthenticated by STA'
 mac: E0:D9:E3:49:C1:A0 ssid: 'test' interface: wlan0-va0 channel: 1 rssi: -64 location:
'root' reason: 3 description: 'Deauth at STA leave BSS'
```

5.7.9 Spectrum analyzer

The spectrum analyzer provides information about channel load.

The analysis time for all the radio channels in the range is approximately 5 minutes.

> ✅ **Please note that all clients will disconnect from the base station during spectrum analyzer operation. The client stations will be connected again only when the spectrum analyzer finishes its work.**

As a result of the spectrum analyzer operation, information on the loading of each channel (in percent) will be displayed in the console:

WOP-2ac-LR2(root):/# **monitoring spectrum-analyzer**

```
Channel| CCA
      1| 57%
      2| 39%
      3| 12%
      4| 6%
      5| 47%
      6| 43%
      7| 30%
      8| 5%
      9| 9%
     10| 42%
     11| 56%
     12| 24%
     13| 18%
```

6 System recovering after firmware update failure

If during the firmware update (through the web interface or through autoupdate mechanism based on DHCP) a failure occures (e.g. due to power cutoff) and the device does not operate (the 'Power' indicator is constantly solid red), use the following algorithm to recover the device:

- Unpack the archive with firmware file.
- Connect PC to the device port. Set the following subnet mask on the network interface: 192.168.1.0/24.
- Run the TFTP client on the PC (for Windows, it is recommended to use the Tftpd32), specify 192.168.1.6 as the remote host address, and select the linux.bin file from the unpacked software archive for transfer.
- Run the command to send a file to a remote host (the **Put** command). The process of file transmission will be launched.
- If the transmission has started, please, wait for finishing. The device will write the firmware to its memory and launch the system automatically. The time of writing takes approximately 8 minutes. If the process is completed successfully, 'Power' indicator will be green or orange. The configuration of the device before failure is saved. If you can not connect the device, reset it to factory settings.
- If the process has not started, make sure that the network settings of PC are correct and try again. If it does not work, sent the device to maintanence service or proceed recovery using the connection via COM port through a special adapter (if available).

7 List of changes

Document version	Issue date	Revisions
Version 1.7	31.01.2022	Synchronization with firmware version 1.10.0 Added: • 4.10.3 The 'Ping Watchdog' submenu Corrected: • 4.5.1 The 'Wi-Fi clients' submenu • 4.5.7 The 'Radio Information' submenu • 4.9.1 The 'System Configuration' submenu • 5.3.4 Advanced VAP settings
Version 1.6	11.10.2021	Synchronization with firmware version 1.9.0 Added: • 3.3 Recommendations for lightning protection • 5.6.5 DHCP Snooping configuration Corrected: • 4.5.1 The «Wi-Fi clients» submenu • 4.5.2 The «WDS» submenu • 5.3.4 Advanced VAP settings • 5.7 Monitoring
Version 1.5	25.06.2021	Synchronization with firmware version 1.8.2 Added: • 4.5.8 The 'Cluster Synchronisation' submenu • 5.6.4 Authentication mode configuration • 5.7.2 Speed Testing Corrected: • 2.3 Technical features • 4.5.1 The 'Wi-Fi Clients' submenu • 4.5.7 The 'Radio Information' submenu • 4.6.3 The 'Synchronization' submenu • 4.10.4 The 'Authentication' submenu • 5.2 Network parameters configuration • 5.4.1 Advanced Radio settings • 5.6.4 Authentication mode configuration • 5.7.3 Device info

Version 1.4	21.12.2020	Synchronization with firmware version 1.7.0 Added: • 4.6.3 The 'Synchronization' submenu • 5 Managing the device using the command line
Version 1.3	20.08.2020	Synchronization with firmware version 1.6.0 Added: • 4.3 Test mode • 4.5.7 The 'Radio Information' submenu • The 'MAC ACL' subsection in the 'VAP' submenu Corrected the 'Traffic Statistics' submenu
Version 1.2	07.04.2020	Synchronization with firmware version 1.5.0 Corrected the 'Access' submenu
Version 1.1	11.12.2019	Synchronization with firmware version 1.4.1
Version 1.0	06.11.2019	First issue
Firmware version 1.10.0		

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/