

Wireless access point

# WOP-30L

User manual

Firmware version 2.3.0

IP address: 192.168.1.10

Username: admin

Password: password

## Contents

|          |                                                                     |           |
|----------|---------------------------------------------------------------------|-----------|
| <b>1</b> | <b>Introduction .....</b>                                           | <b>5</b>  |
| 1.1      | Annotation .....                                                    | 5         |
| 1.2      | Symbols .....                                                       | 5         |
| <b>2</b> | <b>Device description .....</b>                                     | <b>6</b>  |
| 2.1      | Purpose .....                                                       | 6         |
| 2.2      | Device specification .....                                          | 6         |
| 2.3      | Technical parameters .....                                          | 8         |
| 2.4      | Design .....                                                        | 10        |
| 2.5      | Light indication .....                                              | 11        |
| 2.6      | Restore the default configuration .....                             | 11        |
| 2.7      | Delivery packgae .....                                              | 11        |
| <b>3</b> | <b>Rules and recommendations for device installation .....</b>      | <b>12</b> |
| 3.1      | Safety rules .....                                                  | 12        |
| 3.2      | Installation recommendations .....                                  | 12        |
| 3.3      | Frequency bandwidths and channels in the 5 GHz band for Wi-Fi ..... | 13        |
| 3.4      | Calculating the number of required access points .....              | 13        |
| 3.5      | Channel selection for neighboring access points .....               | 13        |
| <b>4</b> | <b>Installation .....</b>                                           | <b>15</b> |
| 4.1      | Device installation on a mast/pole .....                            | 15        |
| 4.2      | Device installation on a wall .....                                 | 16        |
| 4.3      | Connection .....                                                    | 18        |
| 4.3.1    | Instructions for sealing antenna connectors .....                   | 19        |
| <b>5</b> | <b>Device management via the web interface .....</b>                | <b>22</b> |
| 5.1      | Getting started .....                                               | 22        |
| 5.2      | Applying configuration and discarding changes .....                 | 23        |
| 5.3      | Web interface basic elements .....                                  | 24        |
| 5.4      | The “Monitoring” menu .....                                         | 25        |
| 5.4.1    | The “Wi-Fi Clients” submenu .....                                   | 25        |
| 5.4.2    | The “Traffic Statistics” submenu .....                              | 27        |
| 5.4.3    | The “Scan Environment” submenu .....                                | 29        |
| 5.4.4    | The “Events” submenu .....                                          | 30        |
| 5.4.5    | The “Network Information” submenu .....                             | 31        |
| 5.4.6    | The “Radio Information” submenu .....                               | 33        |
| 5.4.7    | The “Device Information” submenu .....                              | 34        |

|          |                                                                             |           |
|----------|-----------------------------------------------------------------------------|-----------|
| 5.5      | The “Radio” menu.....                                                       | 35        |
| 5.5.1    | The “Radio 2.4 GHz” submenu .....                                           | 35        |
| 5.5.2    | The “Radio 5 GHz” submenu .....                                             | 39        |
| 5.5.3    | The “Advanced” submenu.....                                                 | 43        |
| 5.6      | The “VAP” menu .....                                                        | 44        |
| 5.6.1    | The “Summary” submenu .....                                                 | 44        |
| 5.6.2    | The “VAP” submenu .....                                                     | 45        |
| 5.7      | The “Network Settings” menu.....                                            | 50        |
| 5.7.1    | The “System Configuration” submenu .....                                    | 50        |
| 5.7.2    | The “Access” submenu .....                                                  | 51        |
| 5.8      | The “External Services” menu .....                                          | 52        |
| 5.8.1    | The “Captive Portal” submenu.....                                           | 52        |
| 5.8.2    | The “AirTune” submenu .....                                                 | 53        |
| 5.9      | The “System” menu .....                                                     | 54        |
| 5.9.1    | The “Device Firmware Upgrade” submenu .....                                 | 54        |
| 5.9.2    | The “Configuration” submenu .....                                           | 55        |
| 5.9.3    | The “Reboot” submenu .....                                                  | 55        |
| 5.9.4    | The “Password” submenu .....                                                | 56        |
| 5.9.5    | The “Log” submenu .....                                                     | 56        |
| 5.9.6    | The “Date and Time” submenu .....                                           | 57        |
| <b>6</b> | <b>Managing the device using the command line .....</b>                     | <b>59</b> |
| 6.1      | Connection to the device.....                                               | 59        |
| 6.2      | Network parameters configuration .....                                      | 60        |
| 6.2.1    | Network parameters configuration via set-management-vlan-mode utility ..... | 61        |
| 6.2.2    | IPv6 network parameters configuration.....                                  | 62        |
| 6.3      | Virtual Wi-Fi access points (VAP) configuration.....                        | 64        |
| 6.3.1    | Configuration of VAP without encryption.....                                | 65        |
| 6.3.2    | Configuration of VAP with OWE encryption .....                              | 66        |
| 6.3.3    | Configuration of VAP with OWE and OWE Transition Mode .....                 | 67        |
| 6.3.4    | Configuration of VAP with WPA-Personal security mode.....                   | 68        |
| 6.3.5    | Configuration of VAP with Enterprise authorization .....                    | 69        |
| 6.3.6    | Configuration of VAP with Captive Portal .....                              | 70        |
| 6.3.7    | Advanced VAP settings.....                                                  | 71        |
| 6.4      | Radio configuration .....                                                   | 78        |
| 6.4.1    | Advanced Radio settings .....                                               | 79        |

|          |                                         |           |
|----------|-----------------------------------------|-----------|
| 6.5      | Configuring DHCP option 82 .....        | 81        |
| 6.6      | System settings .....                   | 83        |
| 6.6.1    | Device firmware update.....             | 83        |
| 6.6.2    | Device configuration management.....    | 83        |
| 6.6.3    | Device reboot .....                     | 84        |
| 6.6.4    | Authentication Mode configuration ..... | 84        |
| 6.6.5    | Setting the date and time .....         | 85        |
| 6.6.6    | Advanced system settings .....          | 85        |
| 6.7      | APB service configuration.....          | 87        |
| 6.8      | Monitoring .....                        | 88        |
| 6.8.1    | Wi-Fi clients .....                     | 88        |
| 6.8.2    | Device information .....                | 89        |
| 6.8.3    | Certificate information .....           | 90        |
| 6.8.4    | Network information .....               | 91        |
| 6.8.5    | Wireless interfaces .....               | 92        |
| 6.8.6    | Event logging .....                     | 93        |
| 6.8.7    | Environment scan .....                  | 93        |
| 6.8.8    | Spectrum analyzer .....                 | 94        |
| <b>7</b> | <b>The list of changes .....</b>        | <b>95</b> |



# 1 Introduction

## 1.1 Annotation

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

WOP-30L is a wireless access point. The device design provides a sealed housing, which allows the access point to be used outdoors in various climatic conditions at temperatures from -45 to +65 °C.

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

## 1.2 Symbols

### Notes and warnings

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

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

## 2 Device description

### 2.1 Purpose

WOP-30L wireless access point is designed to provide the user access to high-speed and secure network.

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

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

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

WOP-30L is an indispensable solution for organizing a wireless network in various climatic conditions, in a wide range of operating temperatures and high humidity (parks, factories, stadiums, etc.), and is also an ideal platform for organizing communications in cottage settlements and remote settlements.

### 2.2 Device specification

#### **Interfaces:**

- 1 port of 10/100/1000/2500BASE-T (RJ-45) with PoE+ support;
- Wi-Fi 2.4 GHz IEEE 802.11b/g/n/ax;
- Wi-Fi 5 GHz IEEE 802.11a/n/ac/ax;
- 4 SMA-type connectors (female) for connecting external antennas (Omni, sector, panel, etc.).

#### **Functions:**

##### *WLAN capabilities:*

- support for IEEE 802.11a/b/g/n/ac/ax;
- support for roaming IEEE 802.11r/k/v<sup>1</sup>;
- data aggregation, including A-MPDU (Tx/Rx) and A-MSDU (Rx);
- WMM-based packet priorities and planning;
- dynamic frequency selection (DFS);
- support for hidden SSID;
- 14 virtual access points;
- detection of access points from other vendors;
- spectrum analyzer<sup>1</sup>;
- APSD.

##### *Network features:*

- automatic speed negotiation, duplex mode negotiation and MDI-MDI-X switch-over;
- VLAN support (Access, Trunk, General);
- DHCP client;
- GRE;
- transmission of subscriber traffic outside of tunnels;
- ACL;
- NTP;
- Syslog;
- IPv6.

*QoS functions:*

- packet priorities and planning based on profiles;
- bandwidth limiting for each SSID.

*Security:*

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

<sup>1</sup>Will be fully supported in future releases.

Figure 1 shows WOP-30L application diagram.

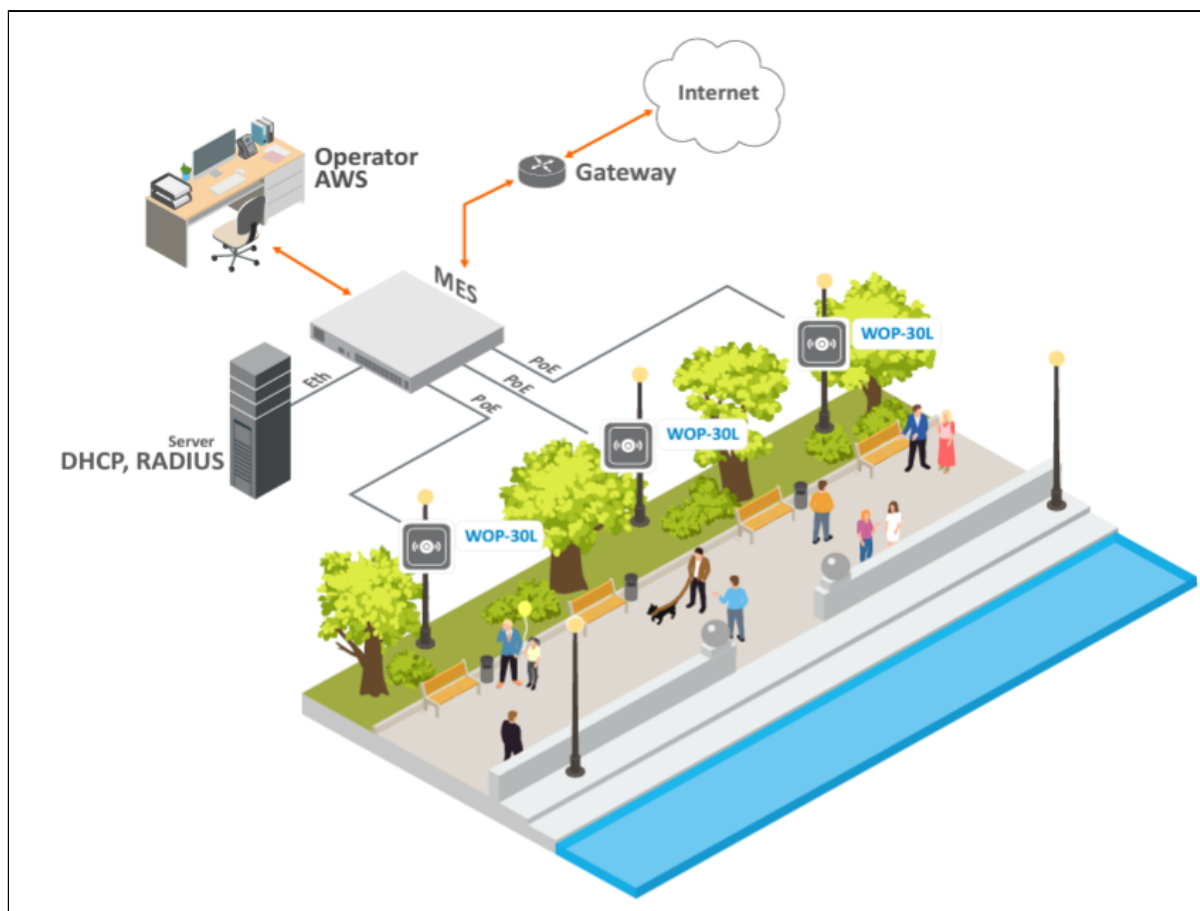


Figure 1 – WOP-30L application diagram

## 2.3 Technical parameters

Table 1 – Main specification

| WAN interface parameters                                           |                                                                                                                                                                                                              |
|--------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Number of ports                                                    | 1                                                                                                                                                                                                            |
| Electrical connector                                               | RJ-45                                                                                                                                                                                                        |
| Data rate                                                          | 10/100/1000/2500 Mbps, auto-negotiation                                                                                                                                                                      |
| Standards                                                          | BASE-T                                                                                                                                                                                                       |
| Wireless interface parameters                                      |                                                                                                                                                                                                              |
| Standards                                                          | 802.11a/b/g/n/ac/ax                                                                                                                                                                                          |
| Frequency range                                                    | 2400–2483.5 MHz; 5150–5350 MHz, 5470–5850 MHz                                                                                                                                                                |
| Modulation                                                         | BPSK, QPSK, 16QAM, 64QAM, 256QAM, 1024QAM                                                                                                                                                                    |
| Operating channels                                                 | 802.11b/g/n/ax: 1–13 (2402–2482 MHz)<br><br>802.11a/n/ac/ax: <ul style="list-style-type: none"> <li>• 36–64 (5170–5330 MHz)</li> <li>• 100–144 (5490–5730 MHz)</li> <li>• 149–165 (5735–5835 MHz)</li> </ul> |
| Data rate                                                          | 2.4 GHz, 802.11ax: 574 Mbps<br>5 GHz, 802.11ax: 1201 Mbps                                                                                                                                                    |
| Maximum number of simultaneous sessions                            | 2.4 GHz: 64<br>5 GHz: 64                                                                                                                                                                                     |
| Maximum output power of the transmitter                            | 2.4 GHz: 20 dBm<br>5 GHz: 20 dBm                                                                                                                                                                             |
| Receiver sensitivity                                               | 2.4 GHz: up to -92 dBm<br>5 GHz: up to -94 dBm                                                                                                                                                               |
| Security                                                           | <ul style="list-style-type: none"> <li>• Centralized authorization via RADIUS server (802.1X WPA/WPA2/WPA3 Enterprise)</li> <li>• WPA/WPA2/WPA3/OWE data encryption</li> <li>• Captive Portal</li> </ul>     |
| The choice of antenna model depends on the use of the access point |                                                                                                                                                                                                              |
| Radio interface with OFDMA and MU-MIMO 2x2 support                 |                                                                                                                                                                                                              |
| Control                                                            |                                                                                                                                                                                                              |
| Remote control                                                     | web interface, Telnet, SSH, CLI, SNMP, NETCONF                                                                                                                                                               |
| Access restriction                                                 | by password, authentication via RADIUS server                                                                                                                                                                |
| General parameters                                                 |                                                                                                                                                                                                              |
| Flash                                                              | 128 MB SPI-NAND Flash                                                                                                                                                                                        |

|                             |                                    |
|-----------------------------|------------------------------------|
| RAM                         | 256 MB DDR3 RAM                    |
| Power supply                | PoE+ 48 V/56 V (IEEE 802.3at-2009) |
| Power consumption           | no more than 15 W                  |
| Ingress protection          | IP55                               |
| Operating temperature range | from -45 to +65 °C                 |
| Relative humidity at 25 °C  | up to 95 %                         |
| Dimensions (W × H × D)      | 125 × 227 × 49 mm                  |
| Weight                      | 0.8 kg                             |
| Service life                | no less than 15 years              |

## 2.4 Design

WOP-30L is made in a plastic case. The layout of WOP-30L panels are shown in Figures 2 and 3.

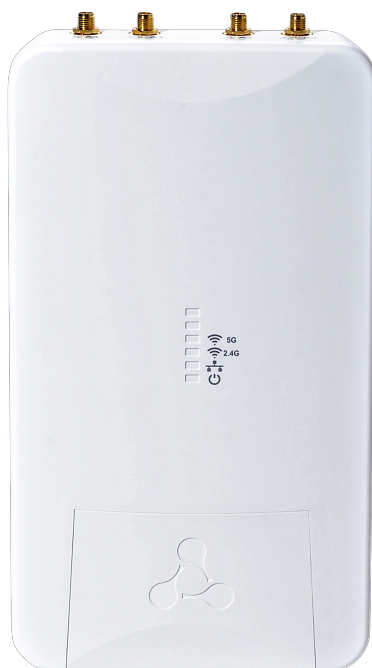


Figure 2 – WOP-30L front panel layout

On the WOP-30L bottom panel (Figure 3) there is a LAN port 10/100/1000/2500 BASE-T (RJ-45 connector) for connecting to the internal network and PoE power, and a factory reset button ("F").



Figure 3 – WOP-30L bottom panel

## 2.5 Light indication

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

Table 2 — Light indication of device status

| LED                                                                                 |                                                                              | LED status                                   | Description                                                                                     |
|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------|----------------------------------------------|-------------------------------------------------------------------------------------------------|
|    | <b>Power</b> — power and device status indicator                             | solid                                        | power connected, normal operation                                                               |
|                                                                                     |                                                                              | flashing                                     | device did not receive an address via DHCP                                                      |
|                                                                                     |                                                                              | flashes quickly for 3 seconds, then stays on | reboot/factory reset                                                                            |
|    | <b>LAN</b> — Ethernet port indicator                                         | solid                                        | channel between WOP-30L Ethernet interface and connected device is active                       |
|                                                                                     |                                                                              | flashing                                     | process of packet data transfer between the WOP-30L Ethernet interface and the connected device |
|  | <b>Wi-Fi 2.4 GHz</b> — wireless network status indicator in the 2.4 GHz band | solid                                        | Wi-Fi network in the 2.4 GHz active                                                             |
|  | <b>Wi-Fi 5 GHz</b> — wireless network status indicator in the 5 GHz band     | solid                                        | Wi-Fi network in the 5 GHz active                                                               |

## 2.6 Restore the default configuration

The device can be reset to the factory configuration using the “F” button on the device. When the device is loaded, press and hold the “F” button (approximately 10–15 seconds) until the Wi-Fi 2.4 and 5 GHz indicators are flashing.

