Wireless bridge

WB-3P-PTP6

User manual

Firmware version 2.6.1

IP address: 192.168.1.10

Username: admin

Password: password

1 Introduction 6

1.1 Annotation 6

1.2 Document conventions 6

2 Device description 7

2.1 Purpose 7

2.2 Device specification 7

2.3 Main technical specifications 9

2.4 Technical parameters of offset parabolic antenna 11

2.5 Radiation patterns 12

2.6 Design 14

2.7 Light indication 15

2.8 Restore the default configuration 16

2.9 Supply package 16

3 Rules and recommendations for device installation 17

3.1 Safety rules 17

3.2 Installation recommendations 17

3.3 Recommendations for lightning protection 19

4 Device preparation 20

5 Device connection 21

6 Preliminary setup 22

7 Device installation 22

7.1 Device installation on a pole/post/wall 22

7.2 Installation of the device as part of an offset parabolic antenna 26

8 Device alignment 32

8.1 Alignment of devices mounted on a pole/post/wall 32

8.2 Alignment of devices mounted on an offset parabolic antenna 33

9 Final device setup 35

10 Device management via web interface 36

10.1 Getting started 36

10.2 User change 37

10.3 Applying configuration and discarding changes 38

10.4 Test mode 39

10.5 Web interface basic elements 40

10.6 "Quick Start" menu 41

10.6.1 "Quick Start" submenu 41

10.7 "Monitoring" menu 44

10.7.1 "Wireless Peer/Wireless Clients" submenu 44

10.7.2 "Traffic Statistics" submenu 46
10.7.3 "Scan Environment" submenu 48
10.7.4 "Spectrum Analyzer" submenu 49
10.7.5 "Events" submenu 50
10.7.6 "Network Information" submenu 51
10.7.7 "Radio Information" submenu 53
10.7.8 "Device Information" submenu 54
10.8 "Radio" menu 55
10.8.1 "Radio" submenu 55
10.8.2 "QoS" submenu 60
10.8.3 "Advanced" submenu 61
10.9 "AP" menu 62
10.9.1 "Access Point" submenu 62
10.10 "STA" menu 70
10.10.1 "Station" submenu 70
10.11 "Network Settings" menu 74
10.11.1 "System Configuration" submenu 74
10.11.2 "Access" submenu 75
10.12 "System" menu 77
10.12.1 "Device Firmware Upgrade" submenu 77
10.12.2 "Configuration" submenu 78
10.12.3 "Ping Watchdog" submenu 79
10.12.4 "Reboot" submenu 80
10.12.5 "Authentication" submenu 80
10.12.6 "Log" submenu 82
10.12.7 "Date and Time" submenu 83
10.12.8 "LEDs" submenu 85
10.12.9 "Troubleshooting" submenu 86
10.13 "Tools" menu 87
10.13.1 "Antenna Align" submenu 87
10.13.2 "Speed Testing" submenu 88
11 Example of device setup 89
12 Managing the device using the command line 91
12.1 Connection to the device 91
12.2 Network parameters configuration 92
12.2.1 Network parameters configuration using the set-management-vlan-mode utility 93
12.2.2 Configuring 802.1p priority for Management VLAN 94

12.2.3 Remote management configuration....94
12.2.4 IPv6 network parameters configuration....97
12.3 Radio settings....98
12.3.1 Advanced Radio settings....99
12.4 Configuring DHCP option 82....103
12.5 Configuring wireless network....104
12.5.1 Network settings for access point (AP)....104
12.5.2 Advanced settings for access point (AP)....106
12.5.3 Network settings for client (STA)....114
12.5.4 Advanced settings for client (STA)....116
12.6 LoopBack Detection configuration....123
12.7 BPDU filter configuration....124
12.8 MAC address learning limiting....124
12.9 Changing the MTU size on interfaces....125
12.10 System settings....125
12.10.1 Upgrading the device firmware....125
12.10.2 Device configuration management....126
12.10.3 Ping watchdog....127
12.10.4 Device reboot....127
12.10.5 Configuring authentication mode....128
12.10.6 Configuring DHCP-snooping....131
12.10.7 Configuring date and time....131
12.10.8 Advanced system settings....132
12.11 Monitoring....134
12.11.1 Wireless Peer/Wireless Clients....134
12.11.2 Device information....152
12.11.3 Network information....153
12.11.4 Wireless interfaces....154
12.11.5 Event logs....155
12.11.6 Environment scan....155
12.11.7 Spectrum analyzer....156
12.11.8 Obtaining troubleshooting information....157
13 Auxiliary utilities....158
13.1 Perftest utility....158
13.2 Manage-remote utility....158
13.2.1 Rebooting....158
13.2.2 Scan environment....159

13.2.3 Spectrum Analyzer 159
13.2.4 Obtaining troubleshooting information 159
13.3 Traceroute utility 161
13.4 Tcpdump utility 161
13.4.1 Traffic capture from the active interface 161
13.4.2 Air Sniffer 161
13.4.3 Uploading the file from device to server 162
13.5 Iperf/iperf3 utility 162
13.5.1 iperf 162
13.5.2 iperf3 162
13.6 Antenna Align 163
14 List of changes 164

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.

WB-3P-PTP6 is a device designed for organizing long-distance radio bridges. A radio bridge is built using two such devices. WB-3P-PTP6 features a sealed housing designed for outdoor installation in various climatic conditions.

This user manual describes the purpose, main technical specifications, design, safe operation rules, installation and setup recommendations for the WB-3P-PTP6 wireless bridge.

1.2 Document conventions

Notes and warnings

Notes contain important information, tips, or recommendations for using and configuring the device.

Warnings inform the user about situations that may harm the device or personnel, cause improper device operation, or data loss.

2 Device description

2.1 Purpose

The WB-3P-PTP6 wireless bridge is a new-generation Wi-Fi 6 device designed to provide modern high-speed services.

With IEEE802.11ax support, the WB-3P-PTP6 wireless bridge provides data rates up to 2402 Mbps. The offset parabolic antenna makes WB-3P-PTP6 a universal solution for long-distance radio bridges.

The WB-3P-PTP6 wireless bridge (then "device") meets modern service quality requirements and allows traffic transmission in priority queues.

WB-3P-PTP6 can operate in a wide temperature range and high humidity conditions.

2.2 Device specification

Interfaces:

- 1 port of Ethernet 10/100/1000BASE-T (RJ-45) with PoE support;
- Wi-Fi 6 GHz IEEE 802.11ax.

The power is supplied via 24 V PoE injector from 220 V.

Using a PoE injector with a voltage different from 24 V will damage the device.

Functions:

WLAN capabilities:

- Support for IEEE 802.11ax;
- Data aggregation, including A-MPDU (Tx/Rx) and A-MSDU (Rx);
- WMM-based packet priority and scheduling;
- Access point mode (AP-PTP/AP-PMP);
- Client mode (STA);
- Auto-distance detection;
- Automatic transmit power control;
- Hidden SSID support;
- MAC ACL support;
- Third-party access point detection;
- APSD support;
- Channel list limiting;
- Spectrum analyzer;
- Fixed center frequency support;
- TDD support;
- Alignment.

Network features:

- automatic speed and duplex negotiation;
- VLAN support (Access, Trunk, General);
- C-VLAN configuration support;
- Management VLAN support;
- DHCP client;
- VLAN Mapping;
- Loopback Detection;
- MVR;
- NTP;

- Syslog;
- DHCP snooping;
- IGMP snooping (limit on the maximum number of groups);
- MAC Address Learning Limit;
- BPDU filtering;
- IPv6;
- LLDP;
- Ping Watchdog.

QoS functions:

- Bandwidth limiting;
- WMM parameter configuration for the radio interface;
- Prioritization support by 802.1p, DSCP and VLAN ID;
- Traffic prioritization based on MAC/IP address.

Security:

- Centralized authorization via RADIUS server (802.1X WPA3 Enterprise);
- WPA3/OWE data encryption;
- RADIUS server authorization when logging into the device;
- User authentication protection system when logging into the device.

Figure 1 shows the WB-3P-PTP6 application diagram.



Figure 1 — WB-3P-PTP6 application diagram

2.3 Main technical specifications

The main technical specifications of the device are listed in Table 1.

Table 1 – Main specifications

Ethernet interface parameters	
Number of ports	1
Electrical connector	RJ-45
Data rate	10/100/1000 Mbps, auto-negotiation
Standards	BASE-T
Wireless interface parameters	
Standards	802.11ax
Frequency range	5935–6425 MHz
Modulation	BPSK, QPSK, 16QAM, 64QAM, 256QAM, 1024QAM
Operating channels[1]	802.11ax: 1–93 (5935–6425 MHz)
Data rate[2]	802.11ax: 2402 Mbps
Maximum number of simultaneous connections	6 GHz: 64
Maximum output power of the transmitter[1]	6 GHz: 26 dBm
Receiver sensitivity	6 GHz: up to -96 dBm
Security	WPA3/OWE
Antenna parameters	
Gain	9 dBi
Polarization	linear, H/V
SWR	no more than 2
Beam width (horizontal)	65°
Beam width (vertical)	65°

Management	
Remote management	web interface, CLI, Telnet, SSH, 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	Passive PoE 24 V
Power consumption	no more than 10.5 W
Ingress protection	IP67
Operating temperature range	from -45 to +65 °C
Relative humidity at 25 °C	up to 95 %
Dimensions (W × H × D)	120 × 110 × 89 mm 120 × 110 × 144 mm (with cable gland)
Weight	0.31 kg
Service life	no less than 15 years

---

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

[2] The maximum wireless data rate is defined according to IEEE 802.11 standards. The real bandwidth can be different. Network operating conditions, environmental factors, including network traffic volume, building materials and structures, as well as network overhead data may reduce the actual bandwidth. The environment can influence the network coverage range.

2.4 Technical parameters of offset parabolic antenna

The main technical specifications of the offset parabolic antenna parameters are listed in Table 2.

Table 2 – Main specifications

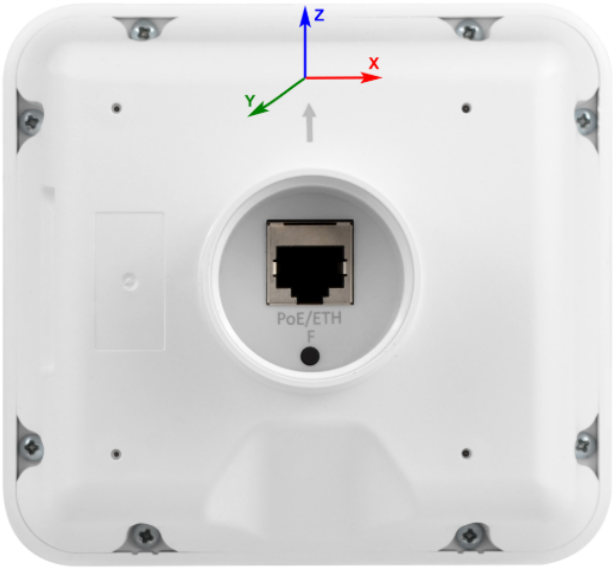
Parameters	**Antenna 450 × 495 mm**
Gain	25.5 dBi
Offset angle	24°
Polarization	linear, H/V
Radiation angle	7°
Focal distance	270 mm
Wind load	130 km/h — operating 185 km/h — limit
Reflector dimensions	450 × 495 mm
Dimensions (W × H × D)	450 × 570 × 492 mm
Weight	1.6 kg
Material	steel

2.5 Radiation patterns

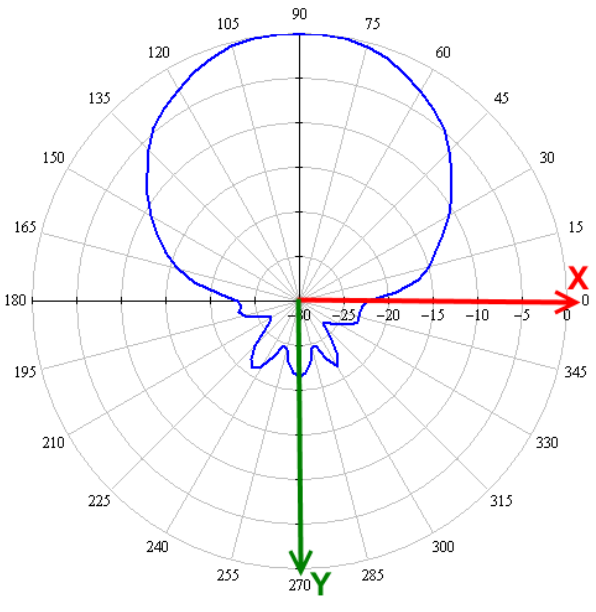
The radiation patterns of the device are shown in the figures below.

WB-3P-PTP6 radiation patterns

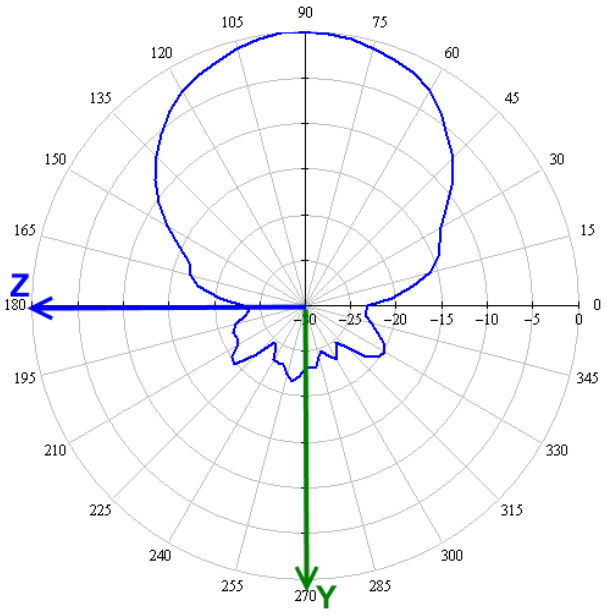
Measurement position



AZIMUTH (XY)

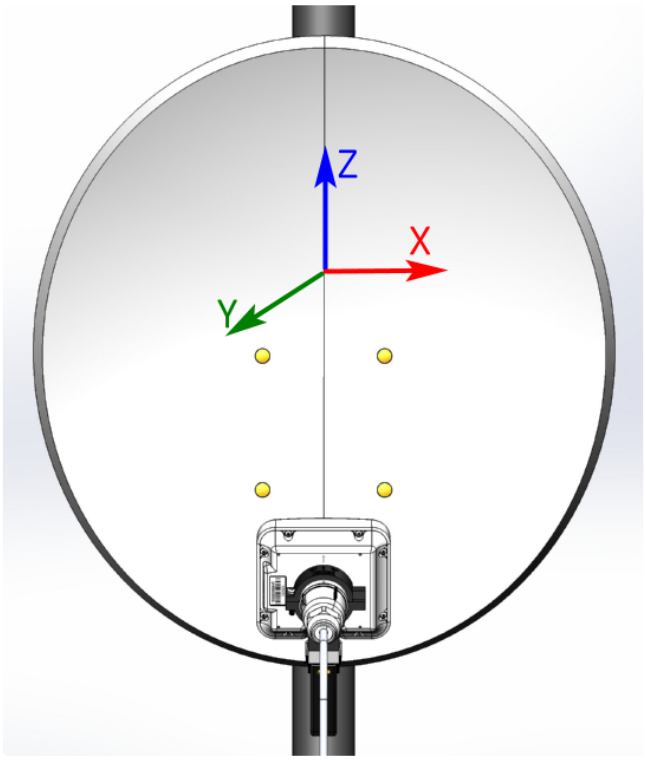


ELEVATION (YZ)

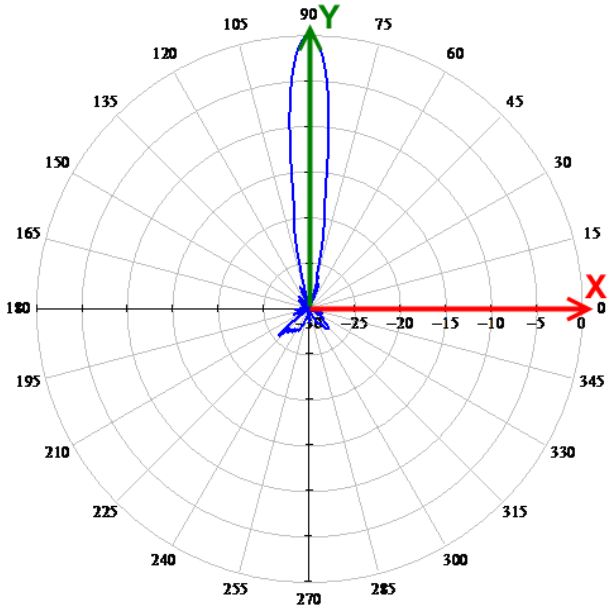


WB-3P-PTP6 radiation patterns

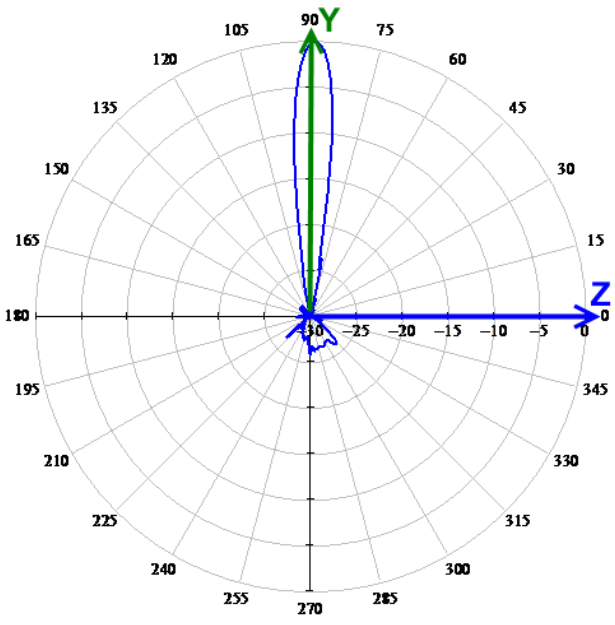
Measurement position



AZIMUTH (XY)



ELEVATION (YZ)



2.6 Design

The WB-3P-PTP6 device features a plastic housing in industrial design. The WB-3P-PTP6 main panel layout is shown in Figure 2.



Figure 2 — WB-3P-PTP6 main panel layout

The WB-3P-PTP6 rear panel is shown in Figure 3.



Figure 3 — WB-3P-PTP6 rear panel

On the WB-3P-PTP6 rear panel under the cable gland, there is a 10/100/1000BASE-T Ethernet port (RJ-45 connector) for connecting to the network and PoE power supply, as well as a factory reset button "F" (see Figure 4).



Figure 4 — RJ-45 connector and function button "F"

2.7 Light indication

The WB-3P-PTP6 indicator panel is shown in Figure 5.

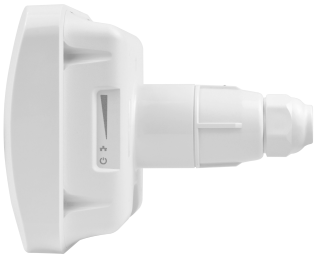


Figure 5 — WB-3P-PTP6 indicator panel

The device status is displayed by indicators on the side panel. The list of indicators and their status is provided in Table 3.

Table 3 — Light indication of device status

	Indicator / LED	Indicator status	Description
	**WLAN** — Received Signal Strength Indicators (RSSI)	solid	device is connected, signal level from the remote device is above -60 dBm
		solid	device is connected, signal level from the remote device is above -70 dBm
		solid	device is connected, signal level from the remote device is above -80 dBm
		solid	device is connected, signal level from the remote device is above -100 dBm
		none of indicators is on	no connection between devices
	**LAN** — Ethernet port indicator	solid	channel between WB-3P-PTP6 Ethernet-interface and connected device is active
		flashing	process of packet data transfer between WB-3P-PTP6 Ethernet-interface and connected device
	**Power** — power and device operation status indicator	solid	power connected, normal operation
		flashing	device did not receive an address via DHCP
		blinks frequently for 3 seconds, then solid	reboot/factory reset

2.8 Restore the default configuration

There are two ways to reset the device to factory settings.

1. Using the "F" button on the device. When the device is loaded, press and hold the "F" button (about 10–15 seconds) on the device rear panel, until all WLAN indicators start flashing.
2. Using the PoE injector, that is included into the supply package. When the device is loaded, press and hold the "RST" button on the injector (for about 10–15 seconds) until all WLAN indicators start flashing.

The device will automatically reboot. Factory settings will start DHCP client. In case the address is not received via DHCP, the device will be available at IP address — **192.168.1.10**, subnet mask — **255.255.255.0**; username/password for web interface — **admin/password**.

2.9 Supply package

The WB-3P-PTP6 basic supply package includes:

- WB-3P-PTP6 wireless bridge;
- Cable gland;
- Power injector Passive PoE 24 V;
- Power cable;
- Patch cord RJ-45, 5e cat., 1.5m;
- User manual on a CD (optional);
- Technical passport.

3 Rules and recommendations for device installation

This section describes safety instructions, installation recommendations, set-up procedure and device power-on sequence.