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

## 2.7 Delivery package

The delivery package includes:

- WOP-30L wireless access point;
- mounting kit;
- user manual on a CD (optionally);
- technical passport.

### 3 Rules and recommendations for device installation

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

#### 3.1 Safety rules

1. Do not open the device case. There are no user serviceable parts inside the device.
2. The unused antenna connectors must be covered with a protective cover, which is supplied with the device.
3. Do not install this device during a thunderstorm. There may be a risk of lightning strike.
4. The voltage, current and frequency requirements specified in this manual should be observed.
5. Before connecting measuring instruments and a computer to the device, they should first be grounded. The potential difference between the housings of equipment and measuring instruments should not exceed 1 V.
6. Before turning on the device, make sure the cables are intact and securely attached to the connectors.
7. Do not install the device near heat sources or in rooms with temperatures below -45°C or above 65°C.
8. When installing the device on high-rise structures, the established standards and requirements for work at height should be followed.
9. The device should be operated by engineering and technical personnel who have undergone special training.
10. Only suitable auxiliary equipment should be connected to the device.

#### 3.2 Installation recommendations

 When installed outdoors or in places with high humidity, the device should be installed so that the Ethernet port faces down.

1. The recommended installation position: attaching to a mast/wall.
2. Before installing the device and turning it on, check the device for visible mechanical defects. If defects are observed, stop the device installation, fill in the corresponding act and contact the supplier.
3. When placing the device, in order to provide the best Wi-Fi coverage consider the following rules:
  - Install the device at the center of a wireless network.
  - Minimize the number of barriers (walls, ceilings, furniture, and etc.) between WOP-30L and other wireless network devices.
  - Do not install the device near (about 2 m) electrical and radio devices.
  - It is not recommended to use radiophones and other equipment operating at frequency of 2.4 GHz or 5 GHz, within the range of a Wi-Fi network.
  - Obstacles like glass/metal constructions, brick/concrete walls, water cans and mirrors can significantly reduce Wi-Fi action radius.
4. When installing several access points, cell action radius must overlap with action radius of a neighboring cell at the level from -65 to -70 dBm. It is allowed to reduce the signal level to -75 dBm at cell boundaries, if it is not intended to use VoIP, video streaming and other sensitive to losses traffic in wireless network.



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

The data transmission in the 5 GHz band is used for IEEE 802.11 a/n/ac/ax standards. The WOP-30L device supports frequency channels in the 5 GHz band with a width of 20, 40 and 80 MHz.

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

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

### 3.4 Calculating the number of required access points

When choosing the number of required access points, you should first **evaluate** the required coverage area, taking into account the antenna patterns in the horizontal and vertical planes.

For more accurate assessment, it is necessary to conduct a radio survey of the area. The coverage range of the access point depends on the installed antennas and the presence of obstacles. Table 3 shows approximate attenuation values.

Table 3 – Attenuation values

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

### 3.5 Channel selection for neighboring access points

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

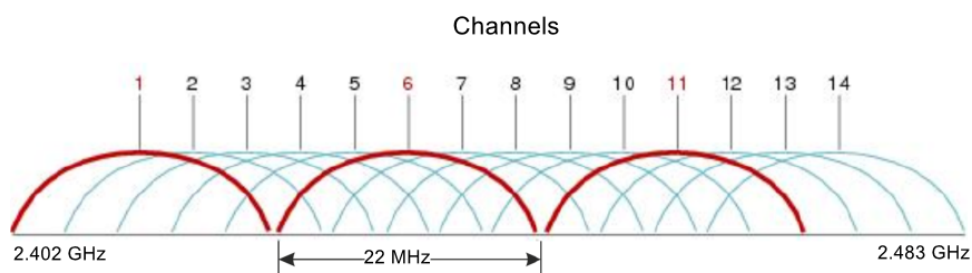


Figure 4 – General diagram of frequency channel overlap in the range of 2.4 GHz

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

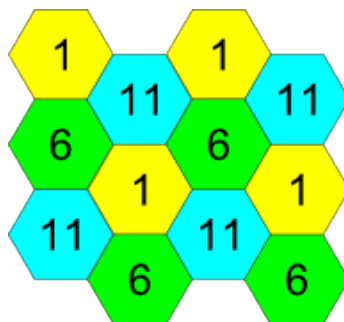


Figure 5 – Scheme of channel allocation among neighboring access points in the frequency range of 2.4 GHz when channel width is 20 MHz

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

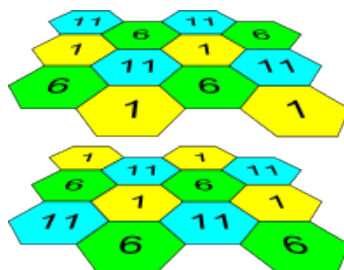


Figure 6 – Scheme of channel allocation between neighboring access points that are located between floors  
With a channel width of 40 MHz there are no non-overlapping channels in the 2.4 GHz band. In such cases, you should select channels maximally separated from each other.

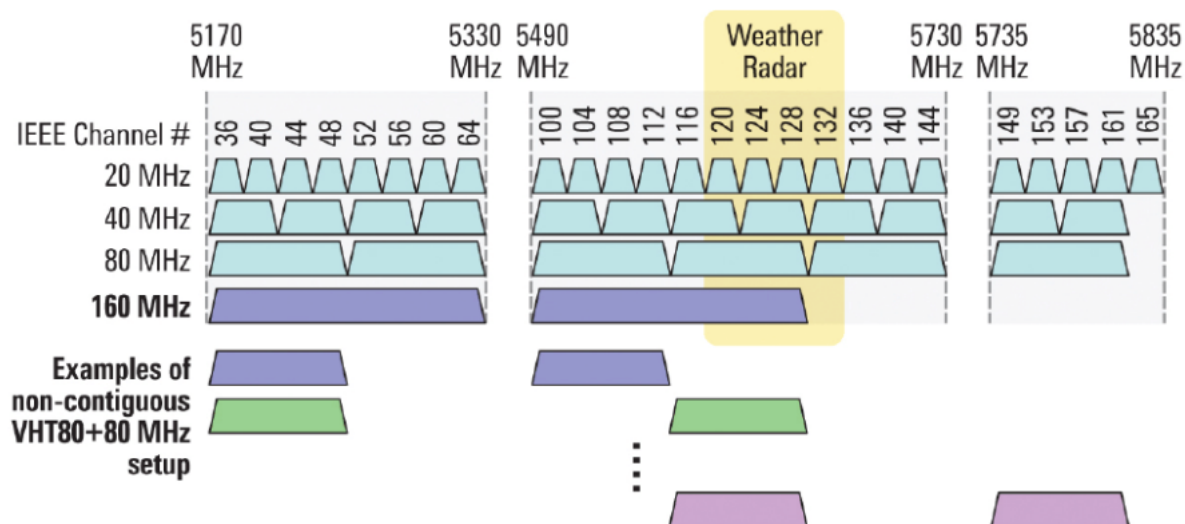


Figure 7 – Channels used in the 5 GHz band when channel width is 20, 40 or 80 MHz

## 4 Installation

There are two mounting options for the WOP-30L access point: it can be installed on a pole and on a wall.

### 4.1 Device installation on a mast/pole

1. Attach the bracket to the device case using the supplied screws as shown in the figure 8.

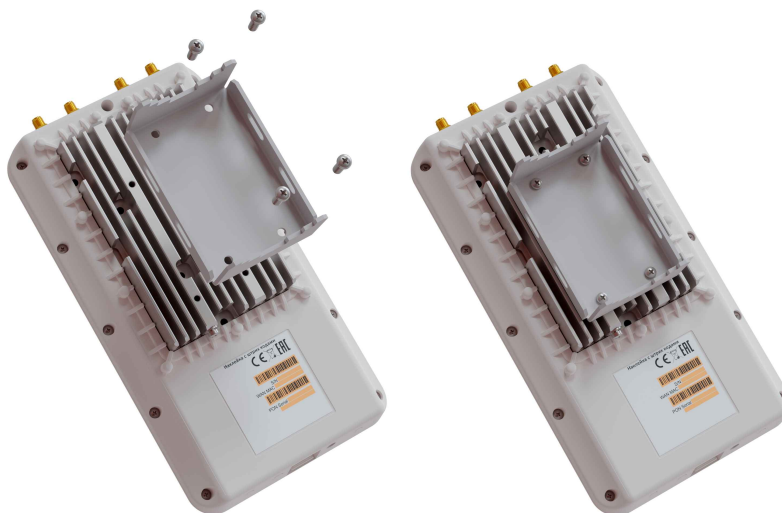


Figure 8 — Attaching the bracket to the device

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



Figure 9 — Attaching the device to the pole

## 4.2 Device installation on a wall

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

1. Align four screw holes on the bracket with the same holes on the device. Using a screwdriver, attach the bracket with screws to the device as shown in the picture 10.

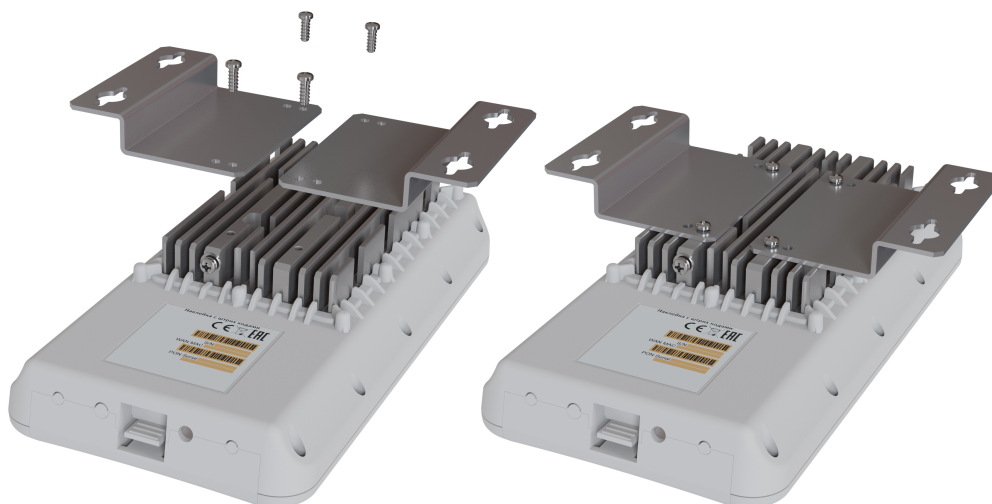


Figure 10 – Attaching the bracket to the device

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



Figure 11 – Placing the device on the wall

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



Figure 12 — Fixing the device to the wall

### 4.3 Connection



Figure 13 – Connecting Ethernet cable to the PoE port

1. Remove the cover protecting the Ethernet port on the bottom of the device, then connect the Ethernet cable to the PoE port (Figure 13).
2. Close the bottom cover.
3. Connect the Ethernet cable from WOP-30L to the injector PoE port or the switch port (IEEE 802.3at-2009).
4. If the PoE injector is used, connect it to a 220V outlet using a power cord.
5. Connect the antenna to the device following the instructions in the [Instructions for sealing antenna connectors](#) section:
  - When using Omni antennas: connect the antennas to the device's SMA connectors;
  - When using panel/sector antennas: connect the antennas to the device's SMA connectors using cable assemblies. Adjust the position of the antenna so that subscriber units are within the coverage area of the installed antenna.

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

### 4.3.1 Instructions for sealing antenna connectors

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

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



Figure 14a



Figure 14b

2. Connect the cable to the device connector (antenna) and tighten the nut as shown in Figure 15 (a, b).



Figure 15a



Figure 15b

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

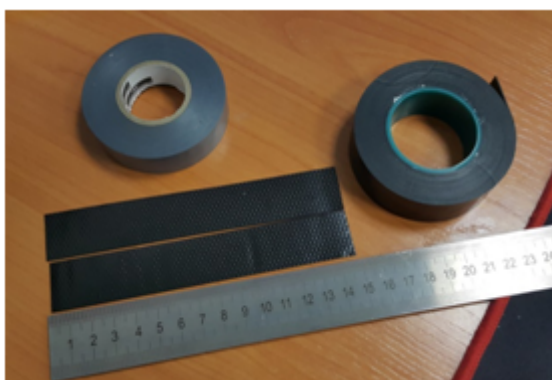


Figure 16a

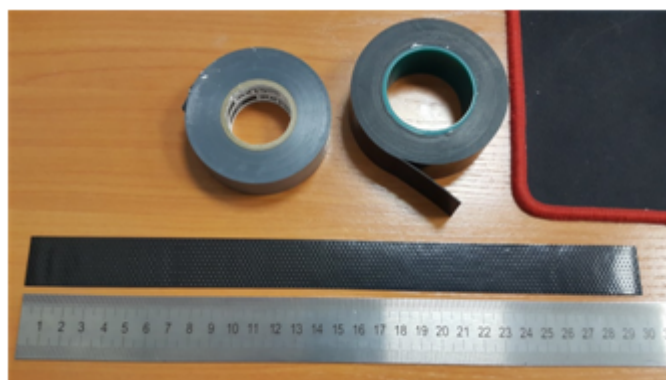


Figure 16b



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



Figure 17

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



Figure 18a



Figure 18b

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



Figure 19a



Figure 19b



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

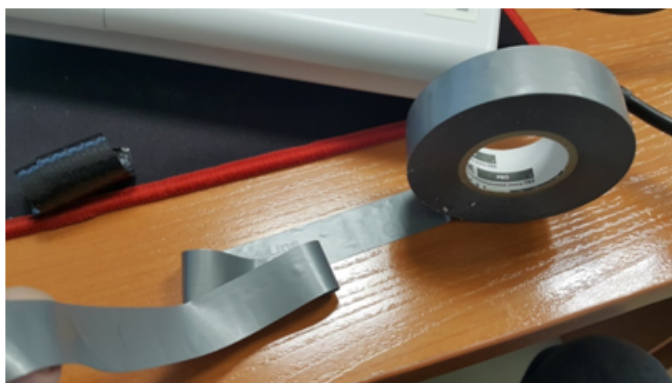


Figure 20

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



Figure 21

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



Figure 22a



Figure 22b

10. Check the sealed connector for visible rubber tape.

## 5 Device management via the web interface

### 5.1 Getting started

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

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

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

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

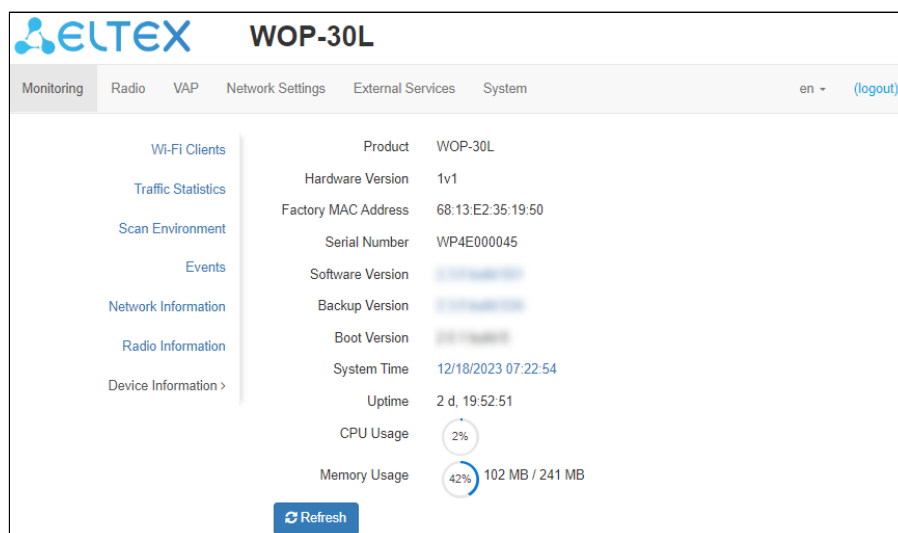


The image shows the login page for the WOP-30L device. It features a white background with a light gray border. At the top center, the text "WOP-30L" is displayed in a bold, black, sans-serif font. Below this, there is a white rectangular box containing two input fields. The first field is labeled "Enter login" and the second is labeled "Enter password". Both fields have a light gray border and a small icon of a person and a key respectively. Below the input fields is a blue button with a white checkmark icon and the text "Log In".

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

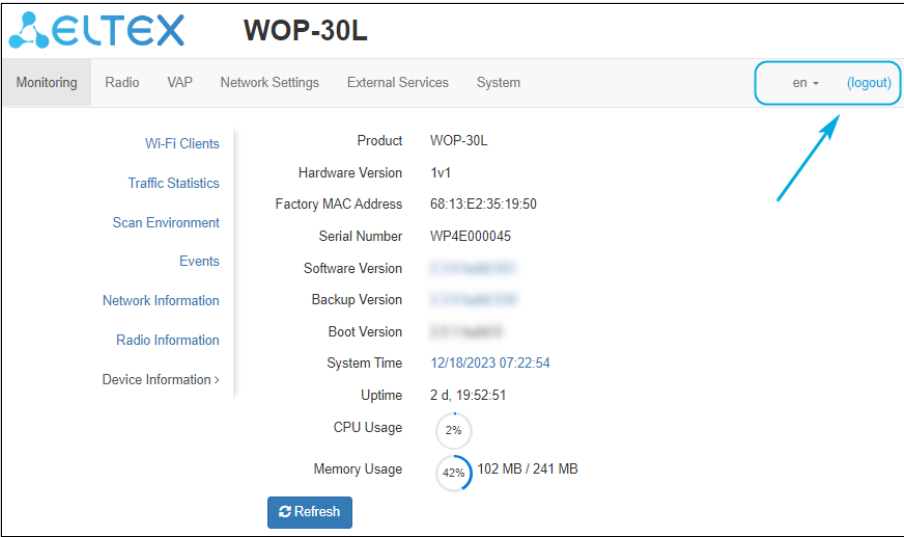
- ✓ Factory settings: login — *admin*, password — *password*.

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



The image shows the monitoring dashboard for the WOP-30L device. The dashboard has a white background with a light gray border. At the top left, the ELTEX logo is displayed. To the right of the logo, the text "WOP-30L" is displayed in a bold, black, sans-serif font. Below the logo and title, there is a horizontal navigation bar with tabs: "Monitoring", "Radio", "VAP", "Network Settings", "External Services", and "System". The "Monitoring" tab is currently selected. To the right of the navigation bar, there is a language selector "en" and a "logout" link. The main content area is divided into two columns. The left column contains a sidebar with links: "Wi-Fi Clients", "Traffic Statistics", "Scan Environment", "Events", "Network Information", "Radio Information", and "Device Information >". The right column contains a table of device information. The table has two columns: "Parameter" and "Value". The parameters and their values are: Product (WOP-30L), Hardware Version (1v1), Factory MAC Address (68:13:E2:35:19:50), Serial Number (WP4E000045), Software Version (1.0.0.0), Backup Version (1.0.0.0), Boot Version (1.0.0.0), System Time (12/18/2023 07:22:54), Uptime (2 d, 19:52:51), CPU Usage (2%), and Memory Usage (42% / 102 MB / 241 MB). At the bottom of the table, there is a blue button with a white refresh icon and the text "Refresh".

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



5.2 Applying configuration and discarding changes

1. Applying configuration



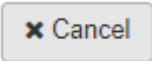
Clicking  starts the process of saving the configuration to the device flash memory and applying the new settings. All the settings come into operation without device rebooting.

The WOP-30L web interface has a visual indication of the current status of the setting applying process (Table 4).

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

| Image                                                                               | State description                                                                                                                                                                                                                                                                        |
|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|   | Clicking “Apply” starts the process of saving the configuration to the device flash memory and applying the new settings. This is indicated by the  icon in the tab name and on the “Apply” button. |
|  | The  icon in the tab name indicates about successful saving and application of the settings.                                                                                                          |

2. Discarding changes

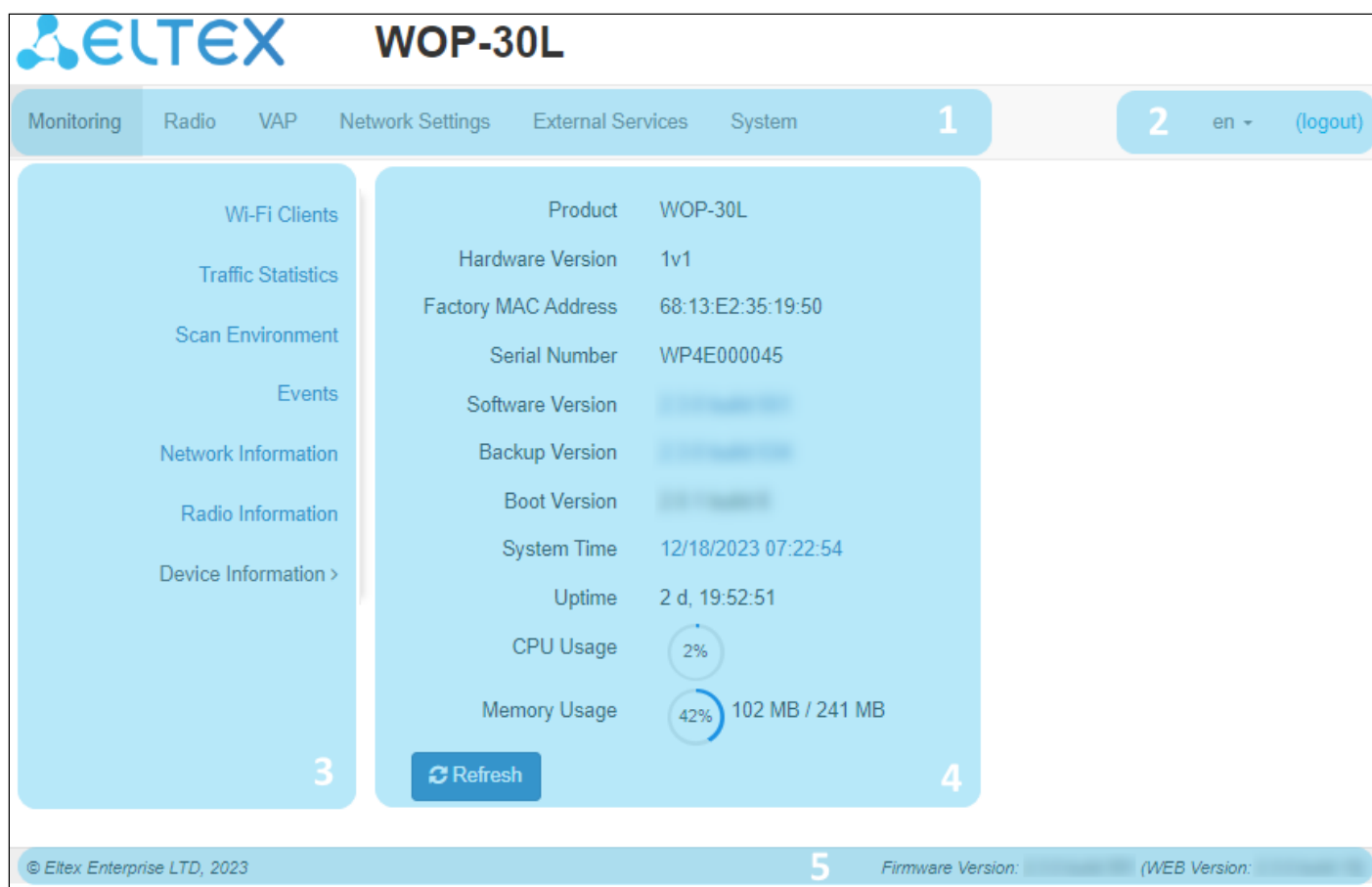


The button for discarding changes appears as follows: .

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

### 5.3 Web interface basic elements

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



User interface window is divided into five general areas:

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

## 5.4 The “Monitoring” menu

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

### 5.4.1 The “Wi-Fi Clients” submenu

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

The screenshot shows the ELTEX WOP-30L web interface. The top navigation bar includes links for Monitoring, Radio, VAP, Network Settings, External Services, and System. The left sidebar lists various monitoring options, with 'Wi-Fi Clients' selected. A 'Refresh' button is present. The main content area displays a table of connected clients and associated statistics.

| # | Hostname | IP Address  | MAC               | Interface | Link Quality | Link Quality Common | RSSI, dBm | SNR, dB | TxRate                | RxRate                 | TX BW, MHz | RX BW, MHz | Uptime   |
|---|----------|-------------|-------------------|-----------|--------------|---------------------|-----------|---------|-----------------------|------------------------|------------|------------|----------|
| 1 |          | 10.24.80.54 | 22:08:bf:a4:2d:0a | wlan1-va0 | 84           | 86                  | -30       | 33      | HE NSS2 MCS8<br>864.7 | HE NSS1 MCS10<br>540.4 | 80         | 80         | 00:00:54 |

|                        |                 |                           |       |
|------------------------|-----------------|---------------------------|-------|
| Total TX / RX, bytes   | 24 215 / 34 742 | Fails, packets            | 0     |
| Total TX / RX, packets | 130 / 162       | TX Period Retry, packets  | 1     |
| Data TX / RX, bytes    | 23 881 / 34 610 | TX Retry Count, packets   | 20    |
| Data TX / RX, packets  | 125 / 158       | Actual TX / RX Rate, kbps | 0 / 0 |

| Rate       | TX Packets |     | RX Packets |     |
|------------|------------|-----|------------|-----|
| NSS1-MCS7  | 0          | 0%  | 2          | 1%  |
| NSS1-MCS8  | 0          | 0%  | 34         | 22% |
| NSS1-MCS9  | 0          | 0%  | 33         | 21% |
| NSS1-MCS10 | 0          | 0%  | 8          | 5%  |
| NSS2-MCS2  | 0          | 0%  | 1          | 1%  |
| NSS2-MCS3  | 0          | 0%  | 3          | 2%  |
| NSS2-MCS4  | 1          | 1%  | 48         | 30% |
| NSS2-MCS5  | 6          | 5%  | 19         | 12% |
| NSS2-MCS6  | 53         | 42% | 5          | 3%  |
| NSS2-MCS7  | 23         | 18% | 5          | 3%  |
| NSS2-MCS8  | 34         | 27% | 0          | 0%  |
| NSS2-MCS9  | 8          | 6%  | 0          | 0%  |

- *No* – number of the connected device in the list;
- *Hostname* – network name of the device;
- *IP address* – IP address of the connected device;
- *MAC address* – MAC address of the connected device;
- *Interface* – WOP-30L interaction interface with the connected device;
- *Link Quality* – parameter that displays the status of the link to the client, calculated based on the number of retransmit packets sent to the client. The maximum value is 100% (all transmitted packets were sent on the first attempt), the minimum value is 0% (no packets were successfully sent to the client). The parameter value is calculated for the last 10 s;
- *Link Quality Common* – parameter that displays the status of the link to the client, calculated based on the number of retransmit packets sent to the client. The maximum value is 100% (all transmitted packets were sent on the first attempt), the minimum value is 0% (no packets were successfully sent to the client). The parameter value is calculated for the entire client connection time;
- *RSSI* – received signal level, dBm;
- *SNR* – signal/noise ratio, dB;
- *TxRate* – channel data rate of transmission, Mbps;

- *RxRate* – channel data rate of receiving, Mbps;
- *Tx BW* – transmission bandwidth, MHz;
- *Rx BW* – reception bandwidth, MHz;
- *Uptime* – Wi-Fi client connection time.

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

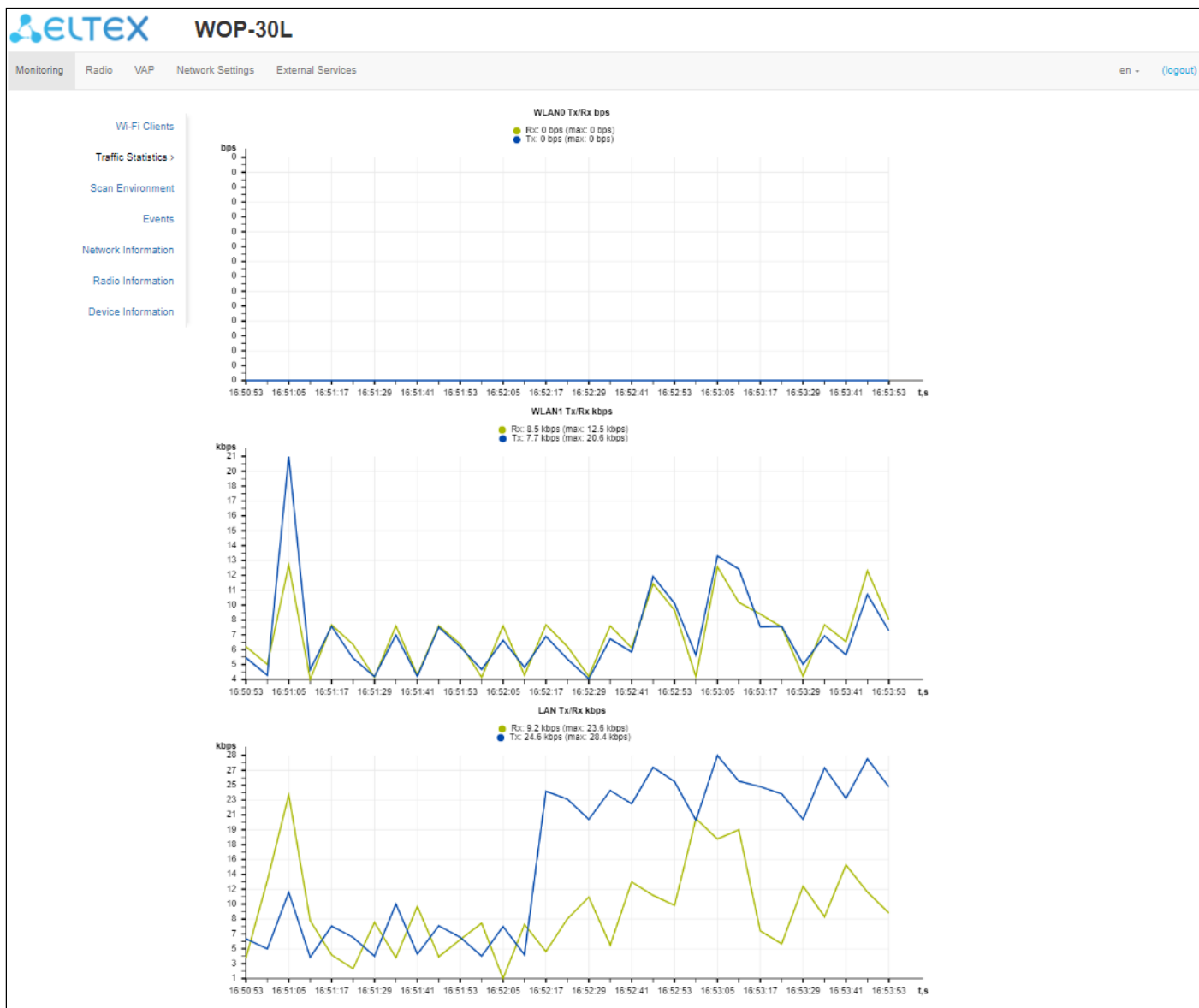
- *Total TX/RX, bytes* – number of bytes sent/received on the connected device;
- *Total TX/RX, packets* – number of packets sent/received on the connected device;
- *Data TX/RX, bytes* – number of bytes sent/received on the connected device;
- *Data TX/RX, packets* – number of packets sent/received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

### 5.4.2 The “Traffic Statistics” submenu

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

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

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



“Transmit” table description:

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

| Transmit ▾ |               |             |            |        |
|------------|---------------|-------------|------------|--------|
| Interface  | Total Packets | Total Bytes | Total Drop | Errors |
| LAN        | 5502          | 4585766     | 0          | 0      |
| WLAN0      | 0             | 0           | 0          | 0      |
| WLAN1      | 1648          | 243911      | 0          | 0      |
| wlan0-va0  | 0             | 0           | 0          | 0      |
| wlan0-va1  | 0             | 0           | 0          | 0      |
| wlan0-va2  | 0             | 0           | 0          | 0      |
| wlan0-va3  | 0             | 0           | 0          | 0      |
| wlan0-va4  | 0             | 0           | 0          | 0      |

“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       | 1357167       | 157190595   | 0          | 0      |
| WLAN0     | 0             | 0           | 0          | 0      |
| WLAN1     | 830           | 136492      | 0          | 0      |
| wlan0-va0 | 0             | 0           | 0          | 0      |
| wlan0-va1 | 0             | 0           | 0          | 0      |
| wlan0-va2 | 0             | 0           | 0          | 0      |
| wlan0-va3 | 0             | 0           | 0          | 0      |
| wlan0-va4 | 0             | 0           | 0          | 0      |



### 5.4.3 The “Scan Environment” submenu

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

| Range   | SSID      | Security Mode | MAC               | Channel / Bandwidth | RSSI, dBm |
|---------|-----------|---------------|-------------------|---------------------|-----------|
| 2.4 GHz | [blurred] | WPA/WPA2      | A8:F9:4B:3F:4F:21 | 1/20                | -37       |
| 2.4 GHz | [blurred] | Open          | E8:28:C1:DA:E8:21 | 1/20                | -37       |
| 2.4 GHz | [blurred] | Open          | E8:28:C1:DA:E8:20 | 1/20                | -37       |
| 2.4 GHz | [blurred] | Open          | E0:D9:E3:49:D5:00 | 1/20                | -42       |
| 2.4 GHz | [blurred] | Open          | E8:28:C1:FC:D9:04 | 1/20                | -45       |
| 2.4 GHz | [blurred] | WPA/WPA2      | 68:13:E2:0F:D1:F3 | 1/20                | -82       |
| 2.4 GHz | [blurred] | WPA/WPA2      | 68:13:E2:0F:D1:F6 | 1/20                | -83       |
| 2.4 GHz | [blurred] | WPA2_1X       | 68:13:E2:0F:D1:F1 | 1/20                | -84       |
| 2.4 GHz | [blurred] | WPA2_1X       | 68:13:E2:0F:D1:F2 | 1/20                | -84       |
| 2.4 GHz | [blurred] | WPA2_1X       | E0:D9:E3:70:94:10 | 6/20                | -85       |