3.1 Safety rules

1. Do not open the device housing. There are no user-serviceable parts inside.
2. Do not install this device during a thunderstorm. There is a risk of lightning strike.
3. Voltage, current and frequency requirements specified in this manual must be observed.
4. Before connecting measuring instruments and a computer to the device, they must be grounded first. The potential difference between equipment housings and measuring instruments must not exceed 1 V.
5. Before power-on, ensure that the cables are intact and securely attached to the connectors.
6. Do not install the device near heat sources or in rooms with temperatures below -45 °or higher 65 °C.
7. When installing on elevated structures, established norms for working at height must be observed.
8. The device must be operated by engineering personnel with special training.
9. Only suitable auxiliary equipment should be connected to the device.

3.2 Installation recommendations

1. The device can be installed to the pole/post, wall, or in an offset parabolic antenna holder. The installation height should be no less than 1 meters from the supporting surface, installation distance — no more than 5 meters from the edge of the surface. If it is not possible to comply with the last condition — increase the suspension height.
2. Before installation and power-on, the device must be checked for visible mechanical damage. If damage is found, stop installation, draw up an inspection report, and contact the supplier.
3. Evaluate signal level at the receiving point using free space propagation formulas.
4. To ensure the best signal level, place the device on a post/pole so that its antenna is pointed as much as possible at the antenna of the remote device. In this case, direct visibility should be ensured between devices, and the Fresnel zone should be clear of obstacles. The highest signal level can be obtained by adjusting the antenna using RSSI indicators, web interface (more details in the Antenna Align submenu) or CLI command.
5. After alignment, ensure that the signal from the remote device is as close as possible to the calculated value as possible and not below the allowable level -65 ÷ -70 dBm.
6. If the signal exceeds -40 dBm, the remote device transmit power must be reduced.
7. When installing offset parabolic antennas, consider the antenna offset angle: so that the maximum radiation direction is parallel to the ground, the tilt angle of the parabolic antenna must equal to the offset angle.

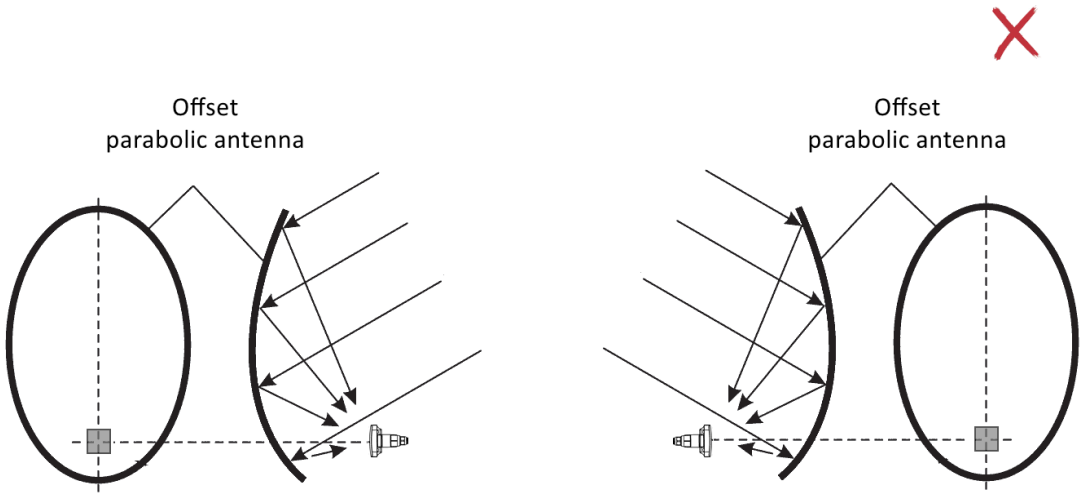


Figure 6 — Incorrect installation of offset parabolic antennas

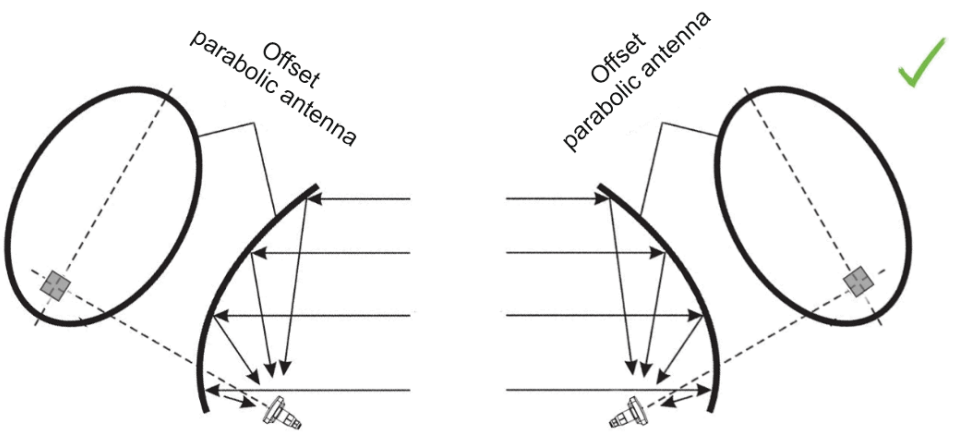


Figure 7 — Correct installation of offset parabolic antennas at the same suspension height

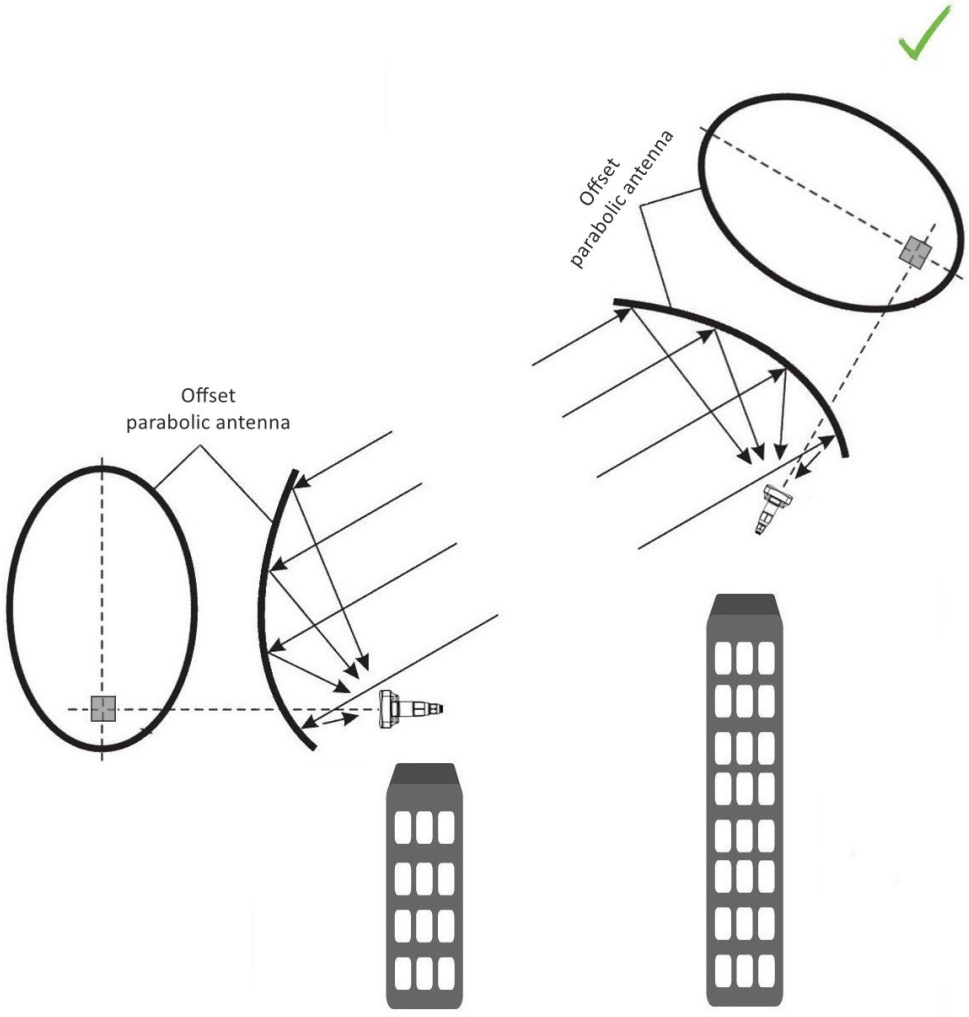


Figure 8 — Correct installation of offset parabolic antennas at different suspension heights

3.3 Recommendations for lightning protection

1. Grounding must be done using an insulated multi-core wire. The grounding device and grounding wire cross-section must comply with the Electrical Installation Code.
2. The first outdoor lightning protection must be installed as close as possible to the device, connecting with a short outdoor cable FTP-cable with shielded connectors.
3. The second outdoor lightning protection must be installed as close as possible to the PoE injector, connecting them with a short outdoor FTP-cable with shielded connectors.
4. The lightning protections are connected to each other with an outdoor FTP cable up to 100 m long.
5. The PoE injector should be connected to a 220V grounded electrical outlet.

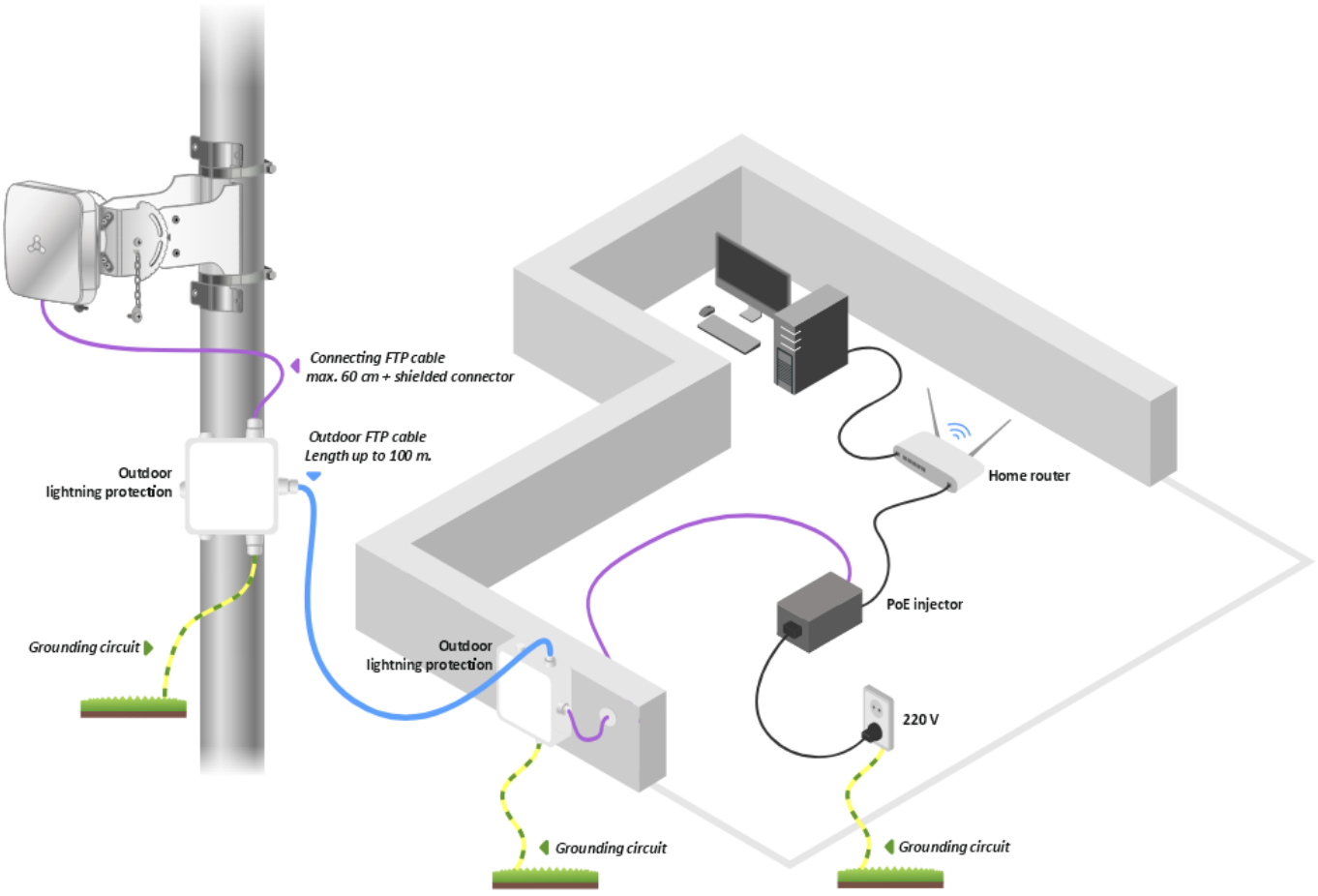


Figure 9 — Device wiring diagram for lightning protection

4 Device preparation

1. Remove the device from the package.
2. Connect the Ethernet cable to the PoE/ETH port.



Figure 10 — RJ-45 connector and "F" button

5 Device connection

1. Connect the Ethernet cable from WB-3P-PTP5 to the PoE port of the injector.



2. Connect the Ethernet cable of your network to the LAN port of the PoE injector.



3. Connect the PoE injector to a 220V outlet using the power cord. After powering on, WB-3P-PTP5 will boot up within a minute.



4. Connect to the WB-3P-PTP5 web configurator using a browser, following the instructions in the section Device management via web interface.

5. If this is the first device startup, proceed to the section Preliminary setup.

6 Preliminary setup

Perform preliminary device configuration before installation.

1. Ensure that the power is connected.
2. Follow the procedure from the section Example of device setup.

Ensure that a wireless connection is established between the devices: signal level indicators should be lit. The possible indicator states are described in the section Light indication.

7 Device installation

The WB-3P-PTP6 wireless bridge has three mounting options: on a pole/post, on a wall and as a part of an offset parabolic antenna.

7.1 Device installation on a pole/post/wall

1. Connect the device to the network and perform preliminary setup following the instructions in the section Preliminary setup. Then disconnect the device from the network and begin installation.
2. Remove the bracket, hardware kit, and clamps from the packaging.
3. Secure the bracket to the pole using a Ø60–80 clamp from the package. Final tightening of the Ø60–80 clamp is performed in step Alignment of devices mounted on a pole/post/wall. Fix the screw with the chain onto the bracket, then put the clamp Ø32–50 onto the tightening slats of the bracket. Follow the safety instructions. See Safety rules and Installation recommendations.



Figure 11 — Installing the bracket on pole

4. Disassemble the cable gland — unscrew the nut and remove the split gland from inside.

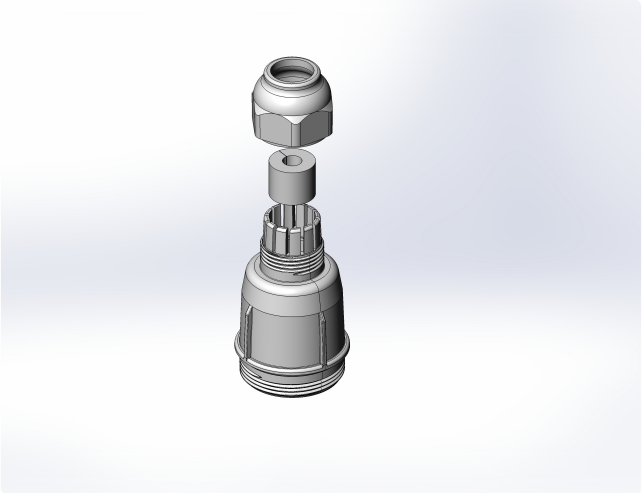


Figure 12 — Dismantling the cable gland

5. Pass the cable through the bracket and the cable gland as shown in Figure 13.

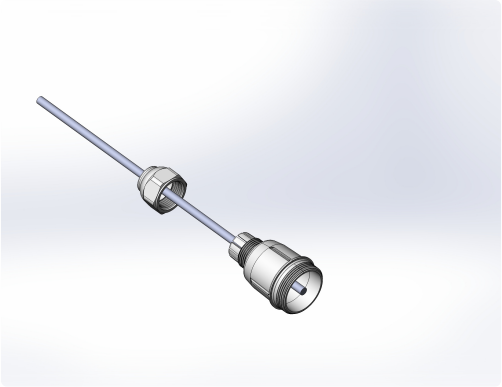


Figure 13 — Cable pulling through the cable gland

6. When installing the device with a deviation ±10 degrees, refer to Figure 14 (a). When installing the device with a deviation ±10–70 degrees, refer to Figure 14 (b).

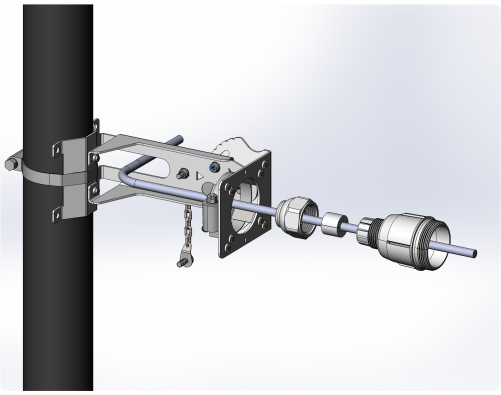


Figure 14 (a)

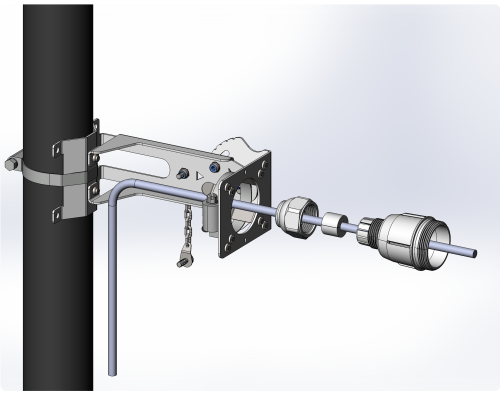


Figure 14 (b)

7. Crimp the RJ-45 connector on the cable and connect it into the mating part on the device housing.

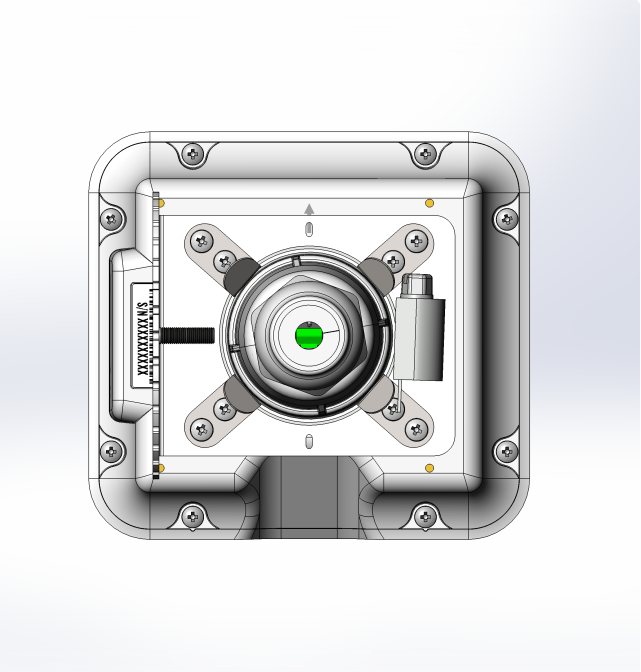


Figure 15 — RJ-45 connector on the device housing

8. Tighten the cable gland securely, place the split gland on the cable and insert it into the cable gland slats. Tighten the nut fully.

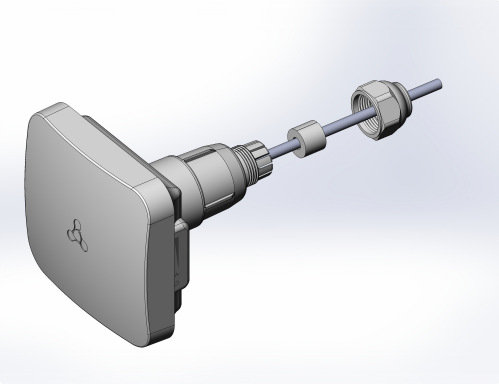


Figure 16 — Installing the cable gland

Incorrect cable gland installation may compromise device sealing.

9. Insert the device into the bracket slats. Adjust the device by aligning the arrow on the housing with the hole in the bracket, then tighten the clamp Ø32–50.

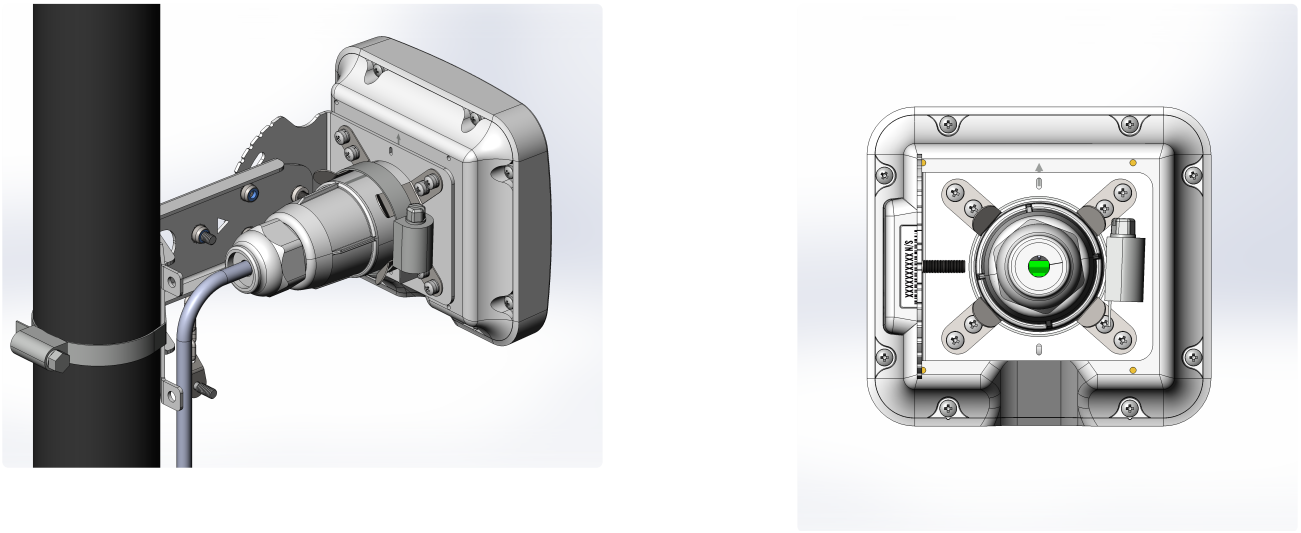


Figure 17 — Installing the device into the bracket

10. After installation, rotate the device to the required angle using the scale on the bracket as a reference. Tilt angle varies from -70 to 70 degrees.

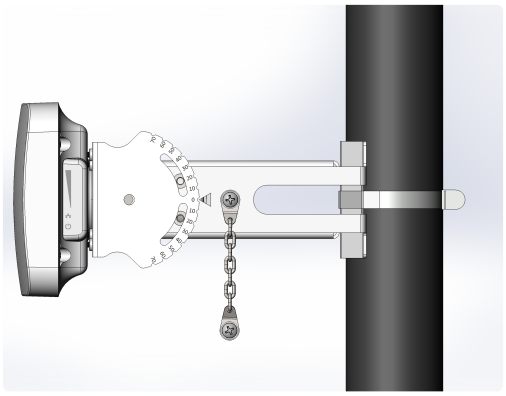


Figure 18 — Setting the required tilt angle

11. The bracket can also be installed on a wall. When installing on a wall, use screws or self-tapping screws 4×40 mm, if necessary — 6×40 mm dowels (Figure 19).

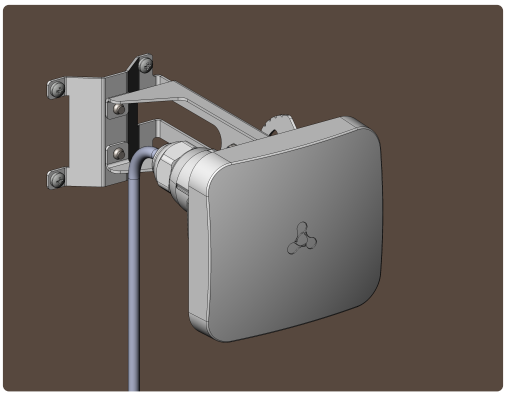


Figure 19 — Installing the device on a wall

12. Connect the device to the network following the procedures in the sections Device preparation and Device connection. Then proceed to device alignment.

Lightning protection is recommended to prevent device failure.

7.2 Installation of the device as part of an offset parabolic antenna

Supply package:

- WB-3P-PTP6 basic supply package;
- Offset parabolic antenna with mounting kit.

To install the device in an offset parabolic antenna, perform the following steps:

1. Connect the device to the network and perform preliminary setup following the instructions in the section Preliminary setup. Then disconnect the device from the network and begin installation.

2. Assemble the device holder by inserting the upper part shaft into the lower part slots. On the right side of the holder, install an M4×20 screw with a nut.

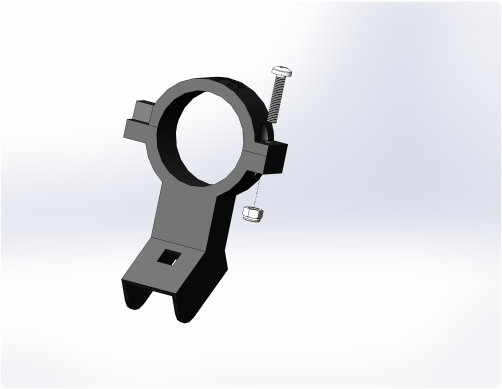


Figure 20 — Assembling the device holder

3. Attach the holder and the movable part of the bracket to the arc using M6×30 bolts, bracket and nuts from the mounting kit. Install a plug on the upper end of the arc.

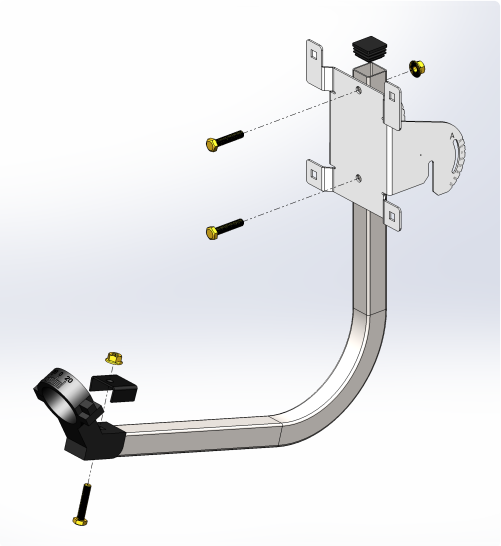


Figure 21 — Attaching the holder and movable bracket part to the arc

4. Connect the movable bracket part and antenna reflector using M6×12 bolts and nuts.

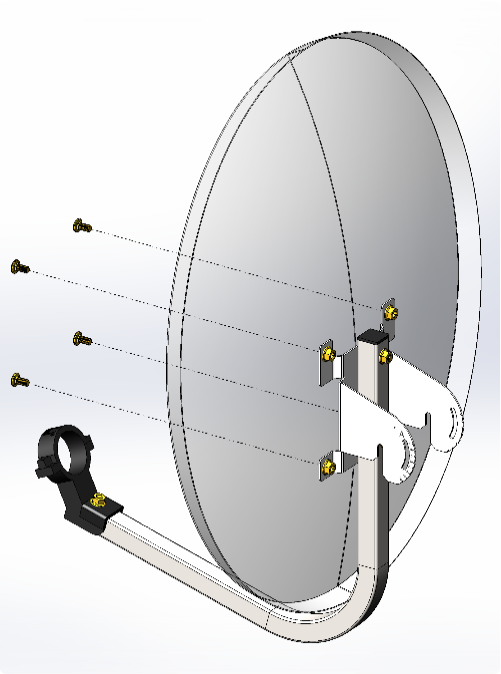


Figure 22 — Attaching the antenna reflector to the movable bracket part

5. Disassemble the cable gland — unscrew the nut and remove the split gland from inside.

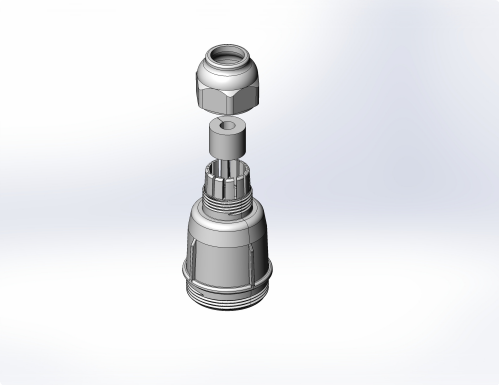


Figure 23 — Dismantling cable gland

6. Pass the cable through the holder and the cable gland.

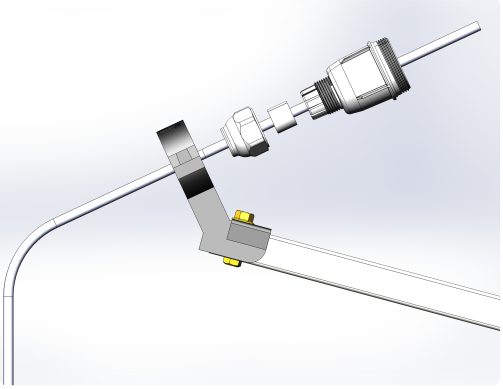


Figure 24 — Cable pulling through the holder and cable gland

7. Crimp the connector RJ-45 on the cable and connect it into the mating part on the device housing.

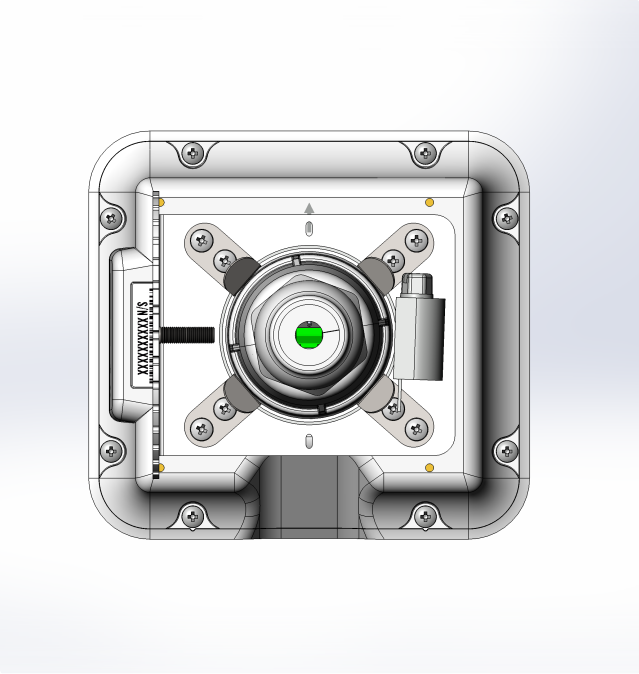


Figure 25 — Connector RJ-45 on the device housing

8. Tighten the cable gland securely, place the split gland on the cable and insert it into the cable gland slats. Tighten the nut fully.

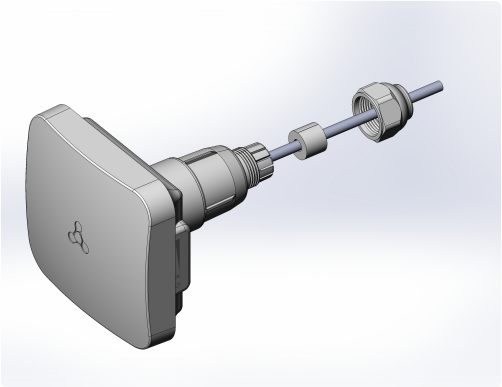


Figure 26 — Installing the cable gland

Incorrect cable gland installation may compromise device sealing.

9. Install the device in the holder and adjust the device to 0°, using the scale on the holder. Tighten the screw on the holder after adjustment.



Figure 27 — Installing the device into the holder

10. Place the fixed part of the bracket on the pole as shown in Figure 28 and secure it with the clamps supplied with the device. The final tightening of the clamps is performed in Alignment of devices mounted on an offset parabolic antenna section. Install the chains; do not tighten the chain screws tightly, leaving a gap for installing the movable part of the bracket. Follow the instructions given in the sections Safety rules and Installation recommendations.

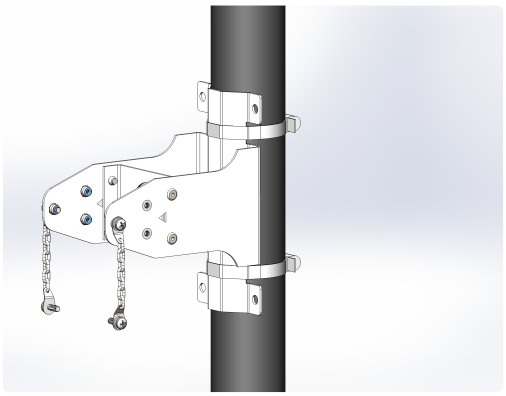


Figure 28 — Installing the fixed part of the bracket

11. Mount the reflector onto the fixed bracket. When installing, the previously under-tightened screws must engage the grooves of the movable bracket part.

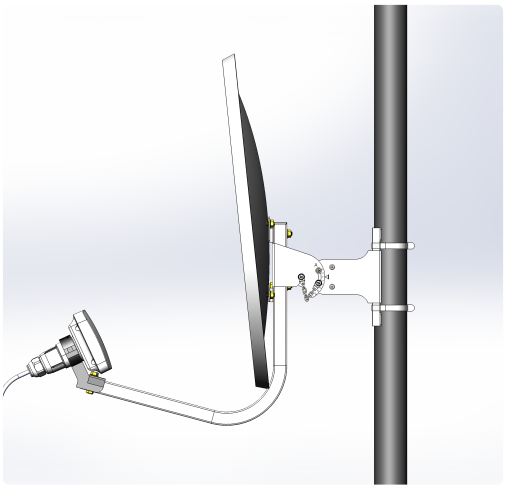


Figure 29 — Mounting the reflector onto the fixed bracket

12. If needed, the parabolic antenna can be mounted on a wall, for example using M6 bolts.

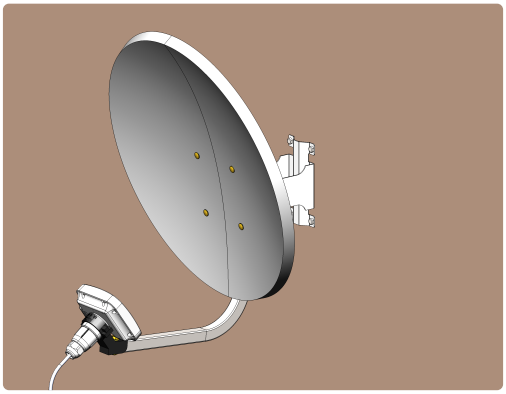


Figure 30 — Wall mounting of the parabolic antenna

13. Connect the device to the network following the procedures in the sections Device preparation and Device connection. Then proceed to device alignment.

8 Device alignment

First, the horizontal alignment of the device is performed, then the vertical one.

8.1 Alignment of devices mounted on a pole/post/wall

1. Always perform alignment sequentially from both sides, using the calculated signal level obtained in the section Installation recommendations (it is necessary to obtain the closest possible value).

2. Adjust device positions by directing antennas approximately at each other, using maps and visual line of sight (for example, using binoculars) to the remote side.

With default settings, the client (STA) does not send a connection request, therefore, to establish a connection, first direct the access point (AP) to the client (STA).

3. When establishing a connection between devices, align them sequentially, gradually increasing the values on the RSSI scale (indicator values are provided in section Light indication) in two planes — vertical and horizontal.

4. In the horizontal plane, one side covers a sector of 45–60 degrees — fixes the maximum, the second side performs a similar action.

5. Next, perform the second pass according to the above scheme. Finally tighten the clamp on the bracket. It is necessary to take into account that during alignment, hitting the side lobe of the radiation pattern may be interpreted as reaching the maximum signal level. To avoid this situation, it is necessary to perform a full pass in the sector and note any nonlinear level changes.

6. Repeat steps 4–5 in the vertical plane. Fix the resulting tilt angle using screws on the chain.

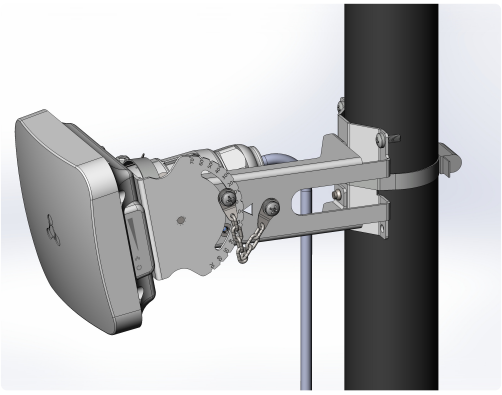


Figure 31 — Setting the required tilt angle

7. For more precise alignment, use the command in CLI or web interface (more details in the "Antenna Align" submenu), achieving maximum signal level values.

8.2 Alignment of devices mounted on an offset parabolic antenna

1. Always perform alignment sequentially from both sides, using the calculated signal level obtained in the section Installation recommendations (it is necessary to obtain the closest possible value).

2. Adjust device positions by pointing antennas approximately at each other, using maps and visual line of sight (for example, using binoculars) to the remote side.

With default settings, the client (STA) does not send a connection request, therefore, to establish a connection, first direct the access point (AP) to the client (STA).

3. When establishing a connection between devices, align them sequentially, gradually increasing the values on the scale RSSI (indicator values are provided in section Light indication) in two planes — vertical and horizontal.

4. In in the horizontal plane, one side covers a 30° sector 45–60 degrees — fixes the maximum, the second side — performs a similar action.

5. Then a second pass is performed following the scheme described above. Fully tighten the clamps on the fixed part of the bracket. Note that during alignment, entering a side lobe of the radiation pattern may be interpreted as reaching the maximum signal level. To avoid this, perform a full sweep across the sector and note nonlinear signal level changes.

6. Repeat the steps in the vertical plane 4–5: Rotate the device to the required angle using scales A and B on the bracket as references. Scale A — tilt angle of the parabolic antenna, scale B — elevation angle. Then secure the obtained tilt angle using the screw on the chain.

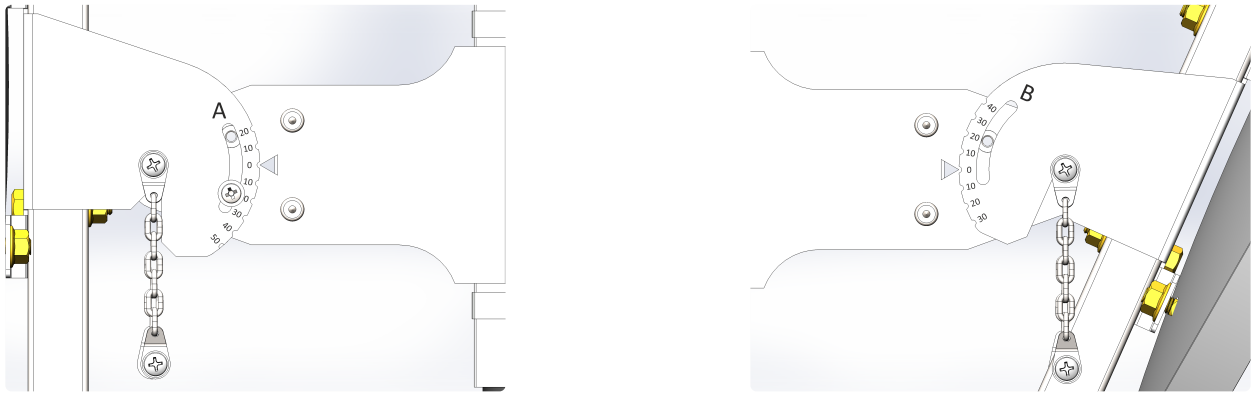


Figure 32 — "A" and "B" scales on the movable part of the bracket

7. When setting the angle on the "A" scale from -10 to 5 degrees, it is recommended to additionally fix the movable part of the bracket with a second screw from the kit.

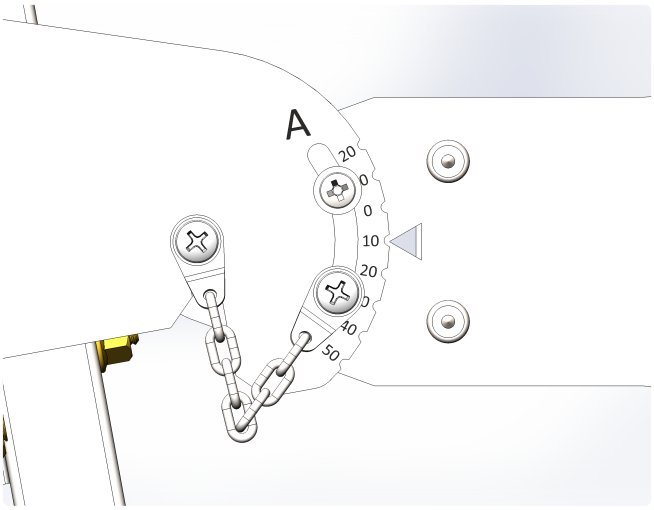


Figure 33 — Additional fixation of the bracket movable part

8. For more precise alignment, use the command in CLI or web interface (more details in the "Antenna Align" submenu), achieving maximum signal level values.

9 Final device setup

1. It is recommended to select and set a static modulation on this and the remote devices. To select a static modulation, run a continuous ping to the devices. Then, in the "Monitoring" menu, under "Wireless Peer"/"Wireless Clients," note the automatically set modulation and set it statically in the channel transmission rate settings in the "Radio" menu. For reliability, you can set the modulation a couple of points lower than the automatic setting.
2. Scan the environment with a spectrum analyzer and select the least congested channel.
3. Set the final channel in the "Radio" menu.

10 Device management via web interface

10.1 Getting started

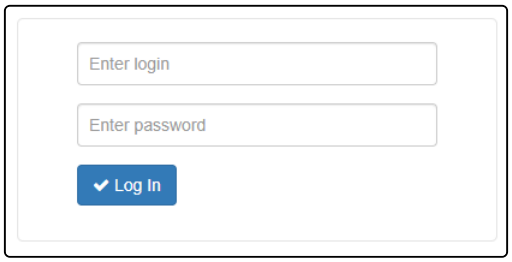
To begin, connect to the device via the Ethernet interface using a web browser:

1. Open web browser (a program for viewing hypertext documents), 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.

After three unsuccessful attempts to enter the login and password, access to the account for this user will be blocked for 60 seconds.