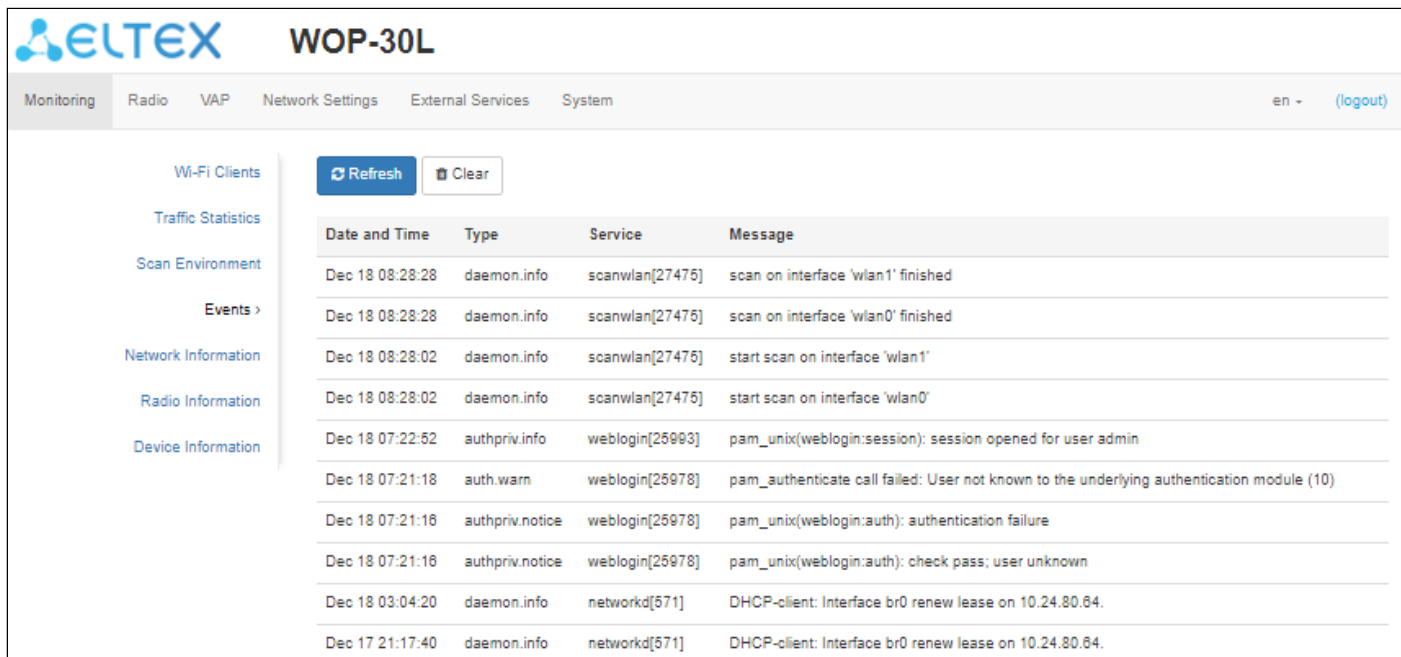
After clicking on the “Scan” button, the process will be launched. After the scan is completed, a list of detected access points and information about them will appear:

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

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

#### 5.4.4 The “Events” submenu

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



| Date and Time   | Type            | Service         | Message                                                                                   |
|-----------------|-----------------|-----------------|-------------------------------------------------------------------------------------------|
| Dec 18 08:28:28 | daemon.info     | scanwlan[27475] | scan on interface 'wlan1' finished                                                        |
| Dec 18 08:28:28 | daemon.info     | scanwlan[27475] | scan on interface 'wlan0' finished                                                        |
| Dec 18 08:28:02 | daemon.info     | scanwlan[27475] | start scan on interface 'wlan1'                                                           |
| Dec 18 08:28:02 | daemon.info     | scanwlan[27475] | start scan on interface 'wlan0'                                                           |
| Dec 18 07:22:52 | authpriv.info   | weblogin[25993] | pam_unix(weblogin:session): session opened for user admin                                 |
| Dec 18 07:21:18 | auth.warn       | weblogin[25978] | pam_authenticate call failed: User not known to the underlying authentication module (10) |
| Dec 18 07:21:16 | authpriv.notice | weblogin[25978] | pam_unix(weblogin:auth): authentication failure                                           |
| Dec 18 07:21:16 | authpriv.notice | weblogin[25978] | pam_unix(weblogin:auth): check pass; user unknown                                         |
| Dec 18 03:04:20 | daemon.info     | networkd[571]   | DHCP-client: Interface br0 renew lease on 10.24.80.64.                                    |
| Dec 17 21:17:40 | daemon.info     | networkd[571]   | DHCP-client: Interface br0 renew lease on 10.24.80.64.                                    |

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

Table 5 — Description of event severity levels

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

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

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

### 5.4.5 The “Network Information” submenu

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

**ELTEX WOP-30L**

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

Wi-Fi Clients  
Traffic Statistics  
Scan Environment  
Events  
Network Information >  
Radio Information  
Device Information

**WAN Status**

|            |                              |
|------------|------------------------------|
| Interface  | br0                          |
| Protocol   | DHCP                         |
| IP Address | 10.24.80.64                  |
| RX Bytes   | 138.8 MB (143 407 195 bytes) |
| TX Bytes   | 2.5 MB (2 617 481 bytes)     |

**Ethernet**

|             |      |
|-------------|------|
| Link Status | Up   |
| Speed       | 100  |
| Duplex      | Full |

**ARP** ▾

| # | IP Address  | MAC               |
|---|-------------|-------------------|
| 0 | 10.24.80.50 | 18:C0:4D:C8:0A:DB |
| 1 | 10.24.80.26 | D8:5E:D3:60:AD:F4 |
| 2 | 10.24.80.1  | E0:D9:E3:E8:E1:40 |

**Routes** ▾

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

#### WAN Status:

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

#### Ethernet:

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

#### ARP:

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

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

Routes:

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

The following flag values exist:

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

### 5.4.6 The “Radio Information” submenu

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

|                                                                                                 |                                                                   |
|-------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
|  <b>WOP-30L</b> |                                                                   |
| Monitoring                                                                                      | Radio VAP Network Settings External Services System en + (logout) |
| Wi-Fi Clients                                                                                   | Radio 2.4 GHz                                                     |
| Traffic Statistics                                                                              | Status Off                                                        |
| Scan Environment                                                                                | MAC 68:13:E2:35:19:50                                             |
| Events                                                                                          | Mode IEEE 802.11b/g/n/ax                                          |
| Network Information                                                                             | Radio 5 GHz                                                       |
| Radio Information >                                                                             | Status Off                                                        |
| Device Information                                                                              | MAC 68:13:E2:35:19:58                                             |
|                                                                                                 | Mode IEEE 802.11a/n/ac/ax                                         |

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

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

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

#### “Off”:

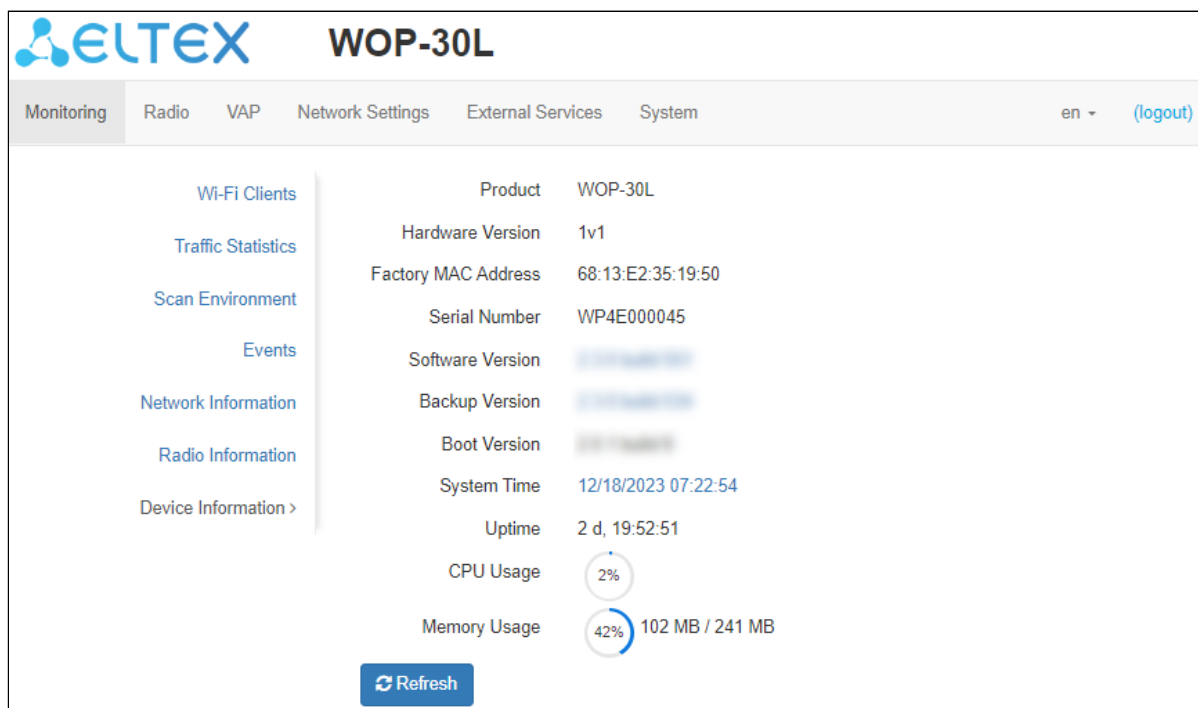
- *Status* — radio interface state;
- *MAC* — radio interface MAC address;
- *Mode* — radio interface operation mode according to IEEE 802.11 standards.

#### “On”:

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

### 5.4.7 The “Device Information” submenu

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



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

## 5.5 The “Radio” menu

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

### 5.5.1 The “Radio 2.4 GHz” submenu

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

The screenshot shows the ELTEX WOP-30L web interface. The top navigation bar includes 'Monitoring', 'Radio', 'VAP', 'Network Settings', 'External Services', and 'System'. The 'Radio' menu is active. On the left, there is a sidebar with 'Radio 2.4 GHz >', 'Radio 5 GHz', and 'Advanced'. The main content area is titled 'Common' and contains the following settings:

- Mode:** A dropdown menu set to 'IEEE 802.11b/g/n/ax'.
- Auto Channel:** A checkbox that is checked.
- Use Limit Channels:** A checkbox that is checked.
- Channel List:** A list of channels with their frequency ranges and a delete icon (X):
  - 1 (2402 — 2442 MHz) X
  - 6 (2427 — 2467 MHz) X
  - 11 (2432 — 2472 MHz) X
- Channel Bandwidth, MHz:** A dropdown menu set to '40'.
- Primary Channel:** A dropdown menu set to 'Lower'.
- Transmit Power Limit, dBm:** A dropdown menu set to '16'.

At the bottom of the 'Common' section, there is an 'Advanced' link with a dropdown arrow. Below the settings are 'Apply' and 'Cancel' buttons.

- **Mode** — interface operation mode according to the following standards:
  - IEEE 802.11ax;
  - IEEE 802.11n/ax;
  - IEEE 802.11b/g;
  - IEEE 802.11b/g/n;
  - IEEE 802.11b/g/n/ax.
- **Auto Channel** — when checked, the device will automatically select the least congested radio channel for the Wi-Fi interface. Unchecking the flag opens the access to install the static operation channel;
- **Channel** — select channel for data transmission;
- **Use Limit Channels** — when checked, the access point will use a user-defined list of channels to work in automatic channel selection mode. If the “Use Limit channels” flag is not checked or there are no channels in the list, the access point will select the operation channel from all available channels in the given band. 2.4 GHz band channels: 1–13;
- **Channel Bandwidth, MHz** — channel bandwidth, on which the access point operates. The parameter may take values 20 and 40 MHz;
- **Primary Channel** — the parameter can only be changed if the bandwidth of a statically specified channel is equal to 40 MHz. The 40 MHz channel can be considered as consisting of two 20 MHz channels, which border in the frequency range. These two 20 MHz channels are called primary and secondary channels. The primary channel is used by clients who only support 20 MHz channel bandwidth:
  - **Upper** — the primary channel will be the upper 20 MHz channel in the 40 MHz band;
  - **Lower** — the primary channel will be the lower 20 MHz channel in the 40 MHz band.
- **Transmit Power Limit, dB** — adjustment of the signal strength of the Wi-Fi transmitter in dBm. Accepts value from 0 to 16 dBm.

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

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

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

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

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

Advanced ▾

|                                        |                                     |
|----------------------------------------|-------------------------------------|
| OBSS Coexistence                       | <input checked="" type="checkbox"/> |
| Fixed Transmit Rate                    | Auto ▾                              |
| Short Guard Interval                   | <input checked="" type="checkbox"/> |
| STBC                                   | <input type="checkbox"/>            |
| Beacon Interval, ms                    | 100                                 |
| Fragmentation Threshold                | 2346                                |
| RTS Threshold                          | 2347                                |
| Frame Aggregation                      | <input checked="" type="checkbox"/> |
| Short Preamble                         | <input checked="" type="checkbox"/> |
| Broadcast/Multicast Rate Limiting, p/s | <input type="checkbox"/>            |
| Wi-Fi Multimedia (WMM)                 | <input checked="" type="checkbox"/> |
| DHCP Snooping Mode                     | ignore ▾                            |
| Enable QoS                             | <input type="checkbox"/>            |

✓ Apply ✕ Cancel

- *OBSS Coexistence* — automatic channel bandwidth reduction when the channel is loaded. When the flag is set, the mode is enabled;
- *Fixed Transmit Rate* — fixed wireless data transfer rate, defined by IEEE 802.11 standards specifications;
- *Short Guard Interval* — support for Short Guard Interval. Access point transmits data using 400 ns guard interval (instead of 800 ns) to clients which also support Short Guard Interval;
- *STBC* — Space-Time Block Coding method dedicated to improve data transmission reliability. The field is only available if the selected operating mode includes 802.11n. When checked, the device transmits one data flow through several antennas. When unchecked, the device does not transmit the same data flow through several antennas;
- *Beacon Interval, ms* — beacon frames transmission period. The frames are sent to detect access points on the air. The parameter takes values from 20 to 2000 ms, by default: 100 ms;
- *Fragmentation Threshold* — frame fragmentation threshold, bytes. The parameter takes values 256–2346, by default: 2346;



- *RTS Threshold* – specifies the number of bytes over which the Request to Send will be sent. Decreasing this value may improve the performance of the access point when there are a lot of connected clients. However this reduces general throughput of wireless network. The parameter takes values from 0 to 2347, by default: 2347;
- *Frame aggregation* – enable support for AMPDU/AMSDU;
- *Short Preamble* – use of the packet short preamble;
- *Broadcast/Multicast Rate Limiting, p/s* – when the flag is set, transmission of broadcast / multicast traffic over the wireless network is restricted. Specify the limit for broadcast traffic in the popup window (p/s);
- *Wi-Fi Multimedia (WMM)* – WMM support activation (Wi-Fi Multimedia);
- *DHCP Snooping Mode*<sup>1</sup> – selection of DHCP option 82 processing policy. Available values for selection:
  - *ignore* – option 82 processing is disabled. Default value;
  - *remove* – access point deletes the value of option 82;
  - *replace* – access point substitutes or replaces the value of option 82. When selecting this value to edit, the following parameters are opened:
    - *Option 82 CID format* – replacement of the CID parameter value, can take values:
      - *APMAC-SSID* – replacement of the CID parameter value to <MAC address of the access point>-<SSID name>. Default value;
      - *SSID* – replacement of the CID parameter value to SSID name, to which the client is connected;
      - *custom* – replacement of the CID parameter value to the value specified in the "Option 82 Unique CID";
        - *Option 82 Unique CID* – an arbitrary string of up to 52 characters that will be passed to the CID. If the parameter value is not set, the point will change the CID to the default value – APMAC-SSID.
    - *Option 82 RID format* – replacement of the RID parameter value, can take the following values:
      - *ClientMAC* – change the RID content to the MAC address of the client device. Default value;
      - *APMAC* – change the RID content to the MAC address of the access point;
      - *APdomain* – change the RID content to the domain in which the access point is located;
      - *custom* – change the RID content to the value specified in the "Option 82 Unique RID";
        - *Option 82 Unique RID* – an arbitrary string of up to 63 characters that will be passed to the RID. If the parameter value is not set, the point will change the RID to the default value – ClientMAC.
  - *MAC-address format* – selection of octet delimiters of the MAC address, which is transmitted in CID and RID:
    - *AA:BB:CC:DD:EE:FF* – the delimiter is a colon (:). Default value;
    - *AA-BB-CC-DD-EE-FF* – the delimiter is a dash (-).
- *Enable QoS* – when the flag is set, the setting of Quality of Service functions is available.

---

<sup>1</sup> Full functionality support is planned for future releases.