Upon successful device detection, the browser displays a username and password login page.

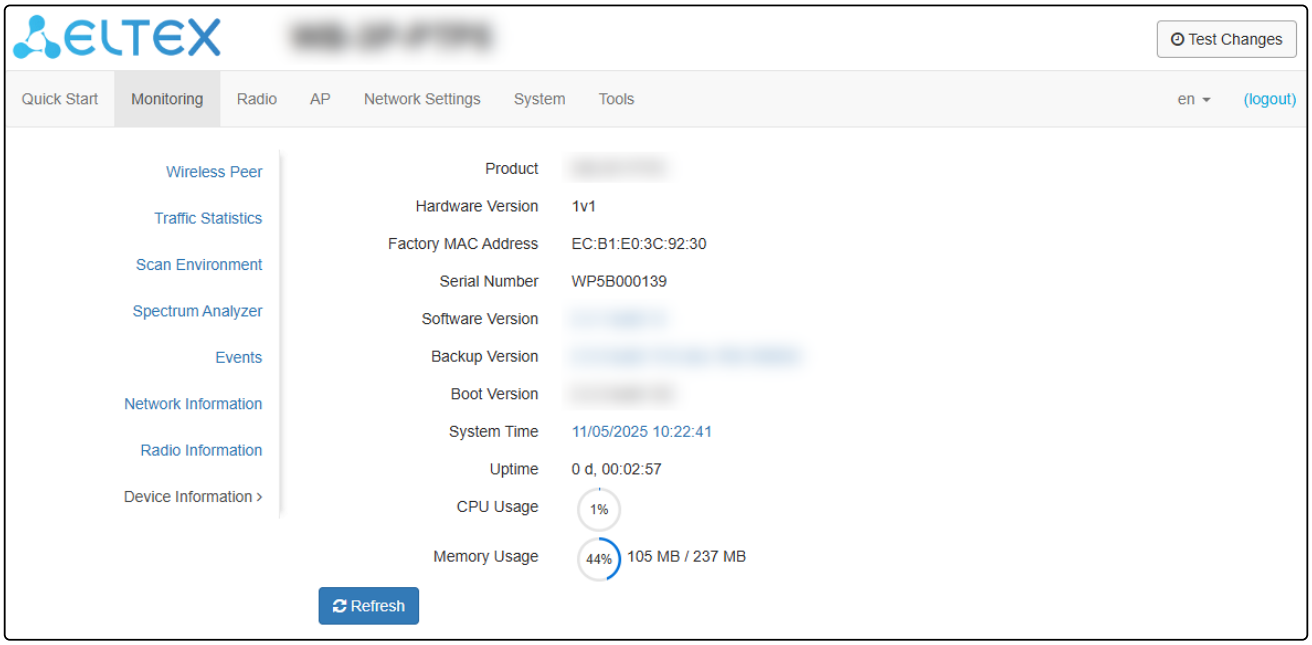


3. Enter the username in the field "Enter Login" and password in the line "Enter Password".

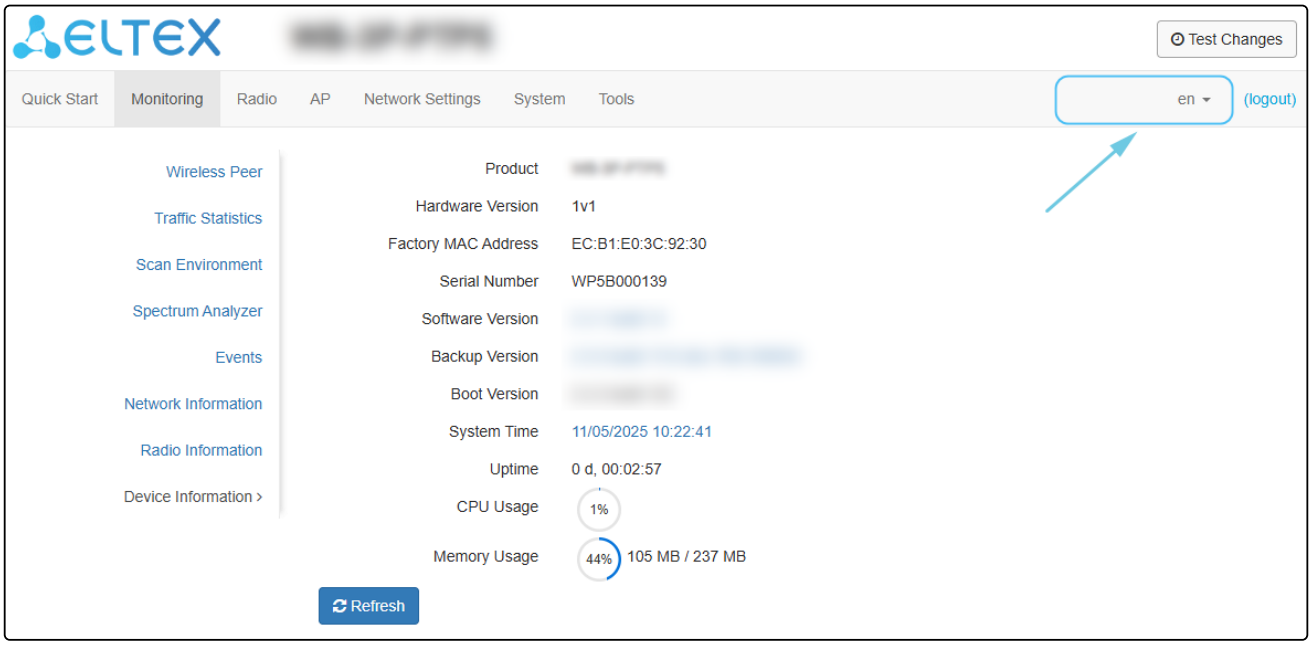
Factory settings: login: **admin**, password: **password**.

After three unsuccessful attempts to enter the username and password, access to the account for this user will be blocked for 60 seconds.

4. Click "Log In". The device status monitoring menu opens in the browser window.



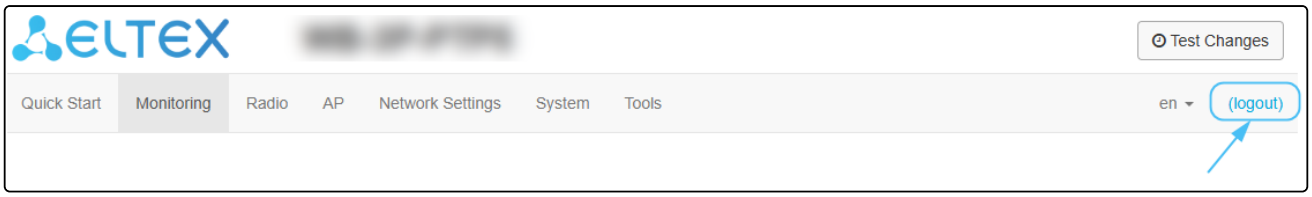
5. If necessary, select the information display language.



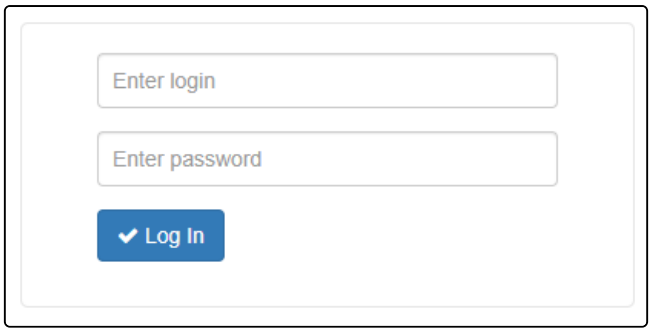
10.2 User change

The device has two types of users: **admin** and **viewer**:

- **admin** (password by default: **password**) has full access to the device: read and write any settings, full device status monitoring.
- **viewer** has read-only access to the entire device configuration with no editing capability; full device monitoring is available.



If to click the "Logout" button, the current user session will be terminated and the authorization window will be displayed:



To change access, specify the appropriate username and password, click the button "Log In".

10.3 Applying configuration and discarding changes

1. Applying configuration

When pressing the button 

the process of saving the configuration to flash-device memory and application of new settings. All settings take effect without a device reboot.

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

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

Appearance	Status description
	After clicking "Apply", the process of settings saving to device memory is launched. This is indicated by the icon  in the tab name and on the "Apply" button.
	The successful save and application of settings is indicated by the icon  in the tab name.

2. Cancel changes

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

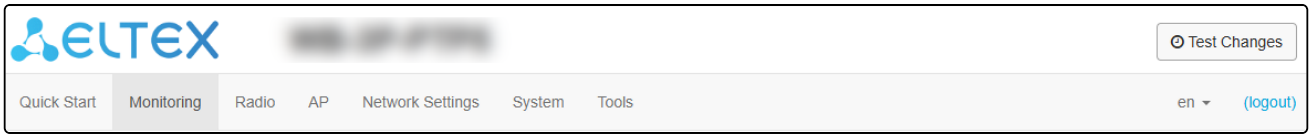
The button for discarding changes appears as follows: 

.

10.4 Test mode

The device has a test mode for testing configurations.

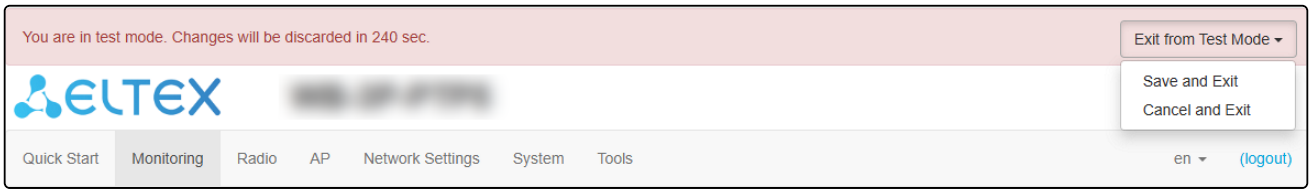
To activate it, click the "Test Mode" button in the top panel of the web interface.



The test mode runs for 300 seconds (5 minutes). During this time, you can navigate the web configurator tabs and make any changes, applying them on each page using the "Apply" button.



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

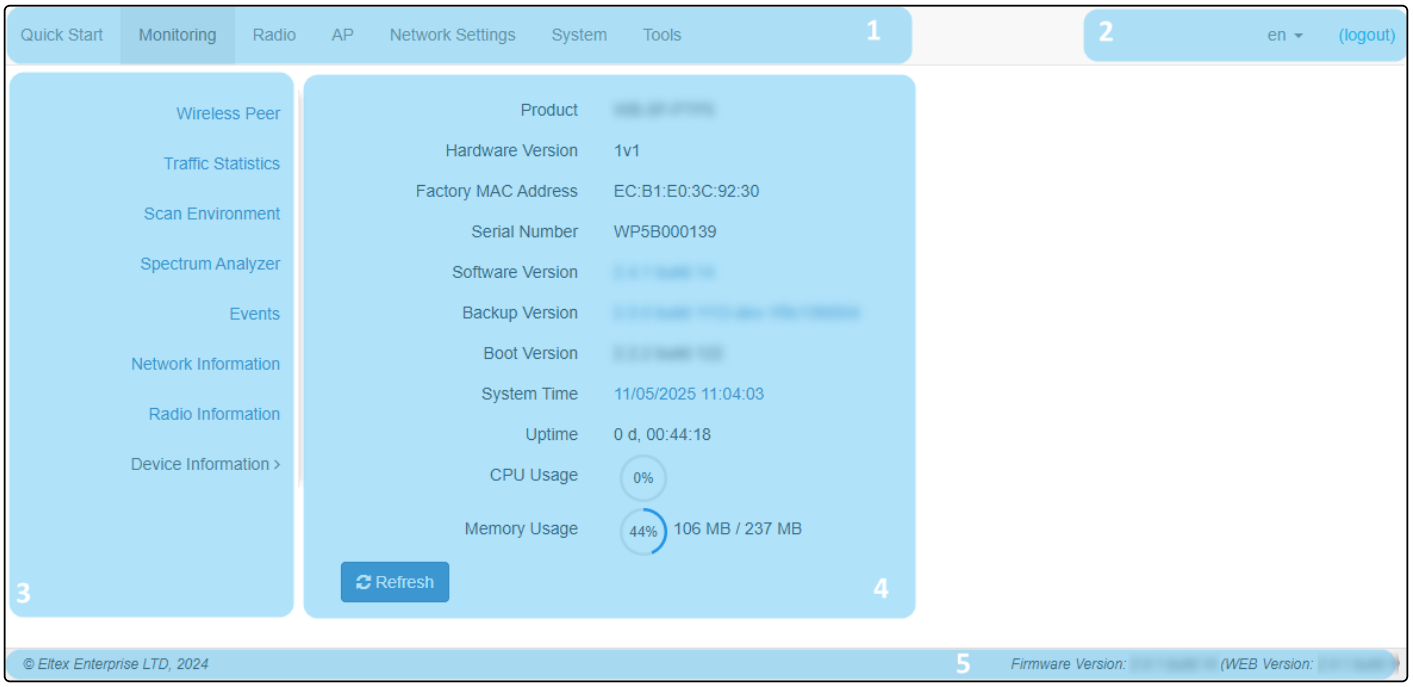


- "Save and Exit" — when pressed, the device will exit test mode and save all configuration changes made and applied in this mode to non-volatile memory. It will be impossible to cancel the changes made in test mode.
- "Cancel and Exit" — when pressed, the device will exit test mode and discard all changes made in this mode. The configuration that was active on the device before enabling test mode will be restored.

If the administrator does not exit test mode within 300 seconds, this will happen automatically, and all changes made in that mode will be undone. After the specified time expires, the configuration will be restored, even if the access to the device was lost as a result of these actions.

10.5 Web interface basic elements

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



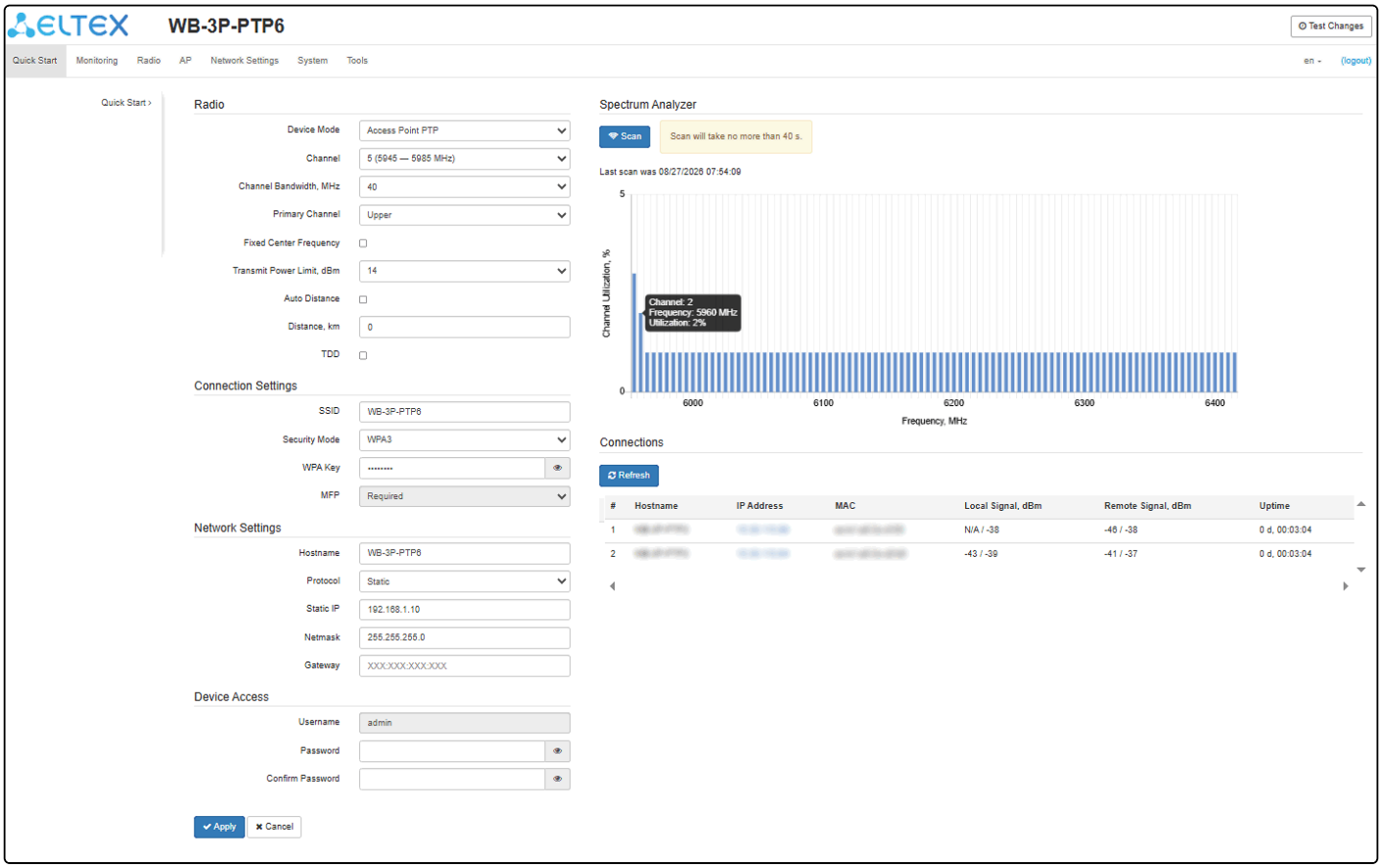
The user interface window is divided into five areas:

1. Menu tabs for grouping submenus by categories: **Quick Start, Monitoring, Radio, AP ("AP" menu available only in device mode "Access Point PTP" or "Access Point PMP") or STA ("STA" menu available only in device mode "Station / Client"), Network Settings, System, Tools.**
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.

10.6 "Quick Start" menu

In the **"Quick Start"** menu, the basic configuration of the device is performed**.**

10.6.1 "Quick Start" submenu



Radio

The **"Radio"** section configures the main device radio interface parameters.

- *Device Mode* — device radio interface operating mode. The following modes are available:
  - *Access Point PTP* — Point-to-Point;
  - *Access Point PMP* — Point-to-Multipoint;
  - *Station* — wireless client (STA).
- *Channel* — data channel selection. If the "Auto Channel" is checked in the Radio menu, this setting will be locked;
- *Channel Bandwidth, MHz* — channel bandwidth on which the device operates; accepts values 20, 40, 80 and 160 MHz;
- *Primary Channel* — this parameter can only be changed when the statically set channel bandwidth equals to 40 MHz. The 40 MHz channel can be considered as consisting of two adjacent 20 MHz channels. These two 20 MHz channels are called primary and secondary channels:
  - *Upper* — primary channel will be the upper 20 MHz channel in the 40 MHz band;
  - *Lower* — primary channel will be the lower 20 MHz channel in the 40 MHz band.

- *Fixed Center Frequency* — when checked, all traffic (data and control packets) will be transmitted on the specified channel center frequency with the specified bandwidth (40/80/160 MHz). The function is proprietary, the transmission is not carried out according to IEEE 802.11 standards, which assume the use of different center frequencies for data and control traffic with a channel bandwidth of 40/80/160 MHz;
- *Transmit Power Limit, dBm* — Wi-Fi transmitter signal power adjustment in dBm;
- *Auto Distance* — when this option is enabled, the device will automatically detect and configure the distance between devices;
- *Distance, km* — distance between devices in kilometers. Changing the distance value will change the ACK timeout value. The distance should be rounded up. For example, if the distance between devices is 3.2 km, then 4 km should be specified;
- *TDD* — when checked, the option is enabled; otherwise, it is disabled. TDD is a collision-free time-division multiplexing (TDD) technology that synchronizes data transmission in both directions within a time frame.

The "Channel", "Channel Bandwidth", "Primary Channel" parameters are only available when the device mode is "Access Point PTP" or "Access Point PMP".

Connection Settings:

- *SSID* — virtual wireless network name;
- *Security Mode* — wireless network access security mode:
  - *OWE (Opportunistic Wireless Encryption)* — encryption method that provides the security of data transmitted over an unsecured network. In this case, users do not need to do any additional actions and enter a password to connect to the network;
  - *WPA3* — encryption methods, the selection of which makes the following settings available:
    - *WPA key* — key/password required to connect to the wireless network. The key length is from 8 to 63 characters.
  - *MFP* — management frame protection (available for WPA3, OWE security modes). When selecting the WPA3 and OWE security mode, MFP is set to Required:
    - *Required* — management frame protection is enabled. The device cannot connect to a wireless network that does not support MFP.

Network Settings:

- *Hostname* — network name of the device, a string of 1–63 characters is specified: Latin uppercase and lowercase letters, digits, the hyphen sign "-" (the hyphen cannot be the last character in the name);
- *Protocol* — protocol used to connect the device via Ethernet interface to service provider network:
  - *DHCP* — operating mode in which IP address, subnet mask, DNS server address, default gateway and other parameters required for operation in the network are obtained from DHCP server automatically;
  - *Static* — operating mode in which IP address and all the necessary parameters for WAN interface are assigned statically. If "Static" is selected, the following parameters will be available to set:
    - *Static IP* — device WAN interface IP address in the provider network;
    - *Netmask* — external subnet mask;
    - *Gateway* — address to which the packet is sent if the route in routing table is not found for it.