The following functions are available for quality assurance configuration:

| AP EDCA Parameters   |                                |                                   |                                     |                                 |
|----------------------|--------------------------------|-----------------------------------|-------------------------------------|---------------------------------|
| Queue                | AIFS                           | cwMin                             | cwMax                               | TXOP Limit                      |
| Data 3 (Background)  | <input type="text" value="7"/> | <input type="text" value="15"/> ▼ | <input type="text" value="1023"/> ▼ | <input type="text" value="0"/>  |
| Data 2 (Best Effort) | <input type="text" value="3"/> | <input type="text" value="15"/> ▼ | <input type="text" value="83"/> ▼   | <input type="text" value="0"/>  |
| Data 1 (Video)       | <input type="text" value="1"/> | <input type="text" value="7"/> ▼  | <input type="text" value="15"/> ▼   | <input type="text" value="94"/> |
| Data 0 (Voice)       | <input type="text" value="1"/> | <input type="text" value="3"/> ▼  | <input type="text" value="7"/> ▼    | <input type="text" value="47"/> |

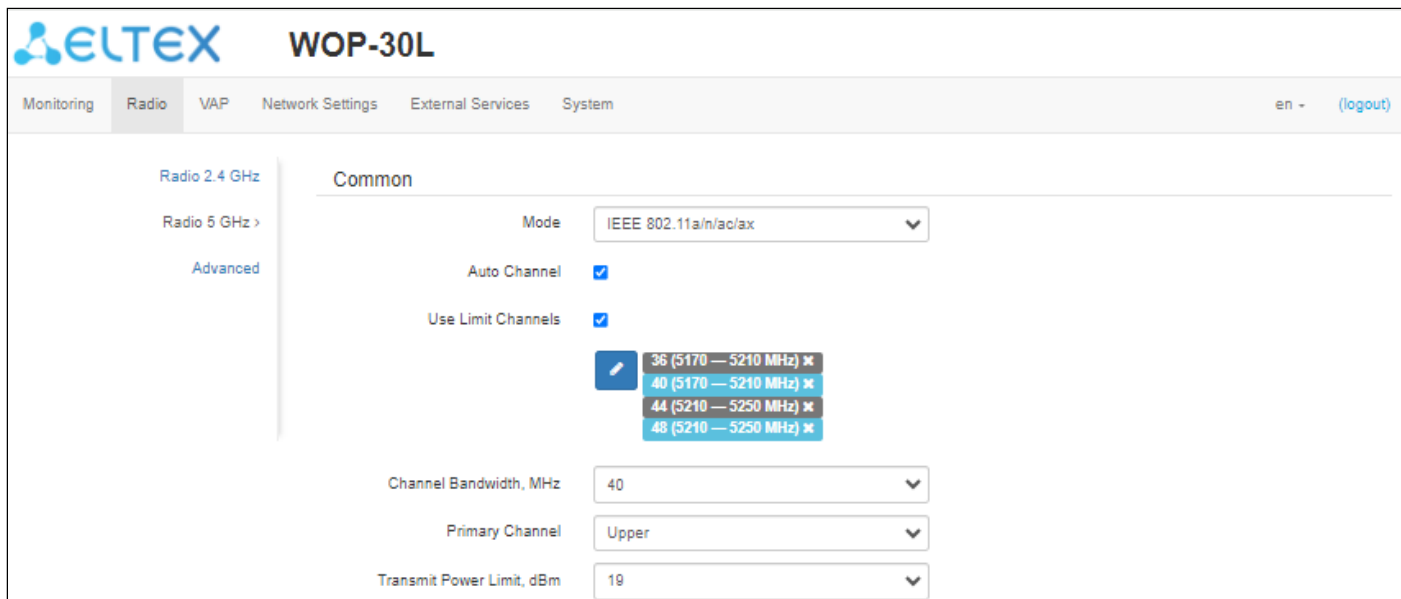
| Station EDCA Parameters |                                |                                   |                                     |                                 |
|-------------------------|--------------------------------|-----------------------------------|-------------------------------------|---------------------------------|
| Queue                   | AIFS                           | cwMin                             | cwMax                               | TXOP Limit                      |
| Data 3 (Background)     | <input type="text" value="7"/> | <input type="text" value="15"/> ▼ | <input type="text" value="1023"/> ▼ | <input type="text" value="0"/>  |
| Data 2 (Best Effort)    | <input type="text" value="3"/> | <input type="text" value="15"/> ▼ | <input type="text" value="1023"/> ▼ | <input type="text" value="0"/>  |
| Data 1 (Video)          | <input type="text" value="2"/> | <input type="text" value="7"/> ▼  | <input type="text" value="15"/> ▼   | <input type="text" value="94"/> |
| Data 0 (Voice)          | <input type="text" value="2"/> | <input type="text" value="3"/> ▼  | <input type="text" value="7"/> ▼    | <input type="text" value="47"/> |

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

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

### 5.5.2 The “Radio 5 GHz” submenu

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



The screenshot shows the ELTEX WOP-30L web interface. The top navigation bar includes 'Monitoring', 'Radio', 'VAP', 'Network Settings', 'External Services', and 'System'. The 'Radio' tab is selected. On the left, there is a sidebar with 'Radio 2.4 GHz', 'Radio 5 GHz >', and 'Advanced'. The 'Radio 5 GHz >' option is selected, leading to the 'Common' configuration page. The settings on this page are as follows:

- Mode:** A dropdown menu set to 'IEEE 802.11a/n/ac/ax'.
- Auto Channel:** A checkbox that is checked.
- Use Limit Channels:** A checkbox that is checked.
- Channel List:** A list of four channels, each with a delete icon (X):
  - 36 (5170 — 5210 MHz)
  - 40 (5170 — 5210 MHz)
  - 44 (5210 — 5250 MHz)
  - 48 (5210 — 5250 MHz)
- Channel Bandwidth, MHz:** A dropdown menu set to '40'.
- Primary Channel:** A dropdown menu set to 'Upper'.
- Transmit Power Limit, dBm:** A dropdown menu set to '19'.

- **Mode** — select interface operation mode according to the following standards:
  - IEEE 802.11ax;
  - IEEE 802.11a/n/ac;
  - IEEE 802.11a/n/ac/ax.
- **Auto Channel** — when checked, the device will automatically select the least congested radio channel for the Wi-Fi interface. Removing the flag opens the access to install the static operation channel;
- **Channel** — select channel for data transmission;
- **Use Limit Channels** — when checked, the access point will use a user-defined list of channels to work in automatic channel selection mode. If the “Use Limit channels” flag is not checked or there are no channels in the list, the access point will select the operation channel from all available channels in the given band. 5 GHz band channels: 36–64, 132–144, 149–165;
- **Channel Bandwidth, MHz** — channel bandwidth, on which the access point operates. The parameter may take values of 20, 40 and 80 MHz;
- **Primary Channel** — the parameter can only be changed if the bandwidth of a statically specified channel is equal to 40 MHz. The 40 MHz channel can be considered as consisting of two 20 MHz channels, which border in the frequency range. These two 20 MHz channels are called primary and secondary channels. The primary channel is used by clients who only support 20 MHz channel bandwidth:
  - **Upper** — the primary channel will be the upper 20 MHz channel in the 40 MHz band;
  - **Lower** — the primary channel will be the lower 20 MHz channel in the 40 MHz band.
- **Transmission Power Limit, dBm** — transmitting Wi-Fi signal power adjustment, dBm. May take values between 0 and 19 dBm.

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

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

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

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

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

Advanced ▾

OBSS Coexistence ☒

Fixed Transmit Rate Auto ▾

DFS Support Enabled ▾

Short Guard Interval ☒

STBC ☐

Beacon Interval, ms 100

Fragmentation Threshold 2346

RTS Threshold 2347

Frame Aggregation ☒

Short Preamble ☒

Broadcast/Multicast Rate Limiting, p/s ☐

Wi-Fi Multimedia (WMM) ☒

DHCP Snooping Mode ignore ▾

Enable QoS ☐

✓ Apply ✕ Cancel

- *OBSS Coexistence* — automatic channel bandwidth reduction when the channel is loaded. When the flag is set, the mode is enabled;
- *Fixed Transmit Rate* — fixed wireless data transfer rate, defined by IEEE 802.11 standards specifications;
- *DFS Support* — dynamic frequency selection mechanism. The mechanism demands wireless devices to scan environment and avoid using channels which coincide with radiolocation system's channels at 5 GHz:
  - *Disabled* — the mechanism is disabled. DFS channels are not available for selection;
  - *Enabled* — the mechanism is enabled;
  - *Forced* — the mechanism is disabled. DFS channels are available for selection.
- *Short Guard Interval* — support for Short Guard Interval. Access point transmits data using 400 ns guard interval (instead of 800 ns) to clients which also support Short Guard Interval;

- *STBC* — Space-Time Block Coding method dedicated to improve data transmission reliability. The field is only available if the selected operating mode includes 802.11n. When checked, the device transmits one data flow through several antennas. When unchecked, the device does not transmit the same data flow through several antennas;
- *Beacon Interval, ms* — beacon frames transmission period. The frames are sent to detect access points. The parameter takes values from 20 to 2000 ms, by default: 100 ms;
- *Fragmentation Threshold* — frame fragmentation threshold, bytes. The parameter takes values 256–2346, by default: 2346;
- *RTS Threshold* — specifies the number of bytes over which the Request to Send will be sent. Decreasing this value may improve the performance of the access point when there are a lot of connected clients. However this reduces general throughput of wireless network. The parameter takes values from 0 to 2347, by default: 2347;
- *Frame aggregation* — enables support for AMPDU/AMSDU;
- *Short Preamble* — use of the packet short preamble;
- *Broadcast/Multicast Rate Limiting, p/s* — when the flag is set, transmission of broadcast / multicast traffic over the wireless network is restricted. Specify the limit for broadcast traffic in the popup window (p/s);
- *Wi-Fi Multimedia (WMM)* — WMM support activation (Wi-Fi Multimedia);
- *DHCP Snooping Mode*<sup>1</sup> — selection of DHCP option 82 processing policy. Available values for selection:
  - *ignore* — option 82 processing is disabled. Default value;
  - *remove* — access point deletes the value of option 82;
  - *replace* — access point substitutes or replaces the value of option 82. When selecting this value to edit, the following parameters are opened:
    - *Option 82 CID format* — replacement of the CID parameter value, can take values:
      - *APMAC-SSID* — replacement of the CID parameter value to <MAC address of the access point>-<SSID name>. Default value;
      - *SSID* — replacement of the CID parameter value to SSID name, to which the client is connected;
      - *custom* — replacement of the CID parameter value to the value specified in the "Option 82 Unique CID";
        - *Option 82 Unique CID* — an arbitrary string of up to 52 characters that will be passed to the CID. If the parameter value is not set, the point will change the CID to the default value — APMAC-SSID.
    - *Option 82 RID format* — replacement of the RID parameter value, can take the following values:
      - *ClientMAC* — change the RID content to the MAC address of the client device. Default value;
      - *APMAC* — change the RID content to the MAC address of the access point;
      - *APdomain* — change the RID content to the domain in which the access point is located;
      - *custom* — change the RID content to the value specified in the "Option 82 Unique RID";
        - *Option 82 Unique RID* — an arbitrary string of up to 63 characters that will be passed to the RID. If the parameter value is not set, the point will change the RID to the default value — ClientMAC.
    - *MAC-address format* — selection of octet delimiters of the MAC address, which is transmitted in CID and RID:
      - *AA:BB:CC:DD:EE:FF* — the delimiter is a colon (:). Default value;
      - *AA-BB-CC-DD-EE-FF* — the delimiter is a dash (-).
- *Enable QoS* — when the flag is set, the setting of Quality of Service functions is available.

---

<sup>1</sup> Full functionality support is planned for future releases.

The following functions are available for quality assurance configuration:

| AP EDCA Parameters   |                                |                                   |                                     |                                 |
|----------------------|--------------------------------|-----------------------------------|-------------------------------------|---------------------------------|
| Queue                | AIFS                           | cwMin                             | cwMax                               | TXOP Limit                      |
| Data 3 (Background)  | <input type="text" value="7"/> | <input type="text" value="15"/> ▼ | <input type="text" value="1023"/> ▼ | <input type="text" value="0"/>  |
| Data 2 (Best Effort) | <input type="text" value="3"/> | <input type="text" value="15"/> ▼ | <input type="text" value="63"/> ▼   | <input type="text" value="0"/>  |
| Data 1 (Video)       | <input type="text" value="1"/> | <input type="text" value="7"/> ▼  | <input type="text" value="15"/> ▼   | <input type="text" value="94"/> |
| Data 0 (Voice)       | <input type="text" value="1"/> | <input type="text" value="3"/> ▼  | <input type="text" value="7"/> ▼    | <input type="text" value="47"/> |

| Station EDCA Parameters |                                |                                   |                                     |                                 |
|-------------------------|--------------------------------|-----------------------------------|-------------------------------------|---------------------------------|
| Queue                   | AIFS                           | cwMin                             | cwMax                               | TXOP Limit                      |
| Data 3 (Background)     | <input type="text" value="7"/> | <input type="text" value="15"/> ▼ | <input type="text" value="1023"/> ▼ | <input type="text" value="0"/>  |
| Data 2 (Best Effort)    | <input type="text" value="3"/> | <input type="text" value="15"/> ▼ | <input type="text" value="1023"/> ▼ | <input type="text" value="0"/>  |
| Data 1 (Video)          | <input type="text" value="2"/> | <input type="text" value="7"/> ▼  | <input type="text" value="15"/> ▼   | <input type="text" value="94"/> |
| Data 0 (Voice)          | <input type="text" value="2"/> | <input type="text" value="3"/> ▼  | <input type="text" value="7"/> ▼    | <input type="text" value="47"/> |

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

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

### 5.5.3 The “Advanced” submenu

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

- *Country* — the name of the country in which the access point operates. To select a country, check the “Unlock”. Depending on the value specified, country-specific frequency band and transmitter power restrictions will apply. The list of available frequency channels depends on the specified country, which affects the automatic selection of a channel in the Channel = Auto mode. If the client equipment is licensed for use in a different region, possibly, you will not be able to communicate with the access point.

⚠ Setting up local (regional) restrictions, including working on permitted frequency channels and output power is the responsibility of the installers.

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

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

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

## 5.6 The “VAP” menu

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

### 5.6.1 The “Summary” submenu

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

The screenshot shows the WOP-30L web interface with the 'VAP' menu selected. The 'Summary' submenu is active, displaying a table of VAP configurations for the 2.4 GHz radio interface. The table has columns for VAP, Enabled, Security Mode, VLAN ID, SSID, Broadcast SSID, Band Steer, VLAN Trunk, General Mode, General VLAN ID, and Station Isolation. Four VAPs are listed: VAP0, VAP1, VAP2, and VAP3. All are currently disabled and have Security Mode set to Off. The SSIDs are WOP-30L\_2.4GHz, WOP-30L\_2.4GHz-1, WOP-30L\_2.4GHz-2, and WOP-30L\_2.4GHz-3 respectively. A 'Show all' link is at the bottom left of the table. At the bottom of the interface are 'Apply' and 'Cancel' buttons.

| VAP  | Enabled                  | Security Mode | VLAN ID              | SSID             | Broadcast SSID           | Band Steer               | VLAN Trunk               | General Mode             | General VLAN ID      | Station Isolation        |
|------|--------------------------|---------------|----------------------|------------------|--------------------------|--------------------------|--------------------------|--------------------------|----------------------|--------------------------|
| VAP0 | <input type="checkbox"/> | Off           | <input type="text"/> | WOP-30L_2.4GHz   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> | <input type="checkbox"/> |
| VAP1 | <input type="checkbox"/> | Off           | <input type="text"/> | WOP-30L_2.4GHz-1 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> | <input type="checkbox"/> |
| VAP2 | <input type="checkbox"/> | Off           | <input type="text"/> | WOP-30L_2.4GHz-2 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> | <input type="checkbox"/> |
| VAP3 | <input type="checkbox"/> | Off           | <input type="text"/> | WOP-30L_2.4GHz-3 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> | <input type="checkbox"/> |

- *VAP0–VAP6* – the sequence number of the virtual access point;
- *Enabled* – when checked, the virtual access point is enabled, otherwise it is disabled;
- *Security Mode* – the type of data encryption used on the virtual access point;
- *VLAN ID* – VLAN number from which the tag will be removed when transmitting Wi-Fi traffic to clients connected to this VAP. When traffic flows in the opposite direction, untagged traffic from clients will be tagged with VLAN ID (when VLAN Trunk mode is disabled);
- *SSID* – virtual wireless network name;
- *Broadcast SSID* – when checked, SSID broadcasting is on, otherwise it is disabled;
- *Band Steer mode*<sup>1</sup> – when the flag is set, the priority connection of the client to 5 GHz network is active. In order for this feature to work, it is required to create a VAP with the same SSID on each radio interface and activate the “Band Steer mode” on them;
- *VLAN Trunk* – when the flag is set, tagged traffic is transmitted to the subscriber;
- *General Mode* – when the flag is set, transmission of untagged traffic jointly with tagged traffic is allowed (available when Trunk VLAN mode is enabled);
- *General VLAN ID* – a tag will be removed from the specified VLAN ID and the traffic of this VLAN will pass to the client without a tag. When traffic passes in the opposite direction, untagged traffic will be tagged with General VLAN ID;
- *Station Isolation* – when checked, traffic isolation between clients in the same VAP is enabled.

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

<sup>1</sup> Full functionality support is planned for future releases.