Device Access:

The **"Device Access"** section is used to change the password.

When Logging In via web interface, administrator (password by default: password) has full access to the device: read and write access to any settings, full device status monitoring. To change the password, enter a new password first in the field "Password", then in the field "Confirm Password" and click the button "Apply" to save the new password.

Spectrum Analyzer:

The **"Spectrum Analyzer"** section is used to launch and monitor the spectrum analyzer.

The WB-3P-PTP6 devices can launch the spectrum analyzer on the Radio 6 GHz.

When the spectrum analyzer is launched, the radio interface will be switched to scanning mode, which will interrupt all Wi-Fi connections on this radio interface.

To start the spectrum analyzer, click the "Scan" button. The information window located to the right of the button displays the time in seconds that has passed since the start of the scan. The scan on the Radio 6 GHz will take no more than 1 minutes.

- *Last scan was...* — date and time of the last scan;
- *Channel Utilization* — information about the radio channel congestion, expressed as a percentage;
- *Frequency* — channel frequency, on which scanning was performed, MHz;
- *Channel* — channel number corresponding to a given frequency.

The spectrum analyzer analyzes all channels in the range, regardless of the settings on the radio interface.

Connections:

The **"Connections"** section displays information about the status of connected devices.

- *#* — number of the connected device in the list;
- *Hostname* — network device name;
- *IP Address* — IP address of the connected device;
- *MAC* — MAC address of the connected device;
- *Local Signal, dBm* — received signal level, dBm;
- *Remote Signal, dBm* — received signal level of the remote device, dBm;
- *Uptime* — connection time.

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

10.7 "Monitoring" menu

In the **"Monitoring"** menu the current system state is displayed.

10.7.1 "Wireless Peer/Wireless Clients" submenu

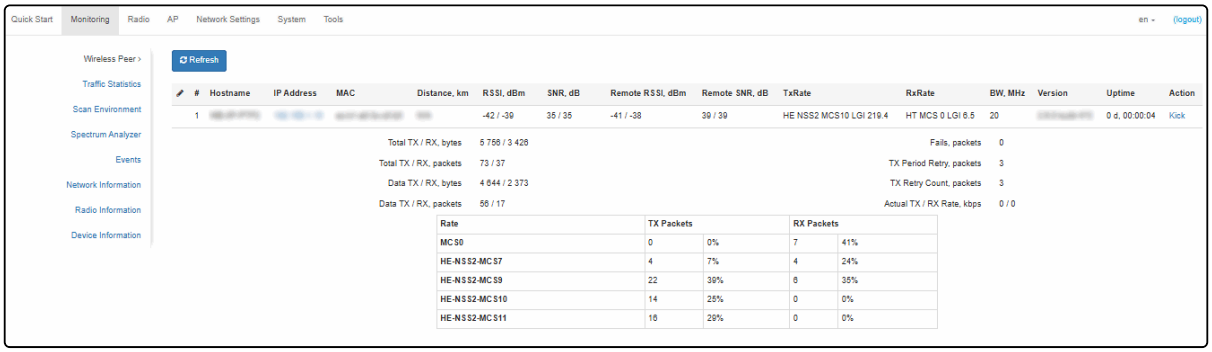
The **"Wireless Peer"/"Wireless Clients"** displays information about connected device status. Information about connected devices is not displayed in real time. To update the information on the page, click the "Refresh" button.

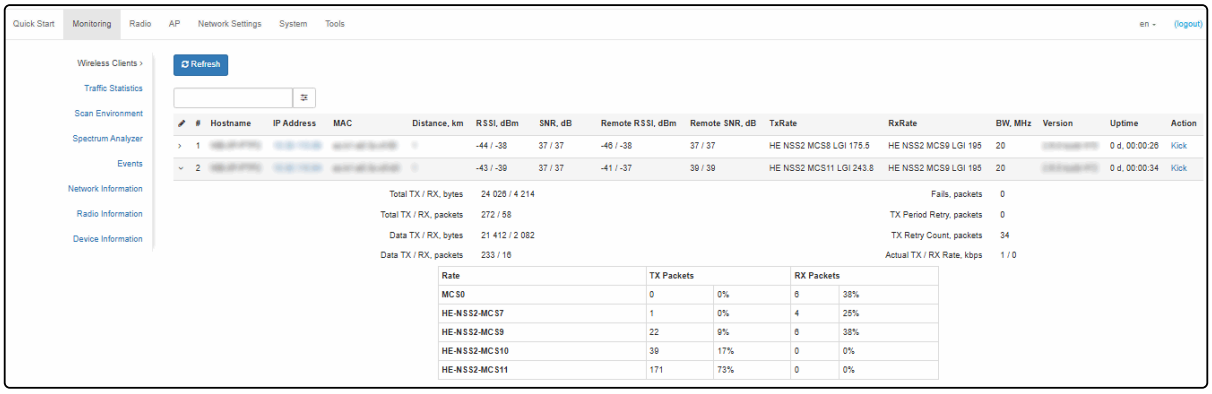
Depending on the mode devices, "Access Point PTP" or "Access Point PMP", the **"Wireless Peer"** or **"Wireless Clients"** submenu will be available respectively.

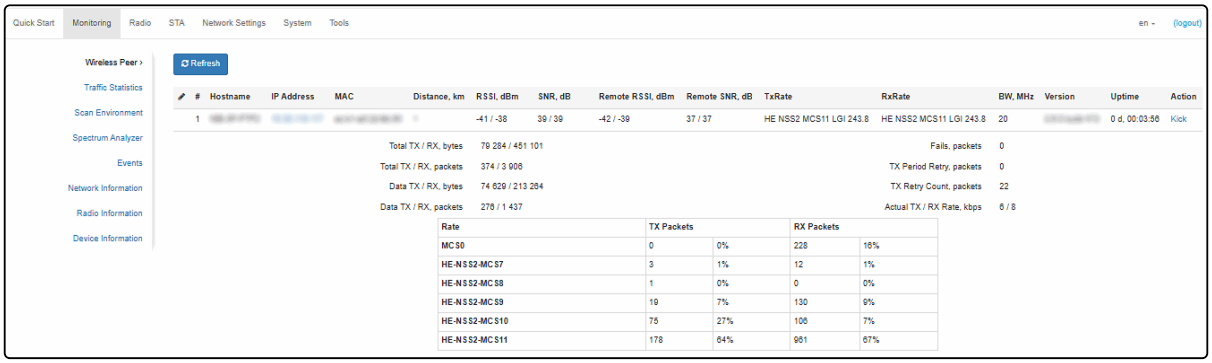
For easy monitoring, it is possible to select the parameters to display. To do this, click . When pressing "By default" button default parameters will be displayed.
The following filters are available for searching connected devices: by all fields, by hostname, by IP Address, by MAC. To select a filter, click . The feature is available only in "Access Point PMP" device mode.

If the Link Quality, Link Quality Common, Link Capacity, RSSI and Remote RSSI values are highlighted in orange, the connection quality is deteriorating. If the values are highlighted in red, this indicates a significant deterioration in the connection. It is recommended to take measures to improve the connection conditions.

Below are examples of the **"Wireless Peer"/"Wireless Clients"** submenus in the "Access Point PTP", "Access Point PMP", and "STA" device modes, respectively.



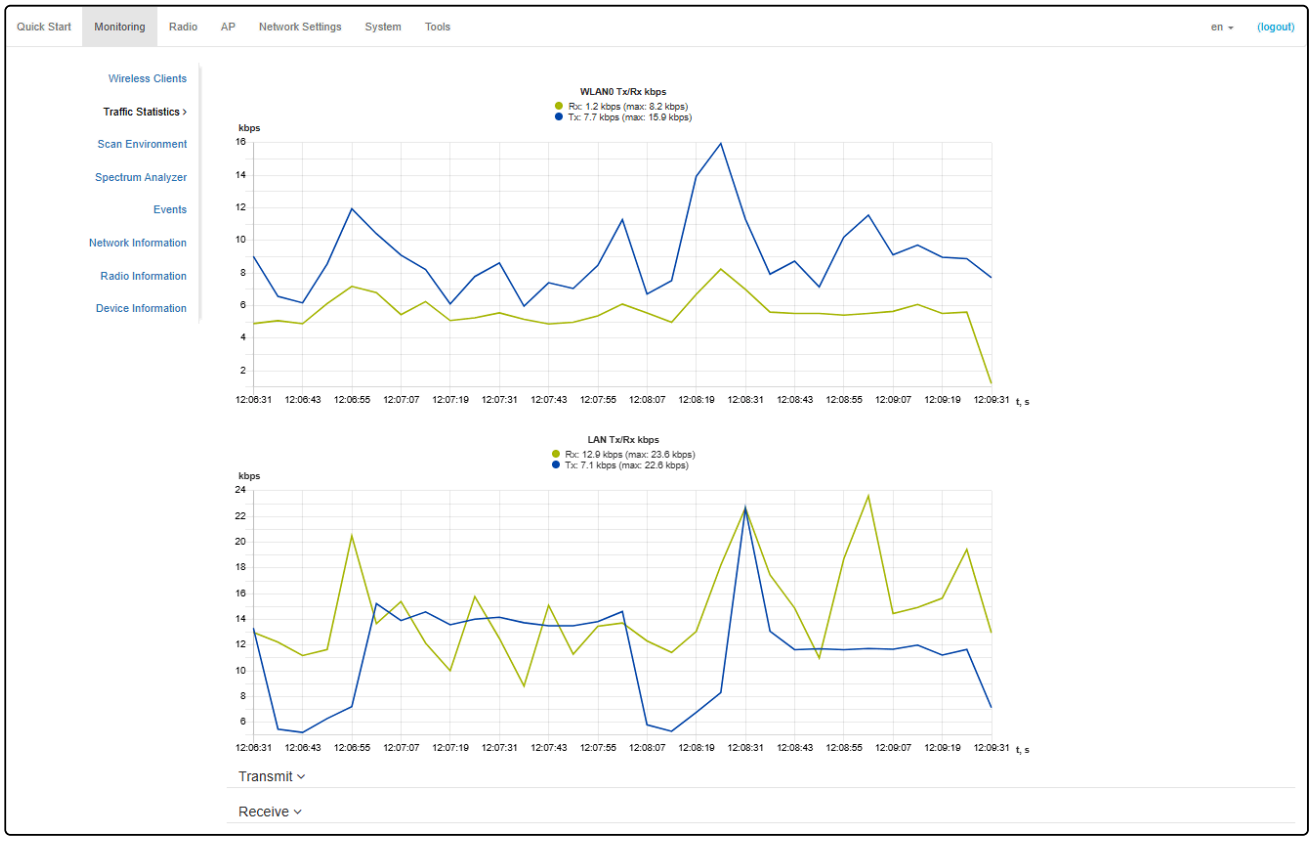




- *#* — number of the connected device in the list;
- *Hostname* — device network name;
- *IP Address* — IP Address of the connected device;
- *MAC* — MAC of the connected device;
- *Distance* — distance to the remote device, km;
- *Link Capacity* — parameter that displays the efficiency of modulation on the transmission used by the device. It is calculated based on the number of packets transmitted to the remote device on each modulation, and the reduction factors. The maximum value is 100% (meaning that all packets are transmitted to the remote device at maximum modulation for the maximum Nss type supported by a remote device). The minimum value is 2% (in the case when the packets are transmitted on the modulation Nss1MCS0 for a remote device with MIMO 3×3 support). The parameter value is calculated for the last 10 seconds;
- *Link Quality* — parameter that displays the status of the link to a remote device, calculated based on the number of retransmit packets sent to the remote device. 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 remote device). The parameter value is calculated for the last 10 seconds;
- *Link Quality Common* — parameter that displays the status of the link to a remote device, calculated based on the number of retransmit packets sent to the remote device. 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 remote device). The parameter value is calculated for the entire remote device connection time;
- *RSSI* — received signal level, dBm;
- *SNR* — signal-to-noise ratio, dB;
- *Remote RSSI* — received signal level of a remote device, dBm;
- *Remote SNR* — signal-to-noise ratio of a remote device, dB;
- *TxRate* — channel data transfer rate, Mbps;
- *RxRate* — channel data reception rate, Mbps;
- *BW* — transmission bandwidth of the wireless channel, MHz;
- *Actual TX Rate* — average data transfer rate over the last 10 seconds, Mbit/s;
- *Actual RX Rate* — average data reception rate over the last 10 seconds, Mbit/s;
- *Version* — firmware version of the connected device;
- *Uptime* — connection time;
- *Action* — if to press "Kick" button, the connection with the connected device will be broken. After disconnecting, the device will reconnect;
- *Total TX/RX, bytes* — number of bytes sent/received on the connected device;
- *Total TX/RX, packets* — number of packets sent/received on the connected device;
- *Data TX/RX, bytes* — number of data bytes sent/received on the connected device;
- *Data TX/RX, packets* — number of data packets sent/received on the connected device;
- *Fails, packets* — number of packets sent with errors on the connected device;
- *TX Period Retry, packets* — number of transmission retries to the connected device in the last 10 seconds;
- *TX Retry Count, packets* — number of transmission retries to the connected device during the entire connection;
- *Actual TX/RX Rate, Kbps* — current traffic transmission rate at the moment.

10.7.2 "Traffic Statistics" submenu

The **"Traffic Statistics"** submenu displays traffic reception/transmission rate graphs for the last 3 minutes, as well as information on the amount of transmitted/received traffic since the device was turned on.

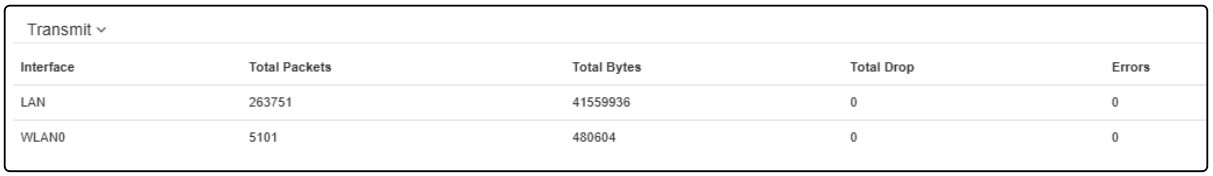


The LAN Tx/Rx graph shows the rate of the transmitted/received traffic via Ethernet interface of the device for the last 3 minutes. The graph is automatically updated every 6 seconds.

The WLAN0 Tx/Rx graph shows the rate of transmitted/received traffic via Radio interface of the device 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.

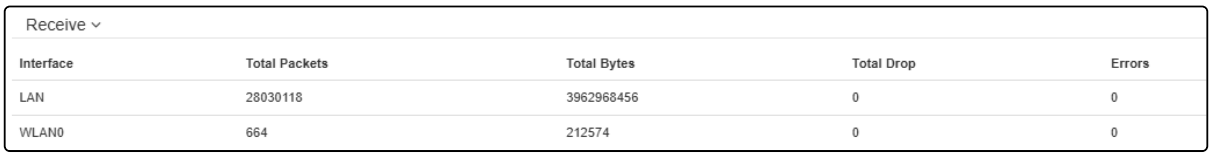


Transmit

Interface	Total Packets	Total Bytes	Total Drop	Errors
LAN	263751	41559936	0	0
WLAN0	5101	480604	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.

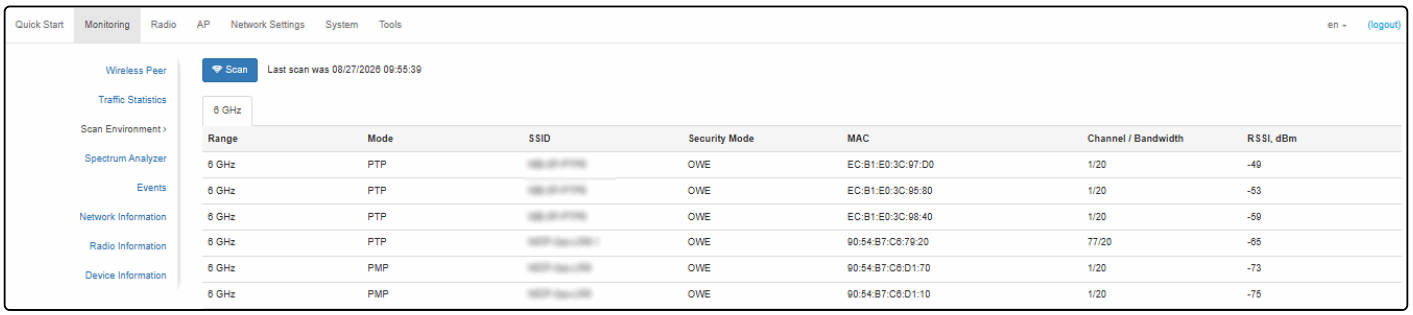


Receive

Interface	Total Packets	Total Bytes	Total Drop	Errors
LAN	28030118	3962968456	0	0
WLAN0	664	212574	0	0

10.7.3 "Scan Environment" submenu

In the "**Scan Environment**" submenu, air scanning and detection of neighboring devices are carried out.



To start the scanning process, click the "Scan" button. After scanning is complete, a list of detected devices and information about them will appear:

- *Last scan was...* — date and time of the last scan;
- *Range* — specifies the 6 GHz range, in which the device was detected;
- *Mode* — device radio interface operating mode;
- *SSID* — SSID of the detected device;
- *Security mode* — security mode of the detected device;
- *MAC* — MAC address of the detected device;
- *Channel/Bandwidth* — radio channel on which the detected device operates;
- *RSSI* — level with which the device receives the signal of the detected device, 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.

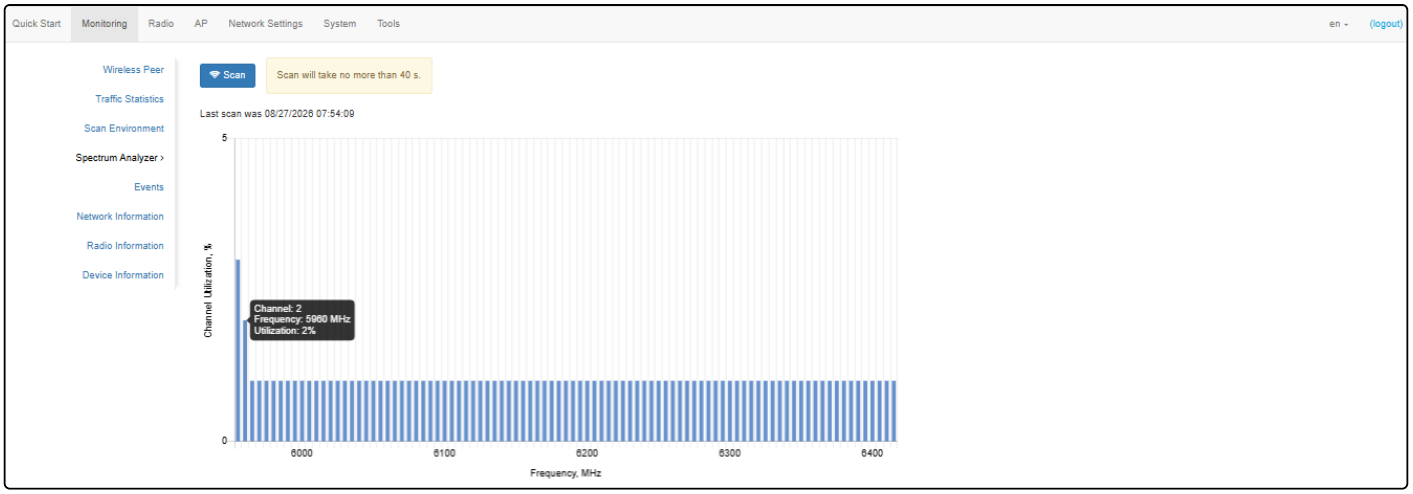
10.7.4 "Spectrum Analyzer" **submenu**

The **"Spectrum Analyzer"** submenu is used to launch and monitor the spectrum analyzer.

On the WB-3P-PTP6 devices, it is possible to launch the spectrum analyzer on the Radio 6 GHz radio interface.

Launching the spectrum analyzer on the radio interface

When the spectrum analyzer is launched, the radio interface will be switched to scanning mode, which will interrupt all Wi-Fi connections on this radio interface.



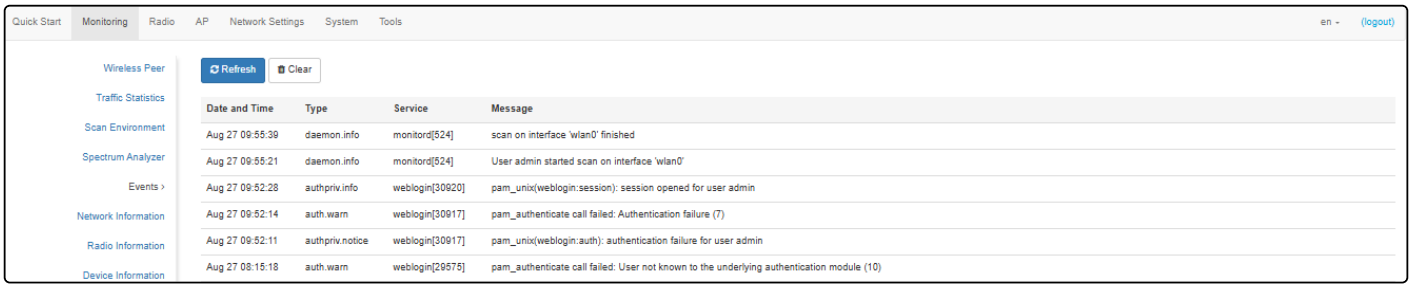
To start the spectrum analyzer, click the "Scan" button. The information window located to the right of the button displays the time in seconds that has passed since the start of the scan. The spectrum analyzer operation time on Radio 6 GHz is no more than 1 minute.

- *Last scan was...* — date and time of the last scan;
- *Channel Utilization* — information about the radio channel congestion, expressed as a percentage;
- *Frequency, MHz* — channel frequency, on which scanning was performed, MHz;
- *Channel* — channel number corresponding to a given frequency.

The spectrum analyzer analyzes all channels in the range, regardless of the radio interface settings.

10.7.5 "Events" submenu

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



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

Table 5 — Description of event severity levels

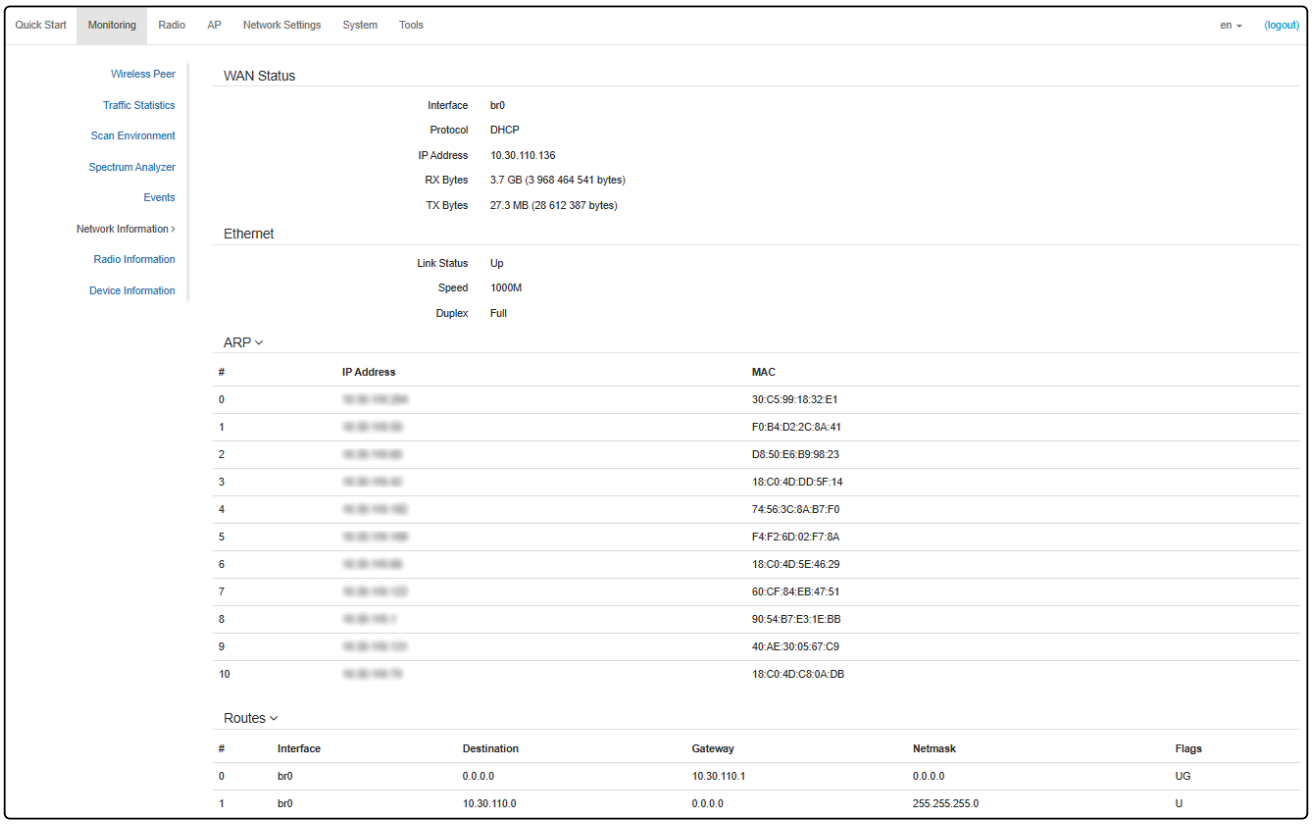
Level	Type message importance	Description
0	Emergency	A critical error has occurred in the system, the system may not work properly
1	Alert	Immediate intervention is required
2	Critical	A critical error has occurred in the system
3	Error	An error has occurred in the system
4	Warning	Warning, non-emergency message
5	Notice	System notice, non-emergency message
6	Informational	Informational system messages
7	troubleshooting	Troubleshooting 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 the "Clear" button.

10.7.6 "Network Information" submenu

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



WAN Status:

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

Ethernet:

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

ARP:

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

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

Routes:

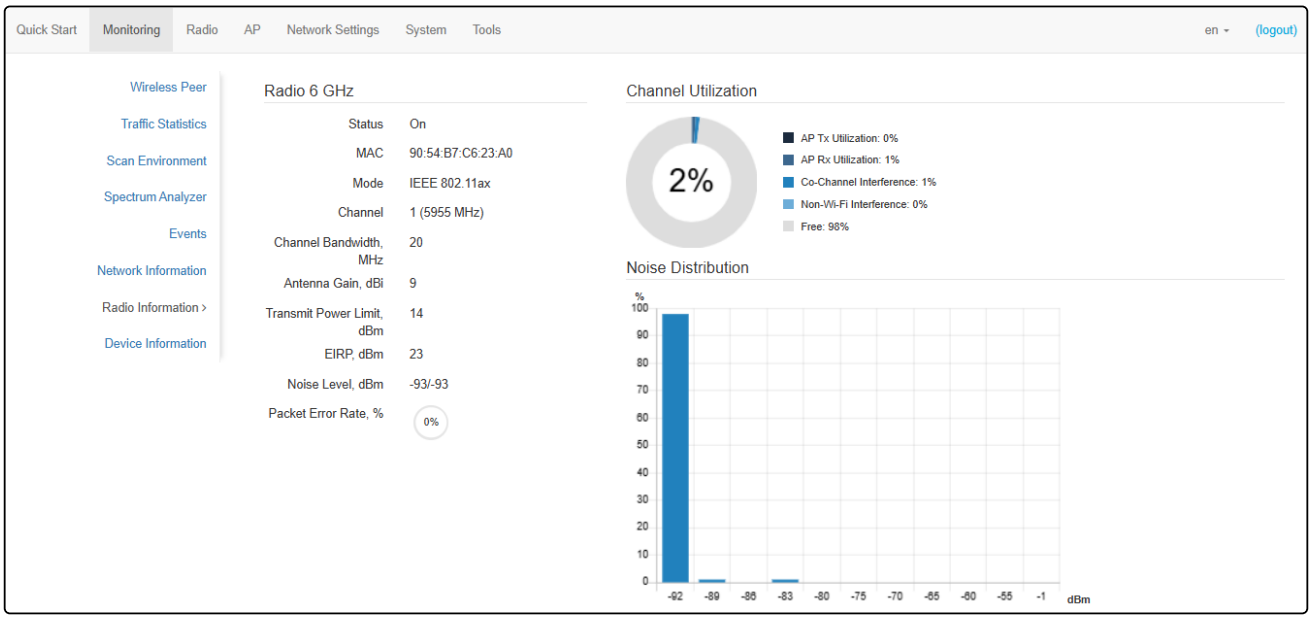
- *Interface* — name of the bridge interface;
- *Destination* — IP address of destination host or subnet that the route is established to;
- *Gateway* — IP address of the gateway through which access to the destination is carried out;
- *Netmask* — subnet mask;
- *Flags* — certain route characteristics.

The following flag values exist:

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

10.7.7 "Radio Information" submenu

In the **"Radio Information"** submenu, the current status of the device radio interface is displayed.



The device radio interface can be in two states: "On" or "Off". Depending on the interface status, the following information is available for monitoring:

"Off":

- *Status* — radio interface status;
- *MAC* — MAC radio interface;

"On":

- *Status* — radio interface status;
- *MAC* — MAC address of radio interface;
- *Mode* — radio interface operating mode in accordance with IEEE 802.11 standards;
- *Connection status* — client connection status (STA) to the access point (AP). Available only for "STA" device mode;
- *Channel* — wireless channel number on which the radio interface operates;
- *Channel Bandwidth, MHz* — channel bandwidth on which the radio interface operates;
- *Antenna Gain, dBi* — gain of the selected antenna;
- *Transmit Power Limit, dBm* — signal power at which the radio interface operates;
- *EIRP, dBm* — effective isotropic-radiated power;
- *Noise Level, dBm* — noise level on the channel where the radio interface operates;
- *Packet Error Rate, %* — proportion of packets that were received but contained errors and were dropped.

"Channel Utilization":

The "Channel utilization" diagram displays radio channel utilization expressed as a percentage. The total channel utilization (value in the center of the diagram) is calculated as the sum of the following components:

- *AP Tx Utilization* — percentage of time the device actively transmits data through the radio interface;
- *AP Rx Utilization* — percentage of time the device is busy receiving data on the radio interface;
- *Co-Channel Interference* — percentage of time the channel is occupied by other Wi-Fi devices using the same or an overlapping channel but not the intended recipient of the signal from the device;
- *Non-Wi-Fi Interference* — percentage of time the channel is busy due to signals generated by non-802.11 compliant devices;
- *Free* — percentage of time the channel is idle.

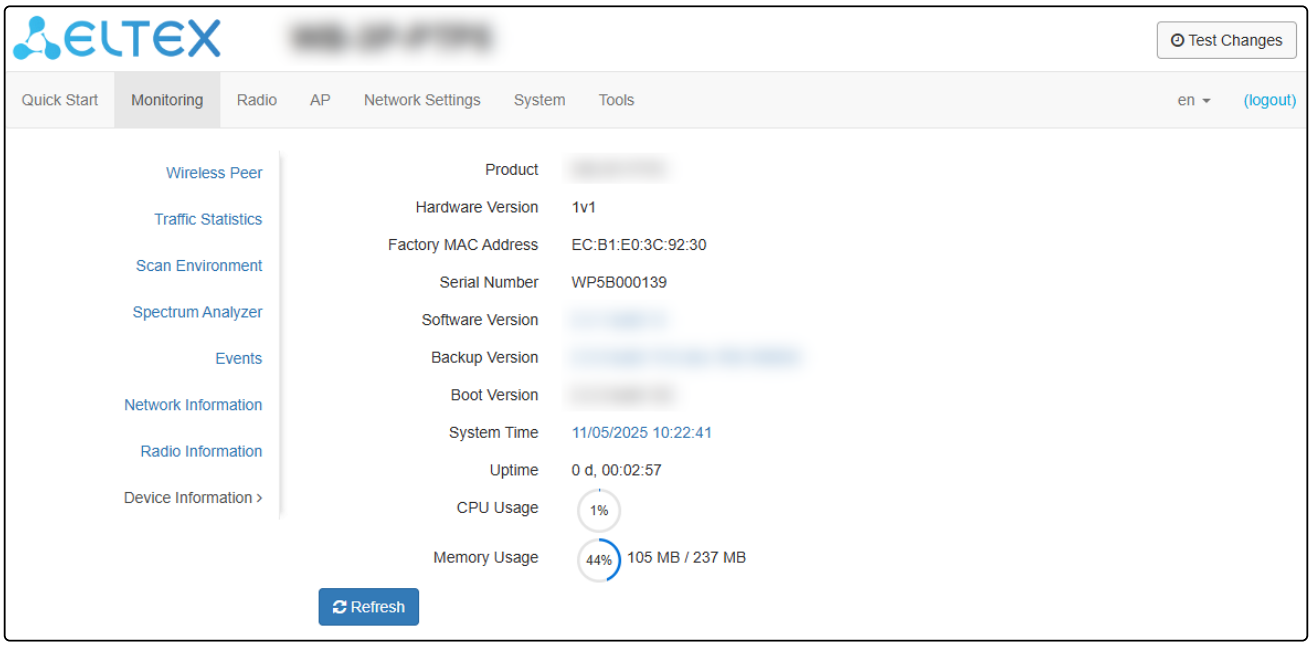
"Noise distribution":

The "Noise Distribution" graph displays statistical air noise distribution, showing the time proportion for each background noise level (dBm).

The data on the page is automatically updated every 5 seconds.

10.7.8 "Device Information" submenu

The **"Device Information"** the main device characteristics are displayed.



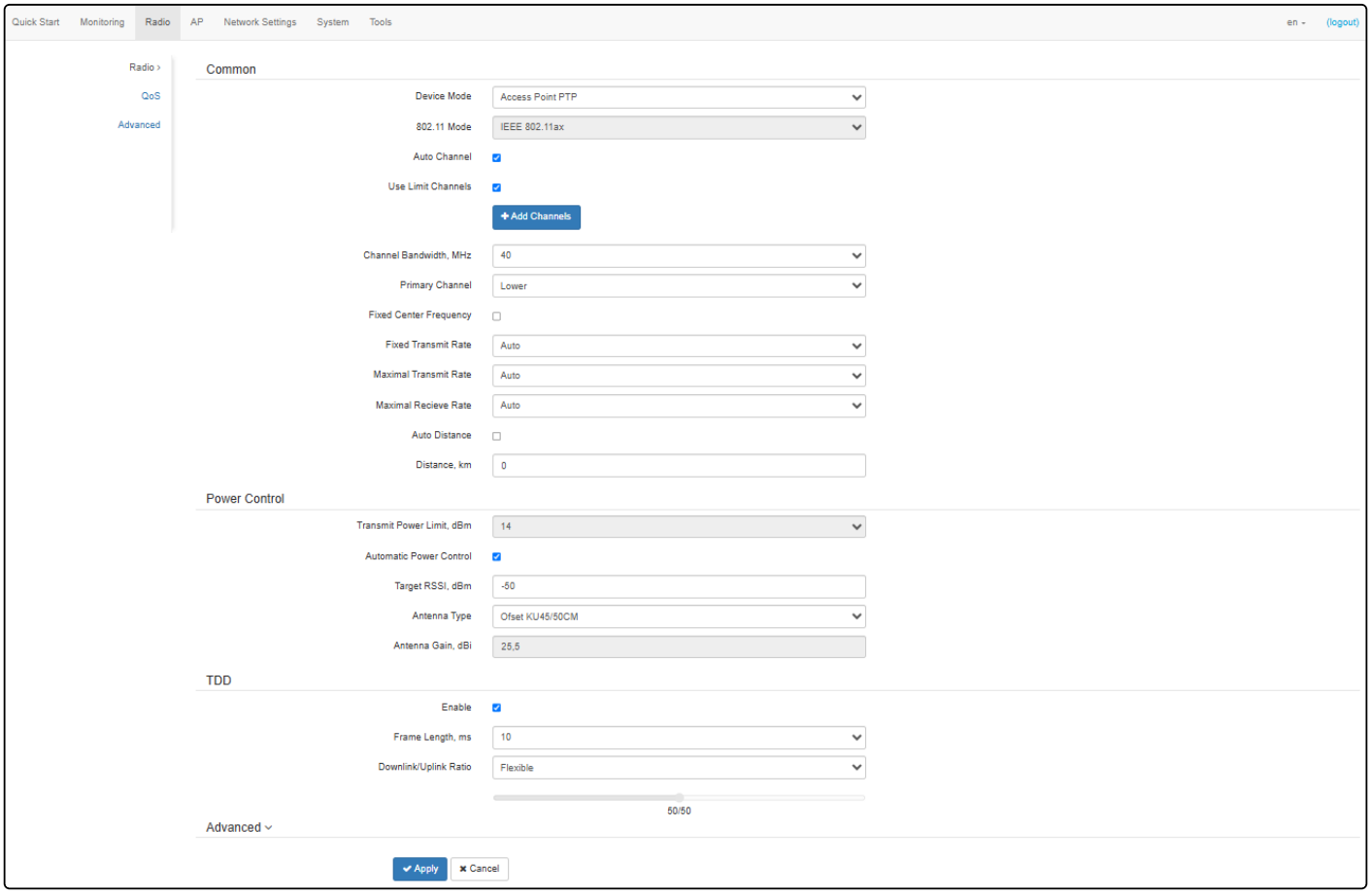
- *Product* — device model name;
- *Hardware Version* — device hardware version;
- *Factory MAC Address* — device WAN interface MAC address, factory set;
- *Serial Number* — device serial number, factory set;
- *Software Version* — device firmware version;
- *Backup Version* — previously installed firmware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

10.8 "Radio" menu

In the **"Radio"** menu wireless interface configuration is performed.

10.8.1 "Radio" submenu

The **"Radio"** submenu configures the main device radio interface parameters.



Common:

- *Device Mode* — operating mode of the device radio interface. The following modes are available:
  - *Access Point PTP* — Point-to-Point;
  - *Access Point PMP* — Point-to-Multipoint;
  - *Station* — wireless client (STA).
- *802.11 Mode* — interface operating mode according to standards:
  - *IEEE 802.11ax*;
- *Auto Channel* — when checked, the device will automatically select the least congested radio channel for the radio interface operation. When unchecked, channel field appears;
- *Channel* — select channel for data transmission;
- *Use Limit Channels* — when checked, the device will use a user-defined list of channels to work in automatic channel selection mode. If "Use Limit channels" is unchecked or there are no channels in the list, the device will select the operation channel from all available channels in the given band. The 6 GHz band channels: 1–93;
- *Limit Channels* — setting is available in the device mode "Station". When checked, the device will use a user-defined list of channels to scan and detect remote devices. If the "Limit Channels" is unchecked or there are no channels in the list, the device will scan all available channels in the given frequency range. The 6 GHz band channels: 1–93;

- *Channel Bandwidth, MHz* — channel bandwidth, on which the device operates. The parameter may take values of 20, 40, 80 and 160 MHz;
- *Primary Channel* — 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:
  - *Upper* — primary channel will be the upper 20 MHz channel in the 40 MHz band;
  - *Lower* — primary channel will be the lower 20 MHz channel in the 40 MHz band.
- *Fixed Center Frequency* — when checked, all traffic (data and control packets) will be transmitted at the specified channel center frequency with the specified bandwidth (40/80/160 MHz). This feature is proprietary and does not comply with IEEE 802.11 standards, which require the use of different center frequencies for data and control traffic with a channel width of 40/80/160 MHz;
- *Fixed Transmit Rate* — fixed wireless data transfer rate defined by IEEE 802.11/ax standard specifications;
- *Maximal Transmit Rate* — maximal wireless data rate of this device as defined by IEEE 802.11ax standard specifications;
- *Maximal Receive Rate* — maximal wireless data transfer rate of remote device, determined by IEEE 802.11ax standard specifications. Available only in the Access Point PTP and STA device modes;
- *Auto Distance* — when checked, the device will automatically determine and configure the distance between devices;
- *Distance, km* — distance between devices in kilometers. Changing the distance value will change the ACK timeout value. The distance should be rounded up. For example, if the distance between devices is 3.2 km, then 4 km should be specified;

The "Channel", "Channel Bandwidth", "Primary Channel" parameters are only available when the device mode is "Access Point PTP" or "Access Point PMP".

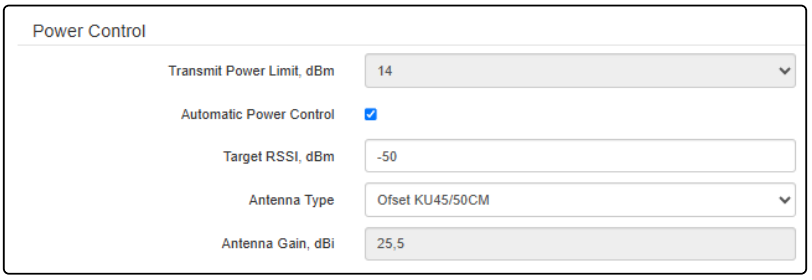
If the "Use Limit Channels" list contains a channel that is not available for selection, it will be marked in grey. In order for the new configuration to be applied to the device, only available (blue highlighted) channels must be specified in the "Use Limit channels" list.
Example. The device has not yet been configured, the default "Channel Bandwidth" for the 6 GHz Radio is set to 20 MHz, and no channels are listed in the "Use Limit Channels" list.
Suppose channels 37, 41, 45, 49 were manually added to the "Use Limit Channels " list and the "Channel Bandwidth" parameter needs to be set to 40 MHz. When changing this parameter from 20 MHz to 40 MHz, the following happens:

- "Primary Channel" becomes available for editing and the default value is "Upper";
- 41 and 49 channels in the "Use Limit Channels" list change 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 clicking the "Apply" button in the browser will display the error — "There are errors in data. Changes were not applied". Accordingly, the device 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.

The "Maximal **Receive** Rate" parameter is used to specify the maximal channel **transmit** rate to a remote device.
Therefore, when configuring the maximal channel **receive** rate, for example, on the client (STA), there is no need to configure the maximal **transmit** rate on an access point (AP).