### 5.6.2 The “VAP” submenu

The screenshot displays the WOP-30L web interface for configuring a Virtual Access Point (VAP). The top navigation bar includes 'Monitoring', 'Radio', 'VAP' (selected), 'Network Settings', 'External Services', and 'System'. A language dropdown is set to 'en' and a '(logout)' link is present. On the left, a sidebar shows 'Summary' and frequency options '2.4 GHz >' and '5 GHz'. The main content area is titled 'Common Settings' for 'VAP0'. The settings are as follows:

- Enabled:** ☒
- VLAN ID:** ☐
- SSID:** WOP-30L\_2.4GHz
- Broadcast SSID:** ☒
- Band Steer:** ☐
- VLAN Trunk:** ☐
- General Mode:** ☐
- Station Isolation:** ☐
- 802.11k/v:** ☐
- Wireless Multicast Forwarding:** ☐
- Priority:** DSCP
- Minimal Signal:** ☒
- Minimal Signal Level, dBm:** -100
- Roaming Signal Level, dBm:** -100
- Minimal Signal Timeout, s:** 10
- Maximum Stations:** 0
- Security Mode:** Off
- OWE Transition Mode:** none

#### Common settings:

- **Enabled** – when checked, the virtual access point is enabled, otherwise it is disabled;
- **VLAN ID** – VLAN number from which the tag will be removed when transmitting Wi-Fi traffic to clients connected to this VAP. When traffic flows in the opposite direction, untagged traffic from clients will be tagged with VLAN ID (when VLAN Trunk mode is disabled);
- **SSID** – virtual wireless network name;
- **Broadcast SSID** – when checked, SSID broadcasting is on, otherwise it is disabled;
- **Band Steer mode**<sup>1</sup> – when the flag is set, the priority connection of the client to 5 GHz network is active. In order for this feature to work, it is required to create a VAP with the same SSID on each radio interface and activate the “Band Steer mode” on them;
- **VLAN Trunk** – when the flag is set, tagged traffic is transmitted to the subscriber;
- **General Mode** – when the flag is set, transmission of untagged traffic jointly with tagged traffic is allowed (available when Trunk VLAN mode is enabled);
- **General VLAN ID** – a tag will be removed from the specified VLAN ID and the traffic of this VLAN will pass to the client without a tag. When traffic passes in the opposite direction, untagged traffic will be tagged with General VLAN ID;
- **Station Isolation** – when checked, traffic isolation between clients in the same VAP is enabled;
- **802.11k/v**<sup>1</sup> – enable support for 802.11k/v standards on virtual access point;
- **Wireless Multicast Forwarding** – when the flag is set, traffic towards clients will be converted to Unicast before each client, if it is disabled, it will pass without modifications;

- *Priority* – select prioritization mode. Defines the field on the basis of which the traffic transmitted to the radio interface will be distributed in WMM queues:
  - *DSCP* – will analyze the priority from the DSCP field of the IP packet header;
  - *802.1p* – will analyze the priority from the CoS (Class of Service) field of the tagged packets.
- *Minimal Signal* – when the flag is set, the function of disabling client Wi-Fi equipment when the signal level is low (Minimal Signal) is enabled. For the functionality to work, configure the following parameters:
  - *Minimal Signal Level, dBm* – signal level in dBm, below which the client equipment is disconnected from the virtual network;
  - *Roaming Signal Level, dBm* – roaming sensitivity level in dBm, below which the client equipment switches to another access point. The parameter should be higher than the “*Minimum signal level*”: if the “*Minimum signal level*” is equal to -75 dBm, then the “*Roaming Signal Level*” should be equal to, for example, -70 dBm;
  - *Minimal Signal Timeout, s* – the period of time after which a decision is made to disconnect the client equipment from the virtual network.
- *Maximum Stations* – the maximum allowable number of clients connected to the virtual network;
- *MFP* – management frame protection (available for WPA2, WPA3, WPA2/WPA3, WPA2-Enterprise, WPA2/WPA3-Enterprise and WPA3-Enterprise selected security mode, selecting other security modes puts the MFP in the disabled state, when the WPA3, WPA3-Enterprise security mode is selected, the MFP is set to the enabled state):
  - *Off* – management frame protection is disabled;
  - *Optional* – protection works if the client supports MFP. Customers without MFP support can connect to this VAP;
  - *On* – management frame protection is enabled, clients that do not support MFP cannot connect.
- *Security Mode* – wireless access security mode:
  - *Off* – do not use encryption for data transfer. The access point is available for any subscriber to connect. For open networks, you can additionally configure “*OWE Transition mode*<sup>2</sup>”. In this field you should specify the interface with the OWE encryption type with which communication will be established;
  - *OWE (Opportunistic Wireless Encryption)* – an encryption method that ensures the security of data transmitted over an unsecured network. In this case, users are not required to take any additional actions or enter a password to connect to the network.  
When this mode is selected, a non-editable field “*OWE Transition Mode*<sup>2</sup>” is displayed, indicating the interface with an open encryption type with which connectivity is currently configured;
  - *WPA, WPA2, WPA/WPA2, WPA2/WPA3, WPA3* – encryption methods, when selecting one of the methods the following setting will be available:
    - *WPA Key* – key/password required to connect to the virtual access point. The length of the key makes from 8 to 63 characters.
  - *WPA-Enterprise, WPA2-Enterprise, WPA/WPA2-Enterprise, WPA2/WPA3-Enterprise, WPA3-Enterprise* – wireless channel encryption mode, in which the client is authorized on the centralized RADIUS server. To configure this security mode, specify the parameters of the RADIUS server. Also specify a key for the RADIUS server. When selecting one of the these methods, the following setting will be available:

| RADIUS                                     |                                                                                                                            |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| Domain                                     | <input type="text" value="root"/>                                                                                          |
| IP Address of RADIUS Server                | <input type="text" value="192.168.0.1"/>                                                                                   |
| Port of RADIUS Server                      | <input type="text" value="1812"/>                                                                                          |
| Password of RADIUS Server                  | <input type="password" value="*****"/>  |
| Use Accounting through RADIUS              | <input checked="" type="checkbox"/>                                                                                        |
| Use Other Settings For Accounting          | <input checked="" type="checkbox"/>                                                                                        |
| IP Address of RADIUS Server for Accounting | <input type="text" value="192.168.0.1"/>                                                                                   |
| Port of RADIUS Server for Accounting       | <input type="text" value="1813"/>                                                                                          |
| Password of RADIUS Server for Accounting   | <input type="password" value="*****"/>  |
| Use Periodic Accounting                    | <input checked="" type="checkbox"/>                                                                                        |
| Accounting Interval                        | <input type="text" value="600"/>                                                                                           |

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

<sup>1</sup> Full functionality support is planned for future releases.

<sup>2</sup> "OWE transition Mode" provides backward compatibility with WiFi clients that do not support OWE authentication. When attempting to connect to an open network where "OWE transition mode" is configured, a client that supports OWE will connect to the encrypted network configured on the specified interface, and a client that does not support OWE will connect to the current open network without encryption.

Captive Portal

Enable ☒

Virtual Portal Name

Redirect URL

RADIUS

Use Accounting through RADIUS ☒

Domain

IP Address of RADIUS Server for Accounting

Port of RADIUS Server for Accounting

Password of RADIUS Server for Accounting

Use Periodic Accounting ☒

Accounting Interval

Shapers

Enable ☒

VAP Limit Down ☐  kbps

VAP Limit Up ☐  kbps

STA Limit Down ☐  kbps

STA Limit Up ☐  kbps

### Captive Portal:

When selecting one of the following security modes: Off, WPA, WPA2, WPA/WPA2, WPA3, WPA2/WPA3, a portal authorization setting is available on the VAP.

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

### RADIUS:

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

### Shapers:

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

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

### MAC ACL:

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

- *Enabled* – when the flag is set, the selected access policy will work;
- *Policy* – access policy. Possible values:
  - *Deny* – clients whose MAC addresses are contained in the list will be prohibited from connecting to this VAP. The access will be allowed to other clients;
  - *Allow* – only those clients whose MAC addresses are contained in the list will be allowed to connect to this VAP. The access will be denied to other clients.
- *List of MAC Addresses* – a list of MAC addresses of clients who are allowed or denied access to this VAP. The list contain up to 128 addresses.

To add an address to the list, click the  button, enter the MAC address in the displayed field. In order to delete the address from the list, click the  button in the corresponding line.

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

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

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

## 5.7 The “Network Settings” menu

### 5.7.1 The “System Configuration” submenu

The screenshot displays the 'System Configuration' submenu for the WOP-30L device. The top navigation bar includes 'Monitoring', 'Radio', 'VAP', 'Network Settings' (active), 'External Services', and 'System'. The 'en' language dropdown and '(logout)' link are on the right. The left sidebar shows 'System Configuration >' and 'Access'. The main configuration area includes the following fields:

- Hostname:** WOP-30L
- AP Location:** root
- Management VLAN:** Disabled (dropdown)
- Protocol:** DHCP (dropdown)
- Primary DNS Server:** xxx.xxx.xxx.xxx
- Secondary DNS Server:** xxx.xxx.xxx.xxx

At the bottom, there are 'Apply' and 'Cancel' buttons.

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

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

### 5.7.2 The “Access” submenu

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

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

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

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

The screenshot displays the 'Access' configuration page in the WOP-30L web interface. The top navigation bar includes 'Monitoring', 'Radio', 'VAP', 'Network Settings' (active), 'External Services', and 'System'. The right side of the bar shows 'en' and a '(logout)' link. The left sidebar has 'System Configuration' and 'Access >'. The main content area lists various access protocols with checkboxes: WEB (checked), WEB-HTTPS (checked), Telnet (checked), SSH (checked), NETCONF (checked), and SNMP (checked). Below these are input fields for 'roCommunity' (public), 'rwCommunity' (private), 'TrapSink', 'Trap2Sink', 'InformSink', 'Sys Name' (WOP-30L), 'Sys Contact' (Contact), 'Sys Location' (Russia), and 'Trap Community' (trap). At the bottom, there are 'Apply' and 'Cancel' buttons.

The WOP-30L software allows changing the device configuration, monitoring the status of the access point and its sensors, as well as managing the device using the SNMP protocol.

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

- *roCommunity* — a password to read the parameters (by default: *public*);
- *rwCommunity* — a password to write parameters (by default: *private*);

- *TrapSink* – IP address or domain name of SNMPv1-trap message recipient in HOST [COMMUNITY [PORT]] format;
- *Trap2Sink* – IP address or domain name of SNMPv2-trap message recipient in HOST [COMMUNITY [PORT]] format;
- *InformSink* – IP address or domain name of Inform message recipient in HOST [COMMUNITY [PORT]] format;
- *Sys Name* – device name;
- *Sys Contact* – device vendor contact information;
- *Sys Location* – device location information;
- *Trap community* – password enclosed in traps (default value: trap).

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

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

where eltexLtd – 1.3.6.1.4.1.35265 is Eltex Enterprise ID.

A detailed description of WOP-30L OID is available at the following link: [OID description on WEP/WOP-xL](#).

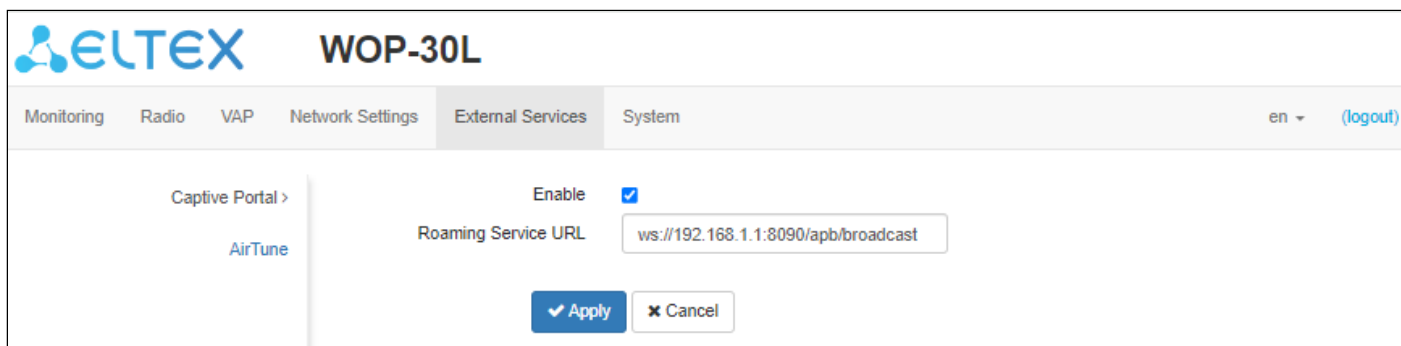
To apply a new configuration and save settings to non-volatile memory, click “Apply”. Click “Cancel” to discard the changes.

## 5.8 The “External Services” menu

### 5.8.1 The “Captive Portal” submenu

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

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



The screenshot shows the WOP-30L web interface. At the top, there's a navigation bar with tabs: Monitoring, Radio, VAP, Network Settings, External Services (selected), and System. On the right of the navigation bar, there's a language dropdown set to 'en' and a '(logout)' link. Below the navigation bar, the 'Captive Portal' submenu is expanded, showing 'AirTune' and 'Enable' (checked). The 'Roaming Service URL' field is set to 'ws://192.168.1.1:8090/apb/broadcast'. At the bottom, there are 'Apply' and 'Cancel' buttons.

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

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



### 5.8.2 The “AirTune” submenu

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

The AirTune service is intended for Radio Resource Management and automatic configuration of 802.11 k/r seamless roaming.

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

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

## 5.9 The “System” menu

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

### 5.9.1 The “Device Firmware Upgrade” submenu

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

The screenshot shows the ELTEX WOP-30L web interface. The top navigation bar includes links for Monitoring, Radio, VAP, Network Settings, External Services, and System (which is active). On the right of the bar are language settings (en) and a (logout) link. The left sidebar under 'Device Firmware Upgrade >' lists Configuration, Reboot, Password, Log, and Date and Time. The main content area displays:
 

- Active Version: 2.3.0 build 551
- Backup Version: 2.3.0 build 534 with a 'Set Active' button.
- A message: 'The latest firmware version is available at: <http://eltex-co.ru/support/downloads/>'
- Firmware Image: A file selection field showing 'Выберите файл' and 'Файл не выбран'.
- A 'Start Upgrading' button with an upload icon.

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

### Firmware upgrade

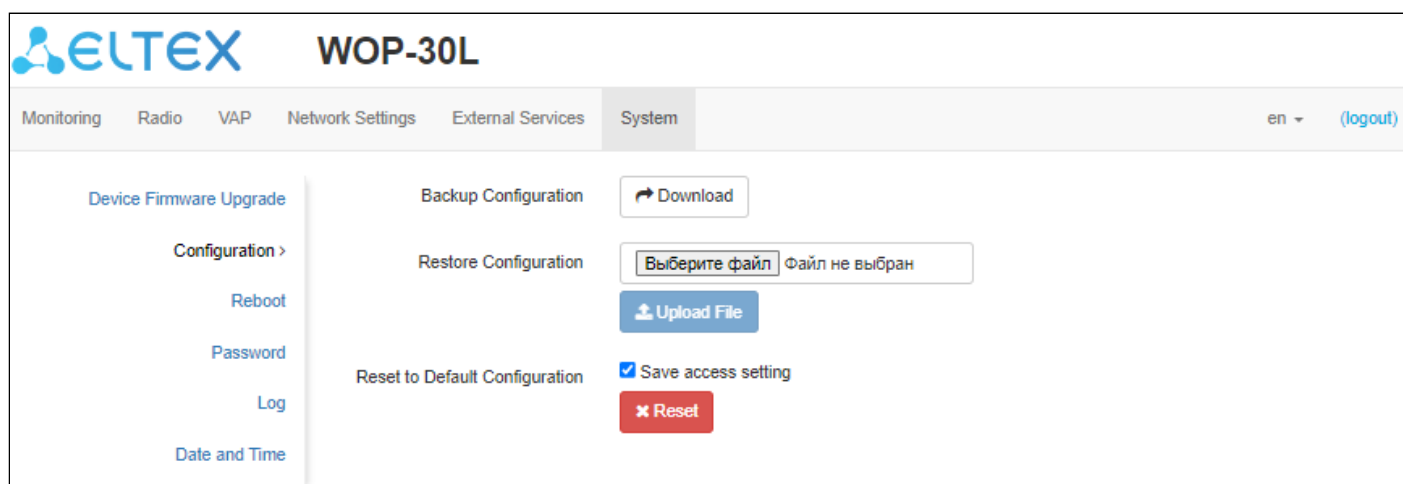
Download the firmware file from <http://eltex-co.com/support/downloads/>, selecting WOP-30L from the equipment list, and save it on your computer. To do this, click “Browse” in the Firmware Image field and specify the path to the firmware file in .tar.gz format.

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

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

### 5.9.2 The “Configuration” submenu

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



#### Backup Configuration

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

#### Restore Configuration

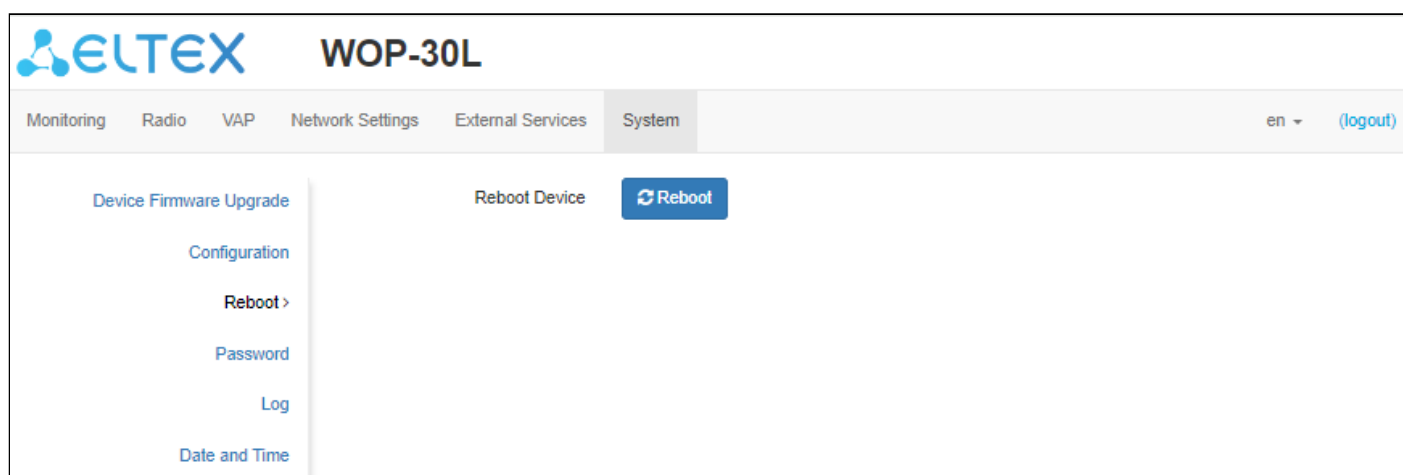
To upload the configuration file saved on the local computer, use the *Restore Configuration* item. To update the device configuration click “Browse”, specify a file (in .tar.gz format) and click “Upload File”. Uploaded configuration will be applied automatically and does not require device reboot.

#### Reset to Default Configuration

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

### 5.9.3 The “Reboot” submenu

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



#### 5.9.4 The “Password” submenu

When logging in via web interface, administrator (default password: **password**) has the full access to the device: read/write any settings, full device status monitoring.

To change the password, enter the new password first in the “Password” field, then in the “Confirm Password” field, and click “Apply” to save the new password.