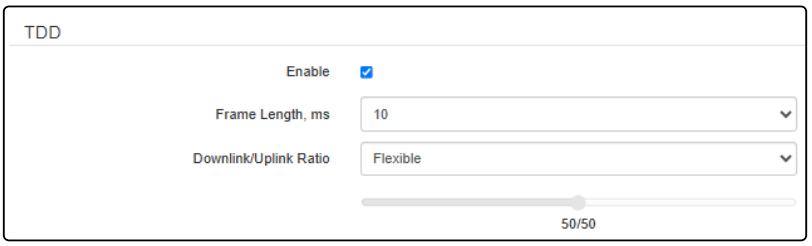
Power Control:



- *Transmit Power Limit, dBm* — Wi-Fi transmitter signal power adjustment;
- *Automatic Power Control* — automatic adjustment of Wi-Fi transmitter signal power;
- *Target RSSI, dBm* — target indicator of received radio signal power;
- *Antenna Type* — selection of the installed antenna type;
- *Antenna Gain, dBi* — gain factor for the selected antenna type.

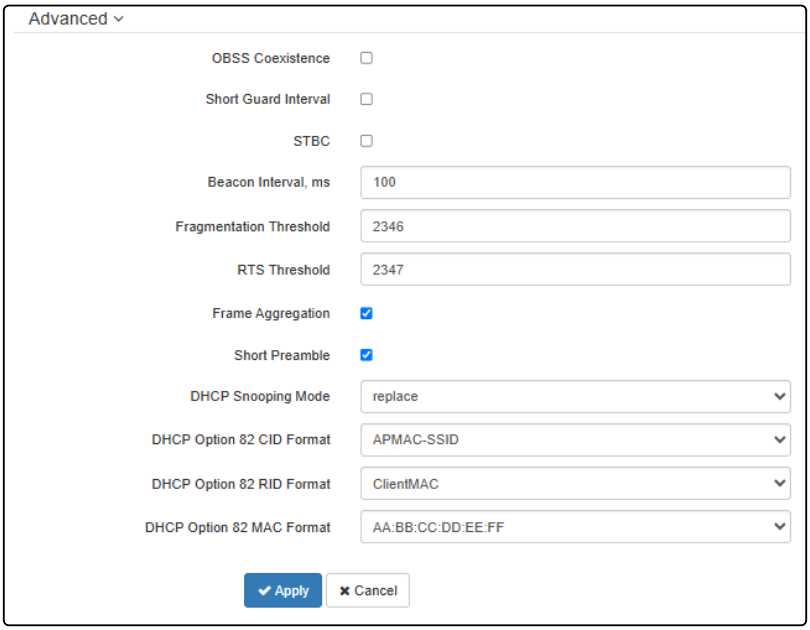
TDD:

TDD — it is a collision-free time-division multiplexing (TDM) technology that synchronizes data transmission in both directions within a time frame:



- *Enable* — when checked, the option is enabled; otherwise — disabled.
- *Frame Length, ms* — TDD frame duration in milliseconds, takes values of 5, 10 ms;
- *Downlink/Uplink Ratio* — time-slot ratio in TDD frame between Downlink and Uplink traffic:
    - *Fixed* — manually set of Downlink and Uplink ratio;
    - *Flexible* — dynamic change of the Downlink/Uplink ratio depending on the current channel load.

Advanced:



- *OBSS Coexistence* — automatic channel bandwidth reduction when the channel is loaded. When checked, the mode is enabled;
- *Short Guard Interval* — support for Short Guard Interval. The device transmits data using 400 ns guard interval (instead of 800 ns) to remote devices which also support Short Guard Interval;
- *STBC* — Space-Time Block Coding method dedicated to improve data transmission reliability. When checked, the device transmits one data flow through several antennas. When unchecked, the device does not transmit the same data flow through several antennas;
- *Beacon Interval, ms* — beacon frames transmission period. The frames are sent to detect a remote device in 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* — number of bytes over which the Request to Send will be sent. Decreasing this value may improve the performance of the device when there are a lot of connected remote devices. 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;
- *DHCP Snooping Mode* — selection of DHCP option 82 processing policy. Available values for selection:
    - *ignore* — option 82 processing is disabled. Default value;
    - *remove* — device deletes the value of option 82;
    - *replace* — device substitutes or replaces the value of option 82. When selecting this value to edit, the following parameters are opened:
        - *DHCP Option 82 CID format* — replacement of the CID parameter value, can take values:
            - *APMAC-SSID* — replacement of the CID parameter value to <MAC address of the device>-<SSID name>. Default value;
            - *SSID* — replacement of the parameter value to device SSID name;
            - *custom* — replacement of the CID parameter value to the value specified in the "DHCP Option 82 Custom CID";
                - *DHCP Option 82 Custom CID* — an arbitrary string of up to 52 characters that will be passed to the CID. If the parameter value is not set, the device will change the CID to the default value — APMAC-SSID.
        - *DHCP Option 82 RID format* — replacement of the RID parameter value, can take the following values:

- *ClientMAC* — change the RID content to the MAC address of the client device. Default value;
- *APMAC* — change the RID content to the MAC address of the device;
- *APdomain* — change the RID content to the domain in which the device is located;
- *custom* — change the RID content to the value specified in the "DHCP Option 82 RID format";
    - *DHCP Option 82 Custom RID* — an arbitrary string of up to 63 characters that will be passed to the RID. If the parameter value is not set, the device will change the RID to the default value — ClientMAC.

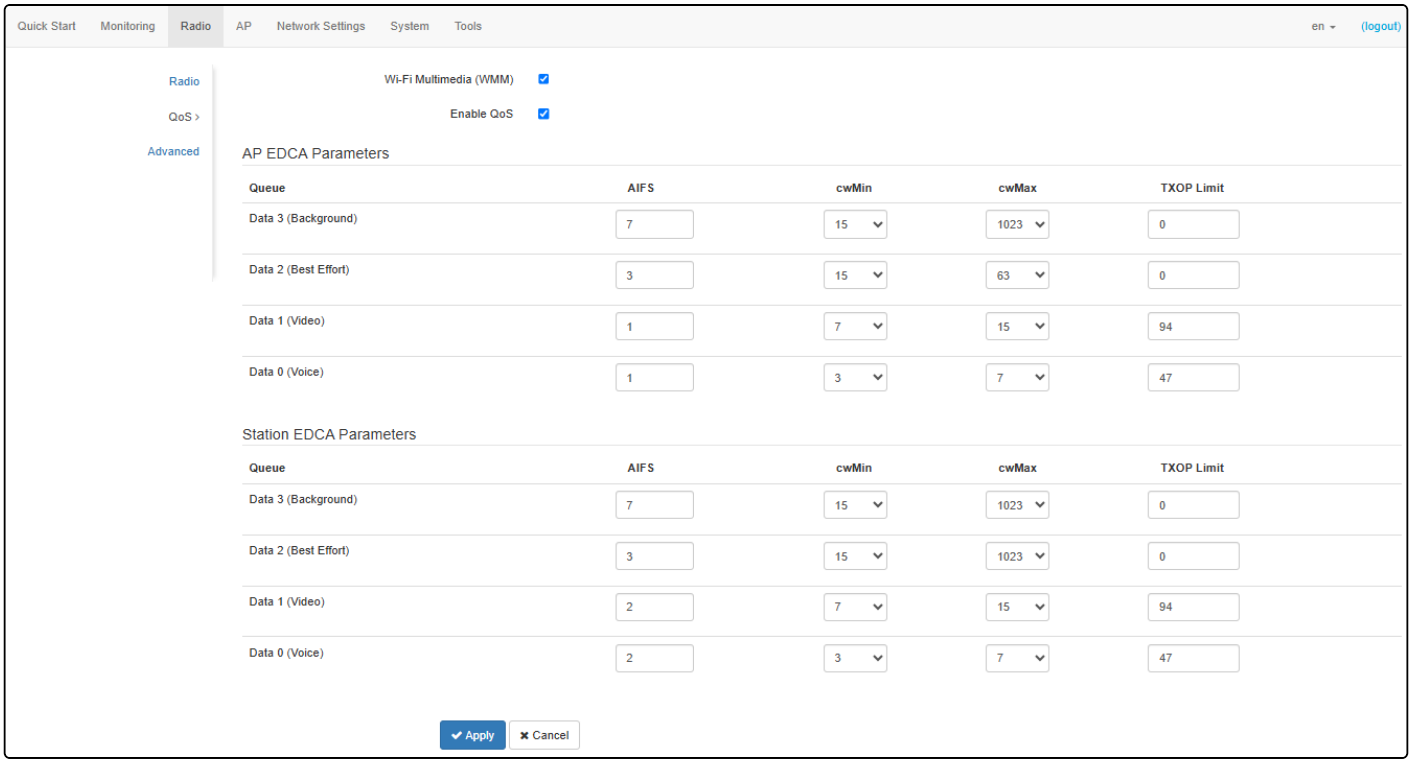
- *DHCP Option 82 MAC Format* — selection of octet delimiters of the MAC address, which is transmitted in CID and RID:
    - *AA:BB:CC:DD:EE:FF* — delimiter is a colon (:). Default value;
    - *AA-BB-CC-DD-EE-FF* — delimiter is a dash (-).

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

10.8.2 "QoS" submenu

The **"QoS"** submenu is used to configure Quality of Service functions.

- *Wi-Fi Multimedia (WMM)* — WMM (Wi-Fi Multimedia) support activation;
- *Enable QoS* — when checked, the setting of Quality of Service functions is available.

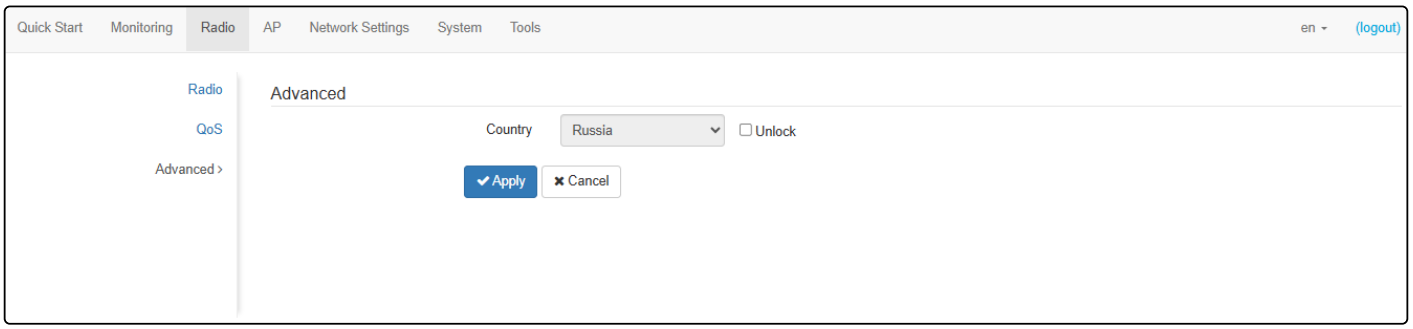


- *AP EDCA parameters* — device settings (traffic is transmitted to the client device):
  - *Queue* — predefined queues for various kinds of traffic:
    - *Data 3 (Background)* — low priority queue, high bandwidth (802.1p: cs1, cs2 priorities);
    - *Data 2 (Best Effort)* — middle priority queue, middle 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* — 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* — 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 device. The transmission capability is the time interval, in milliseconds, when the remote WME station has the rights to initiate data transmission over the wireless medium to the device, the maximum value is 65535 milliseconds;
- *Station EDCA parameters* — table of client device parameter settings (traffic is transmitted from the client device). For description of table fields, see above.

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

10.8.3 "Advanced" submenu

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



- *Country* — country of device operation. Select the "Unlock" checkbox to change a country. Depending on the selected value, the channel bandwidth and transmit power limit restrictions will be applied. The list of available frequency channels depends on the selected country, which affects the automatic channel selection in the Channel = Auto mode.

Local country regulations settings, including operation within legal frequency channels and output power, is the installer's responsibility.

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

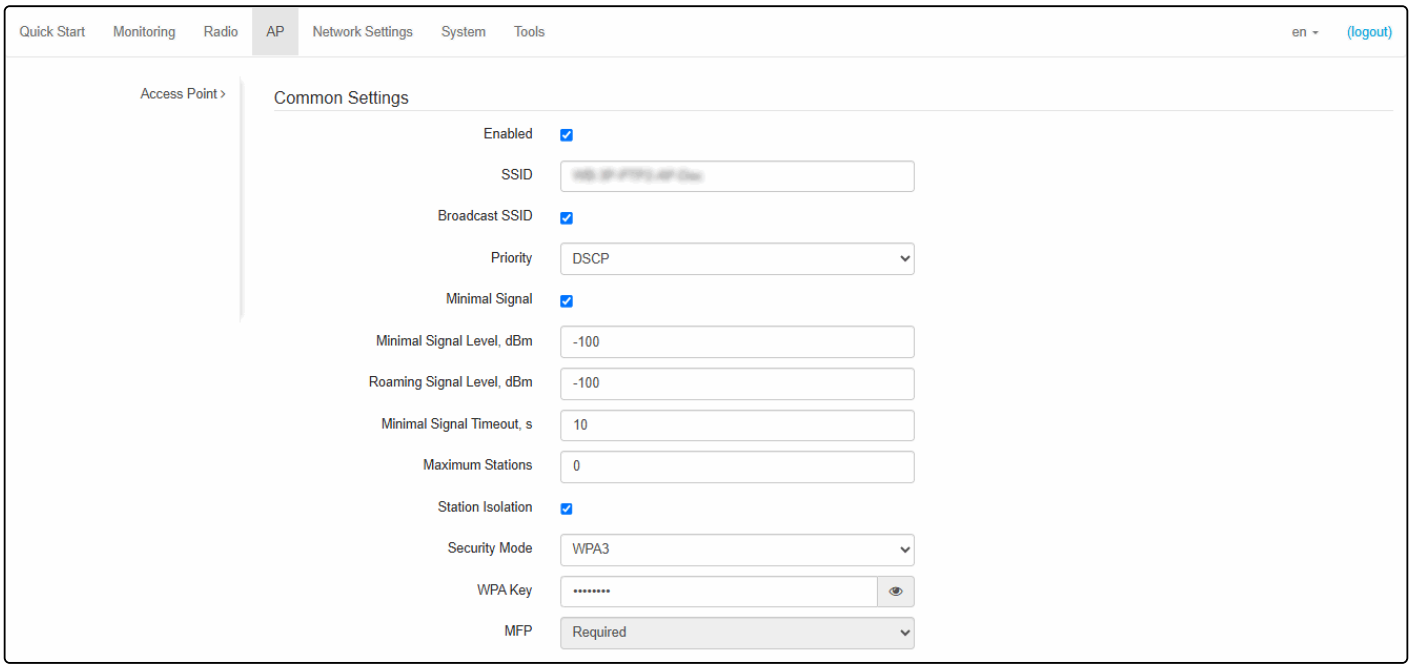
To apply a new configuration and save settings to non-volatile memory, click the "Apply" button. Click the "Cancel" button to discard the changes.

10.9 "AP" menu

In the **"AP"** menu access point configuration is performed (AP — Access Point) (then "AP").

The "AP" menu is available only in "Access Point PTP" or "Access Point PMP" device mode.

10.9.1 "Access Point" submenu



Common Settings:

- *Enabled* — when checked, the access point (AP) is enabled, otherwise it is disabled;
- *SSID* — virtual wireless network name;
- *Broadcast SSID* — when checked, broadcasting to the SSID is enabled, otherwise it is disabled;
- *Priority* — prioritization method. Defines the field based on which traffic transmitted to the radio interface will be distributed among WMM queues:
  - *DSCP* — priority from the DSCP field of IP packet header will be analyzed;
  - *802.1p* — priority from the CoS (Class of Service) field of tagged packets will be analyzed.
- *Minimal Signal* — when checked, the function of disconnecting client devices at a low signal level (Minimal Signal) is enabled. For the functionality to work, the following parameters need to be configured:
  - *Minimal Signal Level, dBm* — signal level, below which the client devices are disconnected from the wireless network;
  - *Roaming Signal Level, dBm* — roaming sensitivity level, below which the client devices switch to another device. The parameter should be higher than the "Minimal Signal Level": if the "Minimal Signal Level" is -75 dBm, then the "Roaming Signal Level" should be, 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 wireless network.
- *Maximum Stations* — maximum number of client devices allowed to connect to the wireless network;
- *Station Isolation* — when checked, traffic isolation between connected devices is enabled;
- *Security Mode* — wireless network access security mode:
  - *OWE (Opportunistic Wireless Encryption)* — encryption method that ensures the security of data transmitted over an unsecured network. Users are not required to take any additional actions or enter a password to connect to the network;

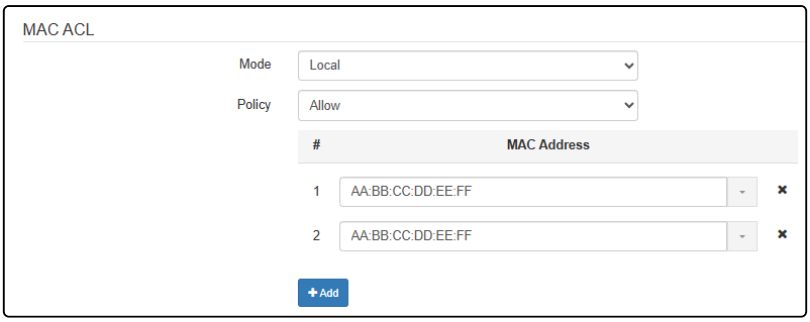
- *WPA3* — encryption method, when selected the following setting will be available:
  - *WPA* Key — key/password required to connect to the wireless network. The key length is from 8 to 63 characters.
- *WPA3-Enterprise* — a wireless link encryption mode in which the device authenticates via a centralized RADIUS server. This security mode requires specifying RADIUS server parameters. Selecting one of these methods makes the following RADIUS setting available (see below).

- *MFP* — management frame protection available in WPA3, WPA3-Enterprise, OWE. When WPA3, WPA3-Enterprise, OWE is selected, MFP is set to Required):
  - *Required* — management frame protection is enabled. The device can not connect to the wireless network, that does not support MFP.

"Maximum Stations" and "Station Isolation" are available only in the "Access Point PMP" device modes.

MAC ACL:

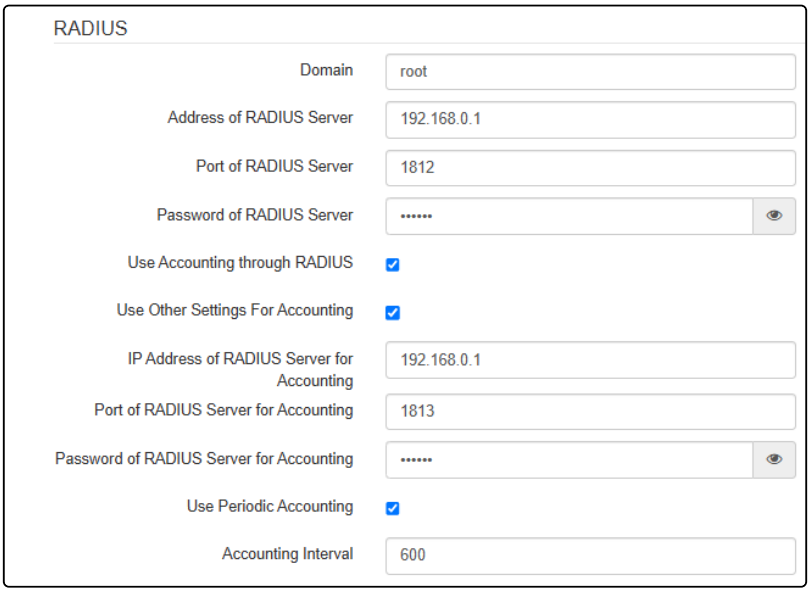
In this subsection, one can configure a list of MAC addresses of remote devices that are allowed or prohibited from connecting to this device, depending on the selected access policy.



- *Mode* — selection of the access control mode by MAC:
  - *Off* — function is not active;
  - *Local* — check MAC by list on the device;
  - *RADIUS* — check MAC via RADIUS server.
- *Policy* — access policy. Acceptable values:
  - *Deny* — remote devices whose MAC addresses are on the list will be prohibited from connecting to this device. All other devices will be allowed access;
  - *Allow* — only those remote devices whose MAC addresses are in the list will be allowed to connect to this device. All others will be denied access.
- *MAC address* — list of MAC addresses of remote devices that are allowed or denied access to this device. This list can contain up to 128 addresses.

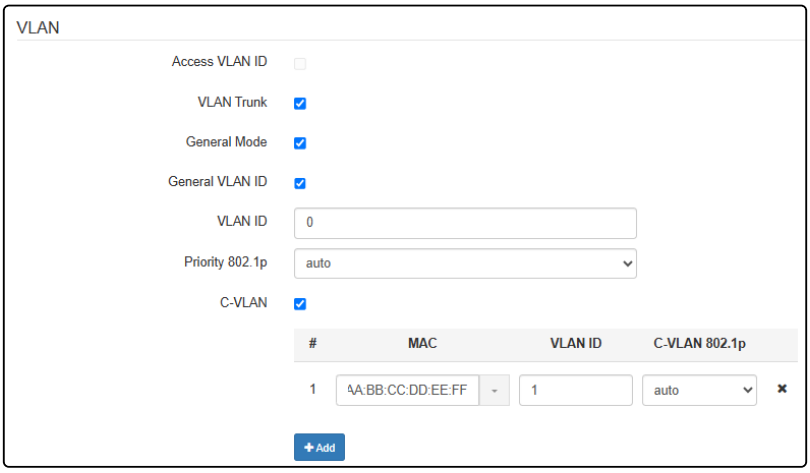
To add an address to the list, click + Add and enter MAC in the field that appears. To remove an address from the list, click the button ✖ in the corresponding row.
If it becomes necessary to add MAC of the connected device to the list: click at the end of the row ▾ and select the required address from the list; it will be automatically added to the field.
By default the list displays up to 10 addresses. To view the full list if it contains more than 10 addresses, click the "Show All" button.