The screenshot shows the WOP-30L web interface with the 'System' tab selected. On the left sidebar, the 'Password' option is highlighted. The main content area contains two input fields: 'Password' and 'Confirm Password', each with a toggle icon to the right. Below these fields are two buttons: 'Apply' (with a checkmark icon) and 'Cancel' (with an 'X' icon). The top navigation bar includes links for Monitoring, Radio, VAP, Network Settings, External Services, and System. The top right corner shows 'en' and a '(logout)' link.

#### 5.9.5 The “Log” submenu

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

The screenshot shows the WOP-30L web interface with the 'System' tab selected. On the left sidebar, the 'Log' option is highlighted. The main content area contains a 'Mode' dropdown menu set to 'Server and File'. Below it are three input fields: 'Syslog Server Address' (containing 'syslog.server'), 'Syslog Server Port' (containing '514'), and 'File Size, KB' (containing '1000'). At the bottom are 'Apply' and 'Cancel' buttons. The top navigation bar and user information are the same as in the previous screenshot.

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

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

### 5.9.6 The “Date and Time” submenu

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

#### 5.9.6.1 Manual

The screenshot displays the 'Date and Time' configuration page for the WOP-30L device. The interface includes a top navigation bar with tabs: Monitoring, Radio, VAP, Network Settings, External Services, and System (selected). A sidebar on the left lists various system functions, with 'Date and Time' currently selected. The main configuration area shows the 'Mode' set to 'Manual' (radio button selected). The 'Date and Time device' is displayed as '12/20/2023 07:50:47' with an 'Edit' link. The 'Time Zone' is set to 'Moscow, Russia' via a dropdown menu. The 'Enable daylight saving time' checkbox is checked. Below this, the 'DST Start' and 'DST End' fields are currently set to '(not selected)' with time components (day, month, year, hour, minute) shown as empty boxes. The 'DST Offset (minutes)' is set to '60'. At the bottom of the configuration area, there are 'Apply' and 'Cancel' buttons.

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

## 5.9.6.2 NTP server

ELTEX WOP-30L

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

Device Firmware Upgrade

Configuration

Reboot

Password

Log

Date and Time >

Mode ☐ Manual ☒ NTP Server

Date and Time device 12/20/2023 07:52:45

NTP Server pool.ntp.org

Time Zone Moscow, Russia

Enable daylight saving time ☒

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

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

DST Offset (minutes) 60

✓ Apply ✕ Cancel

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

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

## 6 Managing the device using the command line

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

### 6.1 Connection to the device

By default, WOP-30L is configured to receive the address via DHCP. If this does not happen, it is possible to connect to the device using the factory IP address.

- ✓ WOP-30L factory default IP address: **192.168.1.10**, subnet mask: **255.255.255.0**.

Connection to the device is performed via SSH/Telnet:

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

## 6.2 Network parameters configuration

### Configuring the static network parameters of the access point

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

### Adding a static route

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

### Configuring the reception of network parameters via DHCP

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



**Configuring IPv4 access settings**

```

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

```

- ✓ Starting from 2.2.0 software version, it is possible to set the MTU via DHCP (option 26). The MTU value obtained via DHCP has higher priority than the parameter specified in the configuration.

- ⚠ The MTU size for a bridge should not be larger than the smallest MTU size on the interfaces that are located in this bridge.

**Setting the MTU size on an interface**

```

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

```

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

**Untagged access**

Obtaining the network parameters via DHCP:

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

Static settings:

```
WOP-30L(root):/# set-management-vlan-mode off protocol static-ip ip-addr X.X.X.X netmask Y.Y.Y.Y gateway Z.Z.Z.Z (where X.X.X.X – static IP address, Y.Y.Y.Y – subnet mask, Z.Z.Z.Z – gateway)
```

**Access via Management VLAN in Terminating mode**

Obtaining the network parameters via DHCP:

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

Static settings:

WOP-30L(root):/# **set-management-vlan-mode terminating vlan-id X protocol static-ip ip-addr X.X.X.X netmask Y.Y.Y.Y gateway Z.Z.Z.Z** (where X – VLAN ID, used for access to the device. Acceptable values: 1–4094; X.X.X.X – static IP address; Y.Y.Y.Y – subnet mask; Z.Z.Z.Z – gateway)

**Access via Management VLAN in Forwarding mode**

Obtaining the network parameters via DHCP:

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

Static settings:

WOP-30L(root):/# **set-management-vlan-mode forwarding vlan-id X protocol static-ip ip-addr X.X.X.X netmask Y.Y.Y.Y gateway Z.Z.Z.Z** (where X – VLAN ID, used for access to the device. Acceptable values: 1–4094; X.X.X.X – static IP address; Y.Y.Y.Y – subnet mask; Z.Z.Z.Z – gateway)

**Completing and saving settings**

WOP-30L(root):/# **save** (save changes)

## 6.2.2 IPv6 network parameters configuration

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

**Enabling access to the device via IPv6 protocol**

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

**Configuring static IPv6 network settings for the access point**

```

WOP-30L(root):/# configure
WOP-30L(config):/# interface
WOP-30L(config):/interface# br0
WOP-30L(config):/interface/br0# common
WOP-30L(config):/interface/br0/common# ipv6
WOP-30L(config):/interface/br0/common/ipv6# address
XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX (where
XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX – static IPv6 address of WOP-30L)
WOP-30L(config):/interface/br0/common/ipv6# address-prefix-length X (where X – static IPv6 address
prefix. Takes values from 0 to 128. By default – 64)
WOP-30L(config):/interface/br0/common/ipv6# gateway XXXX:XXXX:XXXX:XXXX::/64 (IPv6 prefix is
specified, for example 3211:0:0:1234::/64)
WOP-30L(config):/interface/br0/common/ipv6# dns-server-1
XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX/Y (where
XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX/Y – IPv6 address of the DNS server №1 with prefix)
WOP-30L(config):/interface/br0/common/ipv6# dns-server-2
XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX/Y (where
XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX/Y – IPv6 address of the DNS server №2 with prefix)
WOP-30L(config):/interface/br0/common/ipv6# protocol static-ip (enable use of static IPv6 networks
parameters. For obtaining the IPv6 network parameters via DHCP enter dhcp)
WOP-30L(config):/interface/br0/common/ipv6# enabled true (enable access to the device via IPv6
protocol. To disable, enter false)
WOP-30L(config):/interface/br0/common/ipv6# save (save changes)

```

**Configuring IPv6 access settings**

```

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

```

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

### 6.3 Virtual Wi-Fi access points (VAP) configuration

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

Table 7 — Commands for configuring security mode on VAP

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

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

### 6.3.1 Configuration of VAP without encryption

#### Creating a VAP without encryption with periodic sending of account information to the RADIUS server

```

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

```

### 6.3.2 Configuration of VAP with OWE encryption

#### Creating a VAP with OWE encryption

```

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

```

### 6.3.3 Configuration of VAP with OWE and OWE Transition Mode

- ✓ Only Wi-Fi 6 clients are able to connect to a VAP with OWE security mode. So that all other clients were able to connect to such a VAP, OWE Transition Mode should be configured. In this mode, Wi-Fi 6 clients will be connected in OWE security mode, and all other clients will be connected in the open mode.

#### Creating a VAP with OWE and OWE Transition Mode

```

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

```



### 6.3.4 Configuration of VAP with WPA-Personal security mode

#### Creating a VAP with WPA-Personal encryption mode with periodic sending of accounting to RADIUS server

```

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

```



### 6.3.5 Configuration of VAP with Enterprise authorization

#### Creating a VAP with WPA2-Enterprise encryption mode with periodic sending of accounting to the RADIUS server

```

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

```

### 6.3.6 Configuration of VAP with Captive Portal

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

```

WOP-30L(root):/# configure
WOP-30L(config):/# interface
WOP-30L(config):/interface# wlan1-va0
WOP-30L(config):/interface/wlan1-va0# vap
WOP-30L(config):/interface/wlan1-va0/vap# vlan-id X (where X – VLAN-ID on VAP)
WOP-30L(config):/interface/wlan1-va0/vap# ap-security
WOP-30L(config):/interface/wlan1-va0/vap/ap-security# mode off (encryption mode off – without password)
WOP-30L(config):/interface/wlan1-va0/vap/ap-security# exit
WOP-30L(config):/interface/wlan1-va0/vap# ssid 'Portal_WOP-30L' (change SSID name)
WOP-30L(config):/interface/wlan1-va0/vap# captive-portal
WOP-30L(config):/interface/wlan1-va0/vap/captive-portal# scenarios
WOP-30L(config):/interface/wlan1-va0/vap/captive-portal/scenarios# scenario-redirect
WOP-30L(config):/interface/wlan1-va0/vap/captive-portal/scenarios/scenario-redirect# redirect-url http://<IP>:<PORT>/eltex_portal/ (specify URL of virtual portal)
WOP-30L(config):/interface/wlan1-va0/vap/captive-portal/scenarios/scenario-redirect# index 1
WOP-30L(config):/interface/wlan1-va0/vap/captive-portal/scenarios/scenario-redirect# virtual-portal-name default (specify portal name. By default: default)
WOP-30L(config):/interface/wlan1-va0/vap/captive-portal/scenarios/scenario-redirect# exit
WOP-30L(config):/interface/wlan1-va0/vap/captive-portal/scenarios# exit
WOP-30L(config):/interface/wlan1-va0/vap/captive-portal# enabled true
WOP-30L(config):/interface/wlan1-va0/vap/captive-portal# exit
WOP-30L(config):/interface/wlan1-va0/vap# radius
WOP-30L(config):/interface/wlan1-va0/vap/radius# domain root (where root – user domain)
WOP-30L(config):/interface/wlan1-va0/vap/radius# acct-enable true (enable periodic sending of "Accounting" messages to the RADIUS server. By default: false)
WOP-30L(config):/interface/wlan1-va0/vap/radius# acct-address X.X.X.X (where X.X.X.X – IP address of RADIUS server used for accounting)
WOP-30L(config):/interface/wlan1-va0/vap/radius# acct-password secret (where secret – password for RADIUS server used for accounting)
WOP-30L(config):/interface/wlan1-va0/vap/radius# acct-periodic true (enable periodic sending of "Accounting" messages to the RADIUS server. By default: false)
WOP-30L(config):/interface/wlan1-va0/vap/radius# acct-interval 600 (interval for sending "Accounting" messages to the RADIUS server)
WOP-30L(config):/interface/wlan1-va0/vap# exit
WOP-30L(config):/interface/wlan1-va0# common
WOP-30L(config):/interface/wlan1-va0/common# enabled true (enable VAP)
WOP-30L(config):/interface/wlan1-va0/common# save (save changes)

```

### 6.3.7 Advanced VAP settings

#### Assigning VLAN ID on VAP

WOP-30L(config):/interface/wlan1-va0/vap# **vlan-id X** (where X – VLAN ID number on VAP)

✓ Full support for the Band Steer functionality is planned for future releases.

#### Enabling Band Steer mode

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

#### Enabling VLAN trunk on VAP

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

#### Enabling General VLAN on VAP

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

#### Selection of the prioritization method

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

#### Enabling MFP (802.11W)

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

#### Enabling use of TLS at authorization

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

**Enabling hidden SSID**

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

**Enabling client isolation on VAP**

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

**Client limitation on VAP**

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

**Enabling multicast replication on VAP**

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

**Enabling Minimal Signal and Roaming Signal**

WOP-30L(config):/interface/wlan1-va0/vap# **check-signal-enable true** (enabling Minimal Signal functionality. To disable, enter **false**)

WOP-30L(config):/interface/wlan1-va0/vap# **min-signal X** (where X – RSSI threshold value, upon reaching which the point will disconnect the client from the VAP. The parameter can take values from -100 to -1)

WOP-30L(config):/interface/wlan1-va0/vap# **check-signal-timeout X** (where X – the period of time in seconds after which a decision is made to disconnect client equipment from the virtual network)

WOP-30L(config):/interface/wlan1-va0/vap# **roaming-signal X** (where X – RSSI threshold value, upon reaching which the point will switch to other access point. The parameter can take values from -100 to -1. The roaming-signal parameter should be higher than min-signal: if min-signal = -75 dBm, then roaming-signal should be -70 dBm, for example)

WOP-30L(config):/interface/wlan1-va0/vap# **save** (save changes)

**Enabling subscribers traffic transmission outside of GRE tunnel**

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

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

```

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

```

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

```

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

```

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

```

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

```

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

```

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

```

### Setting up MAC access control

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

### Configuring connection blocking for users spoofing MAC address of a wired network device

If, for security reasons, it is necessary to implement protection against connections from users duplicating the MAC address of a wired device (gateway, PC, etc. ), then you need to use the **fdb-filtering** setting, which has the following operating modes:

**on-connect** — mode blocks all attempts to connect devices via Wi-Fi if the MAC address has already been learned on the Ethernet port of the access point;

**by-eth-event** — mode disconnects a connected client via Wi-Fi if its MAC address has been learned on the Ethernet port of the access point (the mode helps clear an old client record when roaming);

**full** — mode combines all the previous ones, that is, it blocks the connection of a new user via Wi-Fi, and also disconnects a previously connected one if its MAC address matches the device on the Ethernet interface.

⚠ When setting the **full** and **on-connect** modes, the roaming of Wi-Fi clients may get worse. So, during operation, all broadcast packets from the client reach other access points of the network and its MAC is learned at all access points of the network, therefore, upon the client's roaming, if its MAC address is in the list on the Ethernet port, reconnection can take a long time time.

```
WOP-30L(config):/interface/wlan1-va0/vap# fdb-filtering
WOP-30L(config):/interface/wlan1-va0/vap/fdb-filtering # enabled true (enabling the functionality. To
disable, enter false. By default: false)
WOP-30L(config):/interface/wlan1-va0/vap/fdb-filtering #mode full (operating mode. By default: by-eth-
event)
```



## 802.11r configuration

✓ Full support for the functionality is planned for future releases.

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

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

See instructions for configuring VAP with WPA2-Personal security mode and others in [Configuration of VAP with WPA-Personal security mode](#).

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

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

### Configuring 802.11r on AP1

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

**Configuring 802.11r on AP2**

```

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

```



## 802.11k configuration

✔ Full support for this functionality is planned for future releases.

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

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

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

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

### Configuring 802.11k

```
WOP-30L(config):/interface/wlan1-va0/vap/w80211kv-config# enabled false
WOP-30L(config):/interface/wlan1-va0/vap/w80211kv-config# mac
WOP-30L(config):/interface/wlan1-va0/vap/w80211kv-config/mac# add E8:28:C1:FC:D6:90 (where
E8:28:C1:FC:D6:90 — MAC address of “friendly” access point)
WOP-30L(config):/interface/wlan1-va0/vap/w80211kv-config/mac# E8:28:C1:FC:D6:90
WOP-30L(config):/interface/wlan1-va0/vap/w80211kv-config/mac/E8:28:C1:FC:D6:90# channel 132
(where 132 — channel on which access point with E8:28:C1:FC:D6:90 MAC address operates)
WOP-30L(config):/interface/wlan1-va0/vap/w80211kv-config/mac/E8:28:C1:FC:D6:90# exit
WOP-30L(config):/interface/wlan1-va0/vap/w80211kv-config/mac# add E8:28:C1:FC:D6:70 (where
E8:28:C1:FC:D6:70 — MAC address of “friendly” access point)
WOP-30L(config):/interface/wlan1-va0/vap/w80211kv-config/mac# E8:28:C1:FC:D6:70
WOP-30L(config):/interface/wlan1-va0/vap/w80211kv-config/mac/E8:28:C1:FC:D6:70# channel 36
(where 36 — channel on which access point with E8:28:C1:FC:D6:70 MAC address operates)
WOP-30L(config):/interface/wlan1-va0/vap/w80211kv-config/mac/E8:28:C1:FC:D6:70# exit
WOP-30L(config):/interface/wlan1-va0/vap/w80211kv-config/mac# exit
WOP-30L(config):/interface/wlan1-va0/vap/w80211kv-config# enabled true (enabling access point
operation via 802.11k protocol)
WOP-30L(config):/interface/wlan1-va0/vap/w80211kv-config# save (save changes)
```

## 6.4 Radio configuration

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

### Change of operation channel and radio interface power

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

### ✓ Lists of available channels

#### Channels available for selection for radio 2.4 GHz:

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

#### Channels available for selection for radio 5 GHz:

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

### 6.4.1 Advanced Radio settings

#### Configuring the limited list of channels

WOP-30L(config):/interface/wlan0/wlan/radio# **use-limit-channels true** (enabling use of limited list of channels in channel autoselection operation. To disable, enter **false**)

WOP-30L(config):/interface/wlan0/wlan/radio# **limit-channels '1 6 11'** (where 1, 6, 11 are channels of range in which the configurable radio interface can operate)

#### Changing the primary channel

WOP-30L(config):/interface/wlan0/wlan/radio# **control-sideband lower** (parameter may take values: lower, upper. By default: for Radio 1: lower; for Radio 2: upper)

#### Enabling the use of Short Guard Interval

WOP-30L(config):/interface/wlan0/wlan/radio# **sgi true** (enabling the use of a Short Guard Interval for data transmission of 400 ns instead of 800 ns. To disable, enter **false**)

#### Enabling STBC

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

#### Enabling aggregation

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

#### Enabling the short preamble

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

#### Enabling the Wi-Fi Multimedia (WMM)

WOP-30L(config):/interface/wlan0/wlan/radio# **wmm true** (enabling the support for WMM (Wi-Fi Multimedia). To disable, enter **false**)

### Configuring DFS mechanism

Configuring is done only on Radio 5 GHz (wlan1)

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

### Enabling automatic channel width switch mode

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

### Enabling Broadcast/Multicast shaper

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

### Enabling QoS and parameter changes

WOP-30L(config):/interface/wlan0/wlan/radio# **qos**  
WOP-30L(config):/interface/wlan0/wlan/radio/qos# **enable true** (enabling the use of Quality of Service functions. To disable, enter **false**)  
WOP-30L(config):/interface/wlan0/wlan/radio/qos# **edca-ap** (configuring QoS parameters of the access point, traffic is transmitted from the access point to the client)  
WOP-30L(config):/interface/wlan0/wlan/radio/qos/edca-ap# **bk** (configuring QoS parameters for low-priority high-bandwidth queues (802.1p priorities: cs1, cs2)  
WOP-30L(config):/interface/wlan0/wlan/radio/qos/edca-ap/bk# **aifs X** (where X – waiting time for frames of data, measured in slots. Takes the values 1–255)  
WOP-30L(config):/interface/wlan0/wlan/radio/qos/edca-ap/bk# **cwmin X** (X – the initial value of the time to wait before resending a frame, specified in milliseconds. Accepts values: 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023. The cwMin value cannot exceed the cwMax value)  
WOP-30L(config):/interface/wlan0/wlan/radio/qos/edca-ap/bk# **cwmax X** (where X – maximum timeout value before resending a frame, specified in milliseconds. Accepts values: 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023. The cwMax value must be greater than the cwMin value)  
WOP-30L(config):/interface/wlan0/wlan/radio/qos/edca-ap/bk# **txop X** (where X – the time interval in milliseconds when the WME client station has the right to initiate data transmission over the wireless medium to the access point. Max value 65535 milliseconds)  
WOP-30L(config):/interface/wlan0/wlan/radio/qos/edca-ap/bk# **exit**  
WOP-30L(config):/interface/wlan0/wlan/radio/qos/edca-ap# **exit**  
WOP-30L(config):/interface/wlan0/wlan/radio/qos# **edca-sta** (configuring QoS parameters of the client station (traffic is transmitted from the client station to the access point))

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

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

## 6.5 Configuring DHCP option 82

- ✓ Full support for this functionality is planned for future releases.
- ✓ DHCP option 82 is configured separately for each radio interface. This section provides examples of configuring option 82 for Radio 2.4 GHz – wlan0.

DHCP snooping operating modes:

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

### Changing the operating mode of DHCP option 82

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

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

#### Configuring Option 82 parameters

WOP-30L(config):/interface/wlan0/common/dhcp-snooping# **dhcp-option-82-CID-format custom** (where **custom** — replacement of the CID content with the value specified in the **dhcp-option-82-custom-CID**. The parameter can take values: **APMAC-SSID** — replacement of the CID content with <MAC address of the access point>-<SSID name>. **SSID** — replacement of the CID content with SSID name, to which the client is connected. By default: **APMAC-SSID**)

WOP-30L(config):/interface/wlan0/common/dhcp-snooping# **dhcp-option-82-RID-format custom** (where **custom** — replacement of the RID content with the value specified in the **dhcp-option-82-custom-RID** parameter. The parameter can take values: **ClientMAC** — replacement of the RID content with MAC address of the client device. **APMAC** — replacement of the RID content with MAC address of the access point. **APdomain** — replacement of the RID content with the domain where the access point is located. By default: **ClientMAC**)

WOP-30L(config):/interface/wlan0/common/dhcp-snooping# **dhcp-option-82-custom-CID longstring** (where **longstring** — value from 1 to 52 characters, which will be transmitted in CID. If the value of **dhcp-option-82-custom-CID** parameter is not defined, the access point will change the CID to the default value: <MAC address of the access point>-<SSID name>)

WOP-30L(config):/interface/wlan0/common/dhcp-snooping# **dhcp-option-82-custom-RID longstring** (where **longstring** — value from 1 to 63 characters, which will be transmitted in RID. If the value of **dhcp-option-82-custom-RID** parameter is not defined, the access point will change the RID to the default value: MAC address of the client device)

WOP-30L(config):/interface/wlan0/common/dhcp-snooping# **dhcp-option-82-MAC-format radius** (selecting octet delimiter of the MAC address which is transmitted in RID and CID. **radius** — a dash is used as a delimiter: AA-BB-CC-DD-EE-FF; **default** — a colon is used as a delimiter: AA:BB:CC:DD:EE:FF)

## 6.6 System settings

### 6.6.1 Device firmware update

#### Device firmware update via TFTP

WOP-30L(root):/# **firmware upload tftp** <IP address of the TFTP server><Firmware file name> (example: firmware upload tftp 192.168.1.15 WOP-30L-2.3.0\_build\_X.tar.gz)  
WOP-30L(root):/# **firmware upgrade**

#### Device firmware update via HTTP

WOP-30L(root):/# **firmware upload http** <URL to upload the firmware file> (example: firmware upload http http://192.168.1.100:8080/files/WOP-30L-2.3.0\_build\_X.tar.gz)  
WOP-30L(root):/# **firmware upgrade**

#### Switching to access point firmware backup

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

### 6.6.2 Device configuration management

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

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

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

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

#### Download the device configuration file to TFTP server

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

#### Upload configuration file from TFTP server to the device

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

### 6.6.3 Device reboot

#### Command to reboot the device

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

### 6.6.4 Authentication Mode configuration

The device has a factory account of "admin" with a password of "password". This account cannot be deleted. The password can be changed using the following commands.

#### Changing the password for the admin account

```
WOP-30L(root):/# configure
WOP-30L(config):/# authentication
WOP-30L(config):/authentication# admin-password <New password for admin account> (from 1 up to 64
characters, including latin letters and digits)
WOP-30L(config):/authentication# save
```

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

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

#### Adding new users

```
WOP-30L(root):/# configure
WOP-30L(config):/# authentication
WOP-30L(config):/authentication# user
WOP-30L(config):/authentication/user# add userX (where userX — the name of the new account. To
delete, use the del command)
WOP-30L(config):/authentication/user# userX
WOP-30L(config):/authentication/user/userX# login userX (where userX — the name of the new account)
WOP-30L(config):/authentication/user/userX# password <Password for userX account> (from 1 to 64
characters, including latin letters and digits)
WOP-30L(config):/authentication/user/userX# role admin (the user is given the rights to configure.
Possible value viewer — only monitoring will be available to the account)
WOP-30L(config):/authentication/user/userX# save
```



For authentication through RADIUS, it is necessary to configure the access parameters to it.

#### Configuring RADIUS Server Access Settings

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

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

#### 6.6.5 Setting the date and time

##### Commands to configure NTP server time synchronization

```
WOP-30L(root):/# configure
WOP-30L(config):/# date-time
WOP-30L(config):/date-time# mode ntp (enabling NTP operation mode)
WOP-30L(config):/date-time# ntp
WOP-30L(config):/date-time/ntp# server <IP address of NTP server> (NTP server configuration)
WOP-30L(config):/date-time/ntp# exit
WOP-30L(config):/date-time# common
WOP-30L(config):/date-time/common# timezone 'Asia/Novosibirsk (Novosibirsk)' (time zone
configuration)
WOP-30L(config):/date-time/common# save (save changes)
```

#### 6.6.6 Advanced system settings

##### Enabling global isolation

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

**Changing device name**

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

**Changing geographical domain**

```
WOP-30L(root):/# configure
WOP-30L(config):/# system
WOP-30L(config):/system# ap-location ap.test.root (where ap.test.root is EMS management system
device tree node domain, where access point is located. By default: root)
WOP-30L(config):/system# save (save changes)
```

**Changing Radius NAS-ID**

```
WOP-30L(root):/# configure
WOP-30L(config):/# system
WOP-30L(config):/system# nas-id Lenina_1.Novosibirsk.root (where Lenina_1.Novosibirsk.root is ID of
this access point. This parameter is intended to identify the device on the RADIUS server if RADIUS
expects a value other than the MAC address. By default: MAC address of the access point)
WOP-30L(config):/system# save (save changes)
```

**Configuring LLDP**

```
WOP-30L(root):/# configure
WOP-30L(config):/# lldp
WOP-30L(config):/lldp# enabled true (enabling LLDP. To disable, enter false. By default: true)
WOP-30L(config):/lldp# tx-interval 60 (changing the sending interval of LLDP messages. By default: 30)
WOP-30L(config):/lldp# system-name WOP-30L_reserv (where WOP-30L_reserv is a new device
name. By default: WOP-30L)
WOP-30L(config):/lldp# save (save changes)
```

**Changing password**

```
WOP-30L(root):/# configure
WOP-30L(config):/# authentication
WOP-30L(config):/authentication# admin-password newpassword (where newpassword is a new
password for access point login. By default: password)
WOP-30L(config):/authentication# save (save changes)
```

## 6.7 APB service configuration

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

### Commands to configure the APB service

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

## 6.8 Monitoring

### 6.8.1 Wi-Fi clients

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

```

index                | 0
interface          | wlan1-va0
state                 | ASSOC SLEEP
hw-addr               | e2:f1:04:a4:bc:2a
ssid                  | WOP-30L_5GHz
ip-addr               | 10.24.80.75
hostname              | Xiaomi-12T
authorized            | true
captive-portal-vap    | false
enterprise-vap        | false
rx-retry-count        | 20879
tx-fails              | 32
tx-period-retry       | 0
tx-retry-count        | 14302
rssi-1                | -45
rssi-2                | -48
rssi                  | -45
snr-1                 | 36
snr                   | 36
snr-2                 | 36
tx-rate               | HE NSS2 MCS8 SGI 864.7
rx-rate               | HE NSS2 MCS7 SGI 720.6
rx-bw                 | 80M
rx-bw-all             | 80M
tx-bw                 | 80M
uptime                | 15:48:50
wireless-mode         | ax
perftest-capable      | false
link-quality           | 100 (not changed)
link-quality-common    | 83
actual-tx-rate         | 0
actual-rx-rate         | 0
shaped-rx-rate         | 0
actual-tx-pps          | 0
actual-rx-pps          | 0
shaped-rx-pps         | 0
name                  | 0

```

| Rate             | Transmitted | Received |
|------------------|-------------|----------|
| -----            | -----       | -----    |
| Total Packets:   | 71978       | 65595    |
| TX success:      | 99          |          |
| Total Bytes:     | 9366733     | 9437792  |
| Data Packets:    | 71894       | 65394    |
| Data Bytes:      | 9348348     | 9425315  |
| Mgmt Packets:    | 84          | 201      |
| Mgmt Bytes:      | 18385       | 12477    |
| Dropped Packets: | 0           | 0        |
| Dropped Bytes:   | 0           | 0        |
| Lost Packets:    | 0           |          |

| Rate       | Transmitted |     | Received |     |
|------------|-------------|-----|----------|-----|
| ofdm6      | 0           | 0%  | 3315     | 5%  |
| nss1-mcs7  | 15          | 0%  | 0        | 0%  |
| nss1-mcs8  | 9           | 0%  | 0        | 0%  |
| nss1-mcs9  | 6           | 0%  | 0        | 0%  |
| nss1-mcs10 | 5           | 0%  | 0        | 0%  |
| nss1-mcs11 | 45          | 0%  | 0        | 0%  |
| nss2-mcs3  | 2           | 0%  | 5        | 0%  |
| nss2-mcs4  | 0           | 0%  | 61       | 0%  |
| nss2-mcs5  | 0           | 0%  | 785      | 1%  |
| nss2-mcs6  | 78          | 0%  | 0        | 0%  |
| nss2-mcs7  | 1666        | 2%  | 19857    | 30% |
| nss2-mcs8  | 7880        | 10% | 29646    | 45% |
| nss2-mcs9  | 26677       | 37% | 7108     | 10% |
| nss2-mcs10 | 33420       | 46% | 578      | 0%  |
| nss2-mcs11 | 2090        | 2%  | 4039     | 6%  |

Multicast groups: none

## 6.8.2 Device information

### WOP-30L(root):/# monitoring information

```

system-time           | 12:50:37 27.09.2023
uptime                | 00:04:25
hostname              | WOP-30L
software-version      | 2.3.0 build X
secondary-software-version | 2.3.0 build X
boot-version          | 2.1.0 build X
memory-usage          | 43
memory-free           | 137
memory-used           | 104
memory-total          | 241
cpu-load               | 9.5
cpu-average            | 6.70
is-default-config     | false
board-type            | WOP-30L
hw-platform           | WOP-30L
factory-wan-mac       | 68:13:E2:35:C3:90
factory-lan-mac       | 68:13:E2:35:C3:90
factory-serial-number | WP52000345
hw-revision           | 1v2
session-password-initialized | false
ott-mode              | false
last-reboot-reason    | firmware update
test-changes-mode     | false

```

### 6.8.3 Certificate information

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

```
ott:
  status: not present
wlc:
  status: present
  url: https://192.168.1.1:8044
```

## 6.8.4 Network information

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

#### Common information:

```

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

```

#### IPv4 information:

```

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

```

#### IPv6 information:

```

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

```

### WOP-30L(root):/# monitoring ethernet

```

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

```

### WOP-30L(root):/# monitoring arp

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

WOP-30L(root):/# **monitoring route**

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

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

WOP-30L(root):/# monitoring lldp

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

## 6.8.5 Wireless interfaces

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

```

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

```



## 6.8.6 Event logging

### WOP-30L(root):/# monitoring events

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

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

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

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

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

## 6.8.7 Environment scan

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

### WOP-30L(root):/# monitoring scan-wifi

| SSID                | Mode | Security | MAC               | Channel | RSSI, dBm | Bandwidth, MHz |
|---------------------|------|----------|-------------------|---------|-----------|----------------|
| ESRAP1_of30_smart   | AP   | off      | A8:F9:4B:B0:2C:C7 | 6       | -65       | 20             |
| litv_hots_2         | AP   | off      | E0:D9:E3:8A:38:52 | 1       | -65       | 20             |
| test_001            | AP   | off      | E0:D9:E3:4B:FB:30 | 11      | -67       | 20             |
| 2G-COVID_TOWER      | AP   | off      | E0:D9:E3:98:12:72 | 11      | -71       | 20             |
| Tam2.4G             | AP   | wpa      | E0:D9:E3:98:1F:7A | 1       | -73       | 20             |
| litv_hots_1         | AP   | off      | E0:D9:E3:8A:38:51 | 1       | -77       | 20             |
| WOP-30L_ZN_Personal | AP   | wpa      | E0:D9:E3:49:79:06 | 44      | -16       | 20             |
| WOP-30L_ZN_Open     | AP   | off      | E0:D9:E3:49:79:07 | 44      | -17       | 20             |
| WOP-30L_ZN_OWE      | AP   | owe      | E0:D9:E3:49:79:08 | 44      | -17       | 20             |
| Eltex-Guest         | AP   | off      | CC:9D:A2:C7:D9:21 | 36      | -38       | 20             |
| Eltex-Local         | AP   | wpa      | CC:9D:A2:C7:D9:22 | 36      | -38       | 20             |
| BRAS-Guest          | AP   | off      | CC:9D:A2:C7:D9:20 | 36      | -38       | 20             |
| 2L_301_nsk          | AP   | off      | E8:28:C1:DA:C8:16 | 56      | -41       | 20             |
| chudo_waffly        | AP   | wpa      | E0:D9:E3:70:94:00 | 60      | -44       | 20             |
| Eltex VAP           | AP   | off      | A8:F9:4B:B0:40:70 | 48      | -46       | 20             |
| VK_enterprise       | AP   | wpa      | E8:28:C1:DA:C8:99 | 56      | -47       | 20             |
| VK_portal           | AP   | off      | E8:28:C1:DA:C8:98 | 56      | -49       | 20             |
| WOP-2ac             | AP   | off      | E8:28:C1:00:FC:A1 | 36      | -50       | 80             |
| Open_VK_switch      | AP   | off      | E8:28:C1:DA:C8:96 | 56      | -50       | 20             |
| testSSID10          | AP   | off      | A8:F9:4B:B0:05:54 | 40      | -51       | 20             |

### 6.8.8 Spectrum analyzer

- ✓ Full support for this functionality is planned for future releases.

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

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

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

#### WOP-30L(root):/# monitoring spectrum-analyzer

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

## 7 The list of changes

| Document version | Issue date | Revisions                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Version 1.2      | 12.2023    | <p>Synchronization with firmware version 2.3.0</p> <p>Added:</p> <p>6.3.2 Configuration of VAP with OWE encryption</p> <p>6.3.3 Configuration of VAP with OWE and OWE Transition Mode</p> <p>6.8.3 Certificate information</p> <p>Changed:</p> <p>2.2 Device specification</p> <p>2.3 Technical parameters</p> <p>5.4.7 The “Device Information” submenu</p> <p>5.5.1 The “Radio 2.4 GHz” submenu</p> <p>5.6.2 The “VAP” submenu</p> <p>6.3 Virtual Wi-Fi access points (VAP) configuration</p> <p>6.3.1 Configuration of VAP without encryption</p> <p>6.3.4 Configuration of VAP with WPA-Personal security mode</p> <p>6.3.5 Configuration of VAP with Enterprise authorization</p> <p>6.3.6 Configuration of VAP with Captive Portal</p> <p>6.3.7 Advanced VAP settings</p> <p>6.8.2 Device information</p> |

| Document version       | Issue date | Revisions                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Version 1.1            | 09.2023    | <p>Synchronization with firmware version 2.2.0</p> <p>Added:</p> <p>5.8.2 The “AirTune” submenu</p> <p>Changed:</p> <p>2.3 Technical parameters</p> <p>5.4.3 The “Scan Environment” submenu</p> <p>5.5 The “Radio” menu</p> <p>5.6.2 The “VAP” submenu</p> <p>6.2 Network parameters configuration</p> <p>6.3 Virtual Wi-Fi access points (VAP) configuration</p> <p>6.3.5 Advanced VAP settings</p> <p>6.6.4 Authentication Mode Access</p> <p>6.6.6 Advanced system settings</p> <p>6.8.3 Network information</p> |
| Version 1.0            | 06.2023    | First issue                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Firmware version 2.3.0 |            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

## TECHNICAL SUPPORT

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

<https://eltex-co.com/support/>

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

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

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