RADIUS:



- *Domain* — user domain;
- *Address of RADIUS Server* — RADIUS server address;
- *Port of RADIUS Server* — port of RADIUS server that used for authentication and authorization;
- *Password of RADIUS Server* — password for 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.

VLAN:



- *Access VLAN ID* — VLAN number from which the tag will be removed when transmitting traffic to client devices. When traffic passes in the opposite direction, untagged traffic from client devices will be tagged with a VLAN ID (available when VLAN Trunk mode is disabled);
- *VLAN Trunk* — when checked, tagged traffic is transmitted to client devices;
- *General Mode* — when checked, client devices are allowed to transmit untagged traffic together with tagged traffic (available when VLAN Trunk mode is enabled);
- *General VLAN ID* — VLAN number from which the tag will be removed when forwarding traffic to client devices. When passing traffic in the opposite direction, untagged traffic from client devices will be tagged with the General VLAN ID (available when VLAN Trunk and General Mode are enabled);
- *Priority 802.1p* — 802.1p priority number assigned to traffic tagged with a VLAN ID using the Access VLAN ID or General VLAN ID functionality (available when Access VLAN ID or General VLAN ID is enabled);
- *C-VLAN* — when checked, lists of MAC addresses of remote devices are configured, assigning them an isolated VLAN ID and an 802.1p priority:
  - *MAC* — MAC address of the remote device;
  - *VLAN ID* — VLAN number from which the tag will be removed when forwarding traffic to the remote device. When passing traffic in the opposite direction, untagged traffic from the remote device will be tagged with the VLAN ID;
  - *C-VLAN 802.1p* — 802.1p priority number assigned to traffic that is tagged with a VLAN ID using the C-VLAN functionality.

To add an address to the list, click 

and enter MAC in the field that appears. To remove an address from the list, click the button  in the corresponding row.

If there is a need to add the MAC address of a connected device to the list: click  at the end of the row and select the required address from the list; it will be automatically added to the field.
By default the list displays up to 10 addresses. To view the full list if it contains more than 10 addresses, click the "Show All" button.

Mapping VLAN:



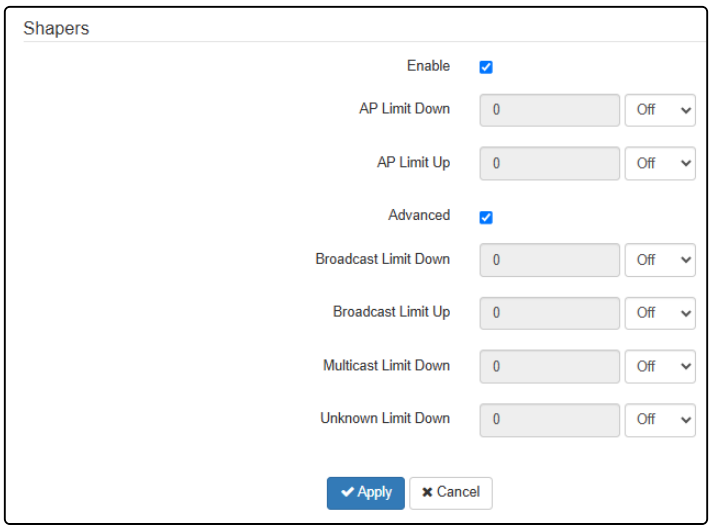
- *Enable* — when checked, the VLAN Mapping function is enabled, otherwise — disabled;
- *Default Rule* — when checked, the rule is activated; otherwise it disables the rule. The default rule determines the system's behavior for VLAN packets that don't match any explicitly defined user rules. It automatically assigns 802.1p priority and a WMM queue to such packets:
  - *WLAN VLAN* — VLAN ID number when transmitting in WLAN. Takes values: 1–4094;
  - *Ethernet VLAN* — VLAN ID number when transmitting to Ethernet. Takes values: 1–4094;
  - *WLAN 802.1p* — 802.1p priority when transmitting in WLAN. Takes values: 0–7, auto. By default — auto;
  - *Ethernet 802.1p* — 802.1p priority when transmitting to Ethernet. Takes values: 0–7, auto. By default — auto;
  - *WMM* — WMM queue for this rule. Takes values: bk, be, vi, vo, auto. If the queue is not set to auto, the DSCP priority will be analyzed in the packet.

Works only when enabled VLAN Trunk.

To add a rule to the list, click +Add. To remove a rule from the list, click the button ✖ in the corresponding row.
By default the list displays up to 9 addresses. To view the full list if it contains more than 9 addresses, click the button "Show All".

Shapers:

For the device mode "Access Point PTP":



Enable — activate the settings field:

- *AP Limit Down* — bandwidth limiting in the direction from access point (AP) to client (STA);
- *AP Limit Up* — bandwidth limiting in the direction from client (STA) to access point (AP).

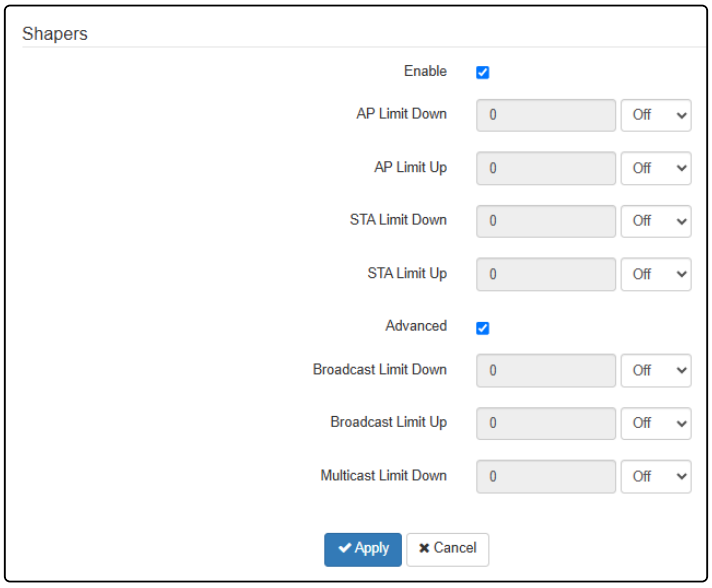
Advanced — activate the additional settings field:

- *Broadcast Limit Down* — bandwidth limiting of broadcast traffic in the direction from access point (AP) to clients (STA);
- *Broadcast Limit Up* — bandwidth limiting of broadcast traffic in the direction from clients (STA) to access point (AP);
- *Multicast Limit Down* — bandwidth limiting of multicast traffic in the direction from access point (AP) to clients (STA);
- *Unknown Limit Down* — bandwidth limiting of unknown traffic in the direction from access point (AP) to clients (STA).

The following parameters are available for configuring restrictions:

- *Off* — bandwidth limiting is not applied;
- *kbps* — bandwidth limiting is applied in kbps;
- *pps* — bandwidth limiting is applied in packets/s.

For the "Access Point PMP" device mode:



Enable — activate the settings field;

- *AP Limit Down* — bandwidth limiting in the direction from access point (AP) to client devices;
- *AP Limit Up* — bandwidth limiting in the direction from client devices to access point (AP);
- *STA Limit Down* — bandwidth limiting in the direction from access point (AP) to each client device;
- *STA Limit Up* — bandwidth limiting in the direction from each client device to access point (AP);

Advanced — activate the additional settings field:

- *Broadcast Limit Down* — bandwidth limiting of broadcast traffic in the direction from access point (AP) to clients (STA);
- *Broadcast Limit Up* — bandwidth limiting of broadcast traffic in the direction from clients (STA) to the access point (AP);
- *Multicast Limit Down* — bandwidth limiting of multicast traffic in the direction from access point (AP) to clients (STA).

The following parameters are available for configuring restrictions:

- *Off* — bandwidth limiting is not applied;
- *kbps* — bandwidth limiting is applied in kbps/s;
- *pps* — bandwidth limiting is applied in packets/s.

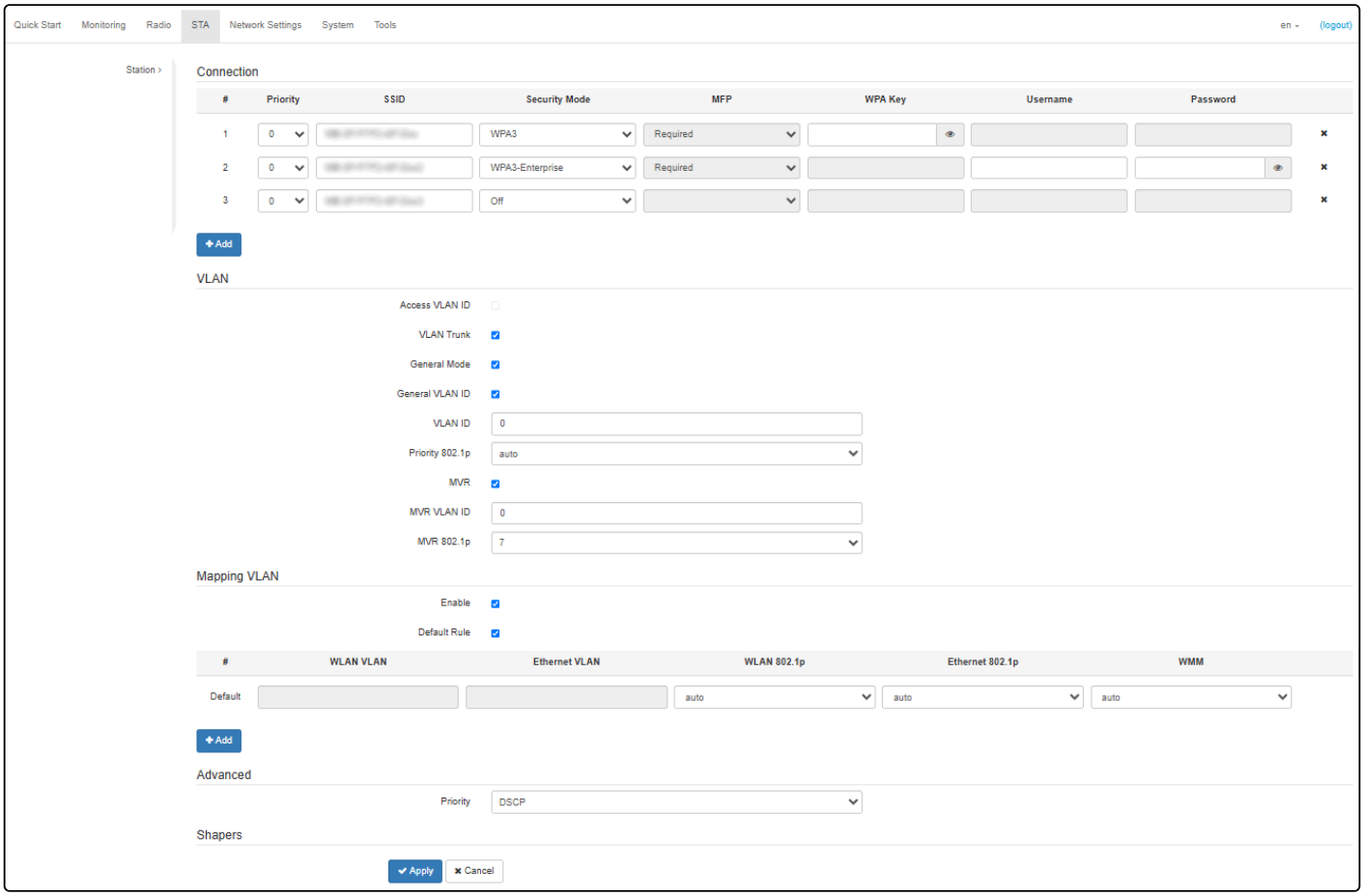
After Changing "SSID" on the access point (AP) access to client devices may be lost. You must first change "SSID" on client devices in the "STA" menu, and then on the access point (AP) In the "AP" menu.

10.10 "STA" menu

In the **"STA"** menu client configuration is performed (STA — Station) (then "STA").

The "STA" menu is only available in the "Station" device mode.

10.10.1 "Station" submenu



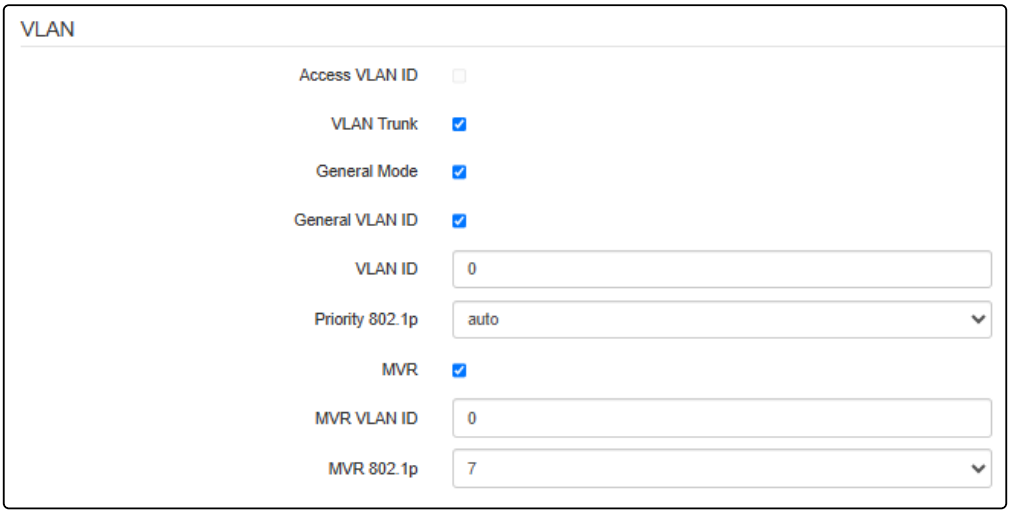
Connection:

- *Priority* — determines the order of profile usage. When searching for a network and connecting, the device uses the highest priority profile first. If priorities are equal, the device determines profile usage order based on encryption mode and RSSI;
- *SSID* — virtual wireless network name;
- *Security Mode* — wireless network access security mode:
  - *OWE (Opportunistic Wireless Encryption)* — encryption method that ensures data security transmitted over an unsecured network.
  - *WPA3* — encryption method; the following settings become available when selected:
    - *WPA Key* — key/password, required to connect to the wireless network. The key length is from 8 to 63 characters.
  - *WPA3-Enterprise* — wireless channel encryption mode in which the device authenticates on a centralized RADIUS server. To use this security mode, connection parameters must be specified:
    - *Username* — login, required for authorization on RADIUS-on the server;
    - *Password* — key/password, required for authorization on RADIUS server.
- *MFP* — protection management frames (available for WPA3, WPA3-Enterprise, OWE security modes. When selecting the security mode WPA3, WPA3-Enterprise, OWE MFP is switched to Required):

- *Required* — protection is enabled. The device cannot connect to a wireless network that does not support MFP.

To add a new connection profile, click "Add profile". Maximum 8 profiles can be added.

VLAN:



VLAN:

- *Access VLAN ID* — VLAN number from which the tag will be removed when forwarding traffic to Ethernet devices connected to the client (STA). When passing traffic in the opposite direction, untagged traffic will be tagged with VLAN ID (available when VLAN Trunk mode is disabled);
- *VLAN Trunk* — when checked, tagged traffic is transmitted to Ethernet devices connected to the client (STA);
- *General Mode* — when checked, Ethernet devices connected to the client (STA) are allowed to transmit untagged traffic with tagged traffic (available when VLAN Trunk mode is enabled);
- *General VLAN ID* — VLAN number from which the tag will be removed when transmitting traffic to Ethernet devices, connected to the client (STA). When traffic passes in the opposite direction, untagged traffic will be tagged with General VLAN ID (available when VLAN Trunk and General Mode are enabled);
- *Priority 802.1p* — 802.1p priority number assigned to traffic that is tagged with a VLAN ID using the Access VLAN ID or General VLAN ID functionality (available when Access VLAN ID or General VLAN ID is enabled);
- *MVR* — when checked, the MVR (Multicast VLAN Registration) functionality is enabled. Allows to use a separate VLAN for Multicast traffic;
- *MVR VLAN ID* — VLAN number of multicast traffic that will be untagged when transmitted to Ethernet devices connected to the client (STA). When traffic passes in the opposite direction, untagged IGMP packets from clients will be tagged with MVR VLAN ID;
- *MVR 802.1p* — 802.1p priority to be assigned to IGMP packets from Ethernet devices connected to the client (STA).

Mapping VLAN:



- Enable — when checked, the function is enabled VLAN Mapping, otherwise — disabled;
- *Default rule* — when checked, the rule is activated; otherwise it disables the rule. The default rule defines system behavior for VLAN-Packets that do not match any user-defined rules. It allows automatically assigning priority to such packets 802.1p and queue WMM:
  - *WLAN VLAN* — VLAN ID number when transmitting in WLAN. Takes values: 1–4094;
  - *Ethernet VLAN* — VLAN ID number when transmitting to Ethernet. Takes values: 1–4094;
  - *WLAN 802.1p* — priority 802.1p when transmitting in WLAN. Takes values: 0–7, auto. By default — auto;
  - *Ethernet 802.1p* — priority 802.1p when transmitting to Ethernet. Takes values: 0–7, auto. By default — auto;
  - *WMM* — WMM queue for this rule. Takes values: bk, be, vi, vo, auto. If the auto queue is not defined in this option, the DSCP priority in the packet will be analyzed.

Works only when enabled VLAN Trunk.

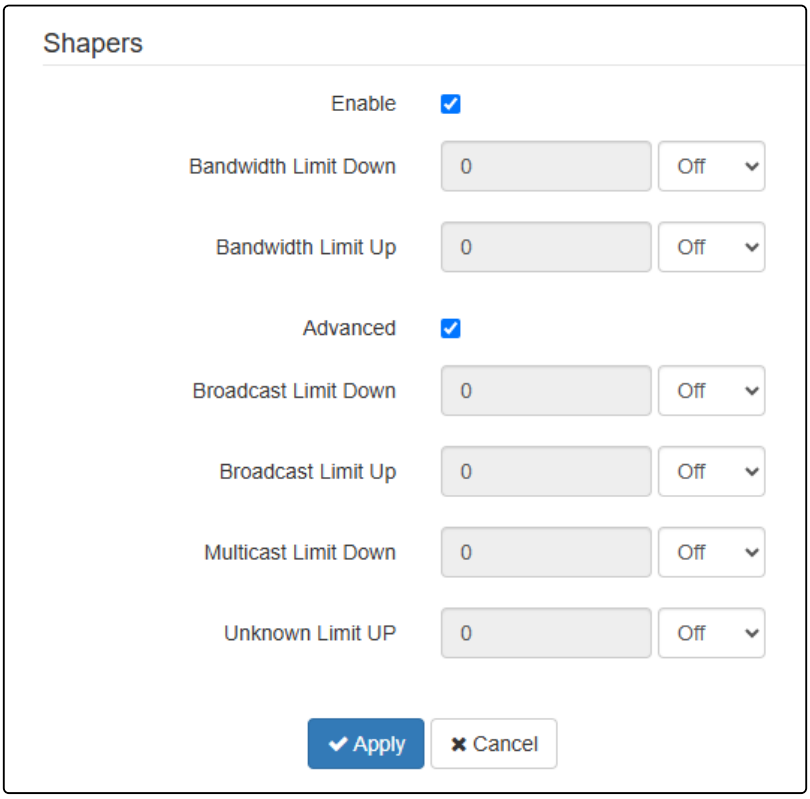
To add a rule to the list, click 

. To remove a rule from the list, click the button  in the corresponding row.
By default the list displays up to 9 addresses. To view the full list if it contains more than 9 addresses, click the button "Show All".

Advanced:

- *Priority* — prioritization method selection. Defines the field for distributing traffic entering the radio interface among queues WMM:
  - *DSCP* — priority from the DSCP field of the IP packet header will be analyzed;
  - *802.1p* — priority from the CoS (Class of Service) field of tagged packets will be analyzed.

Shapers:



Enable — activate the settings field:

- *Bandwidth Limit Down* — bandwidth limiting in the direction from the client (STA) to Ethernet devices;
- *Bandwidth Limit Up* — bandwidth limiting in the direction from Ethernet devices to client (STA).

Advanced — activate the additional settings field:

- *Broadcast Limit Down* — bandwidth limiting of broadcast traffic in the direction from client (STA) to Ethernet devices;
- *Broadcast Limit Up* — bandwidth limiting of broadcast traffic in the direction from Ethernet devices to client (STA);
- *Multicast Limit Down* — bandwidth limiting of multicast traffic in the direction from client (STA) to Ethernet devices;
- *Unknown Limit UP* — bandwidth limiting of unknown traffic in the direction from Ethernet devices to the client (STA).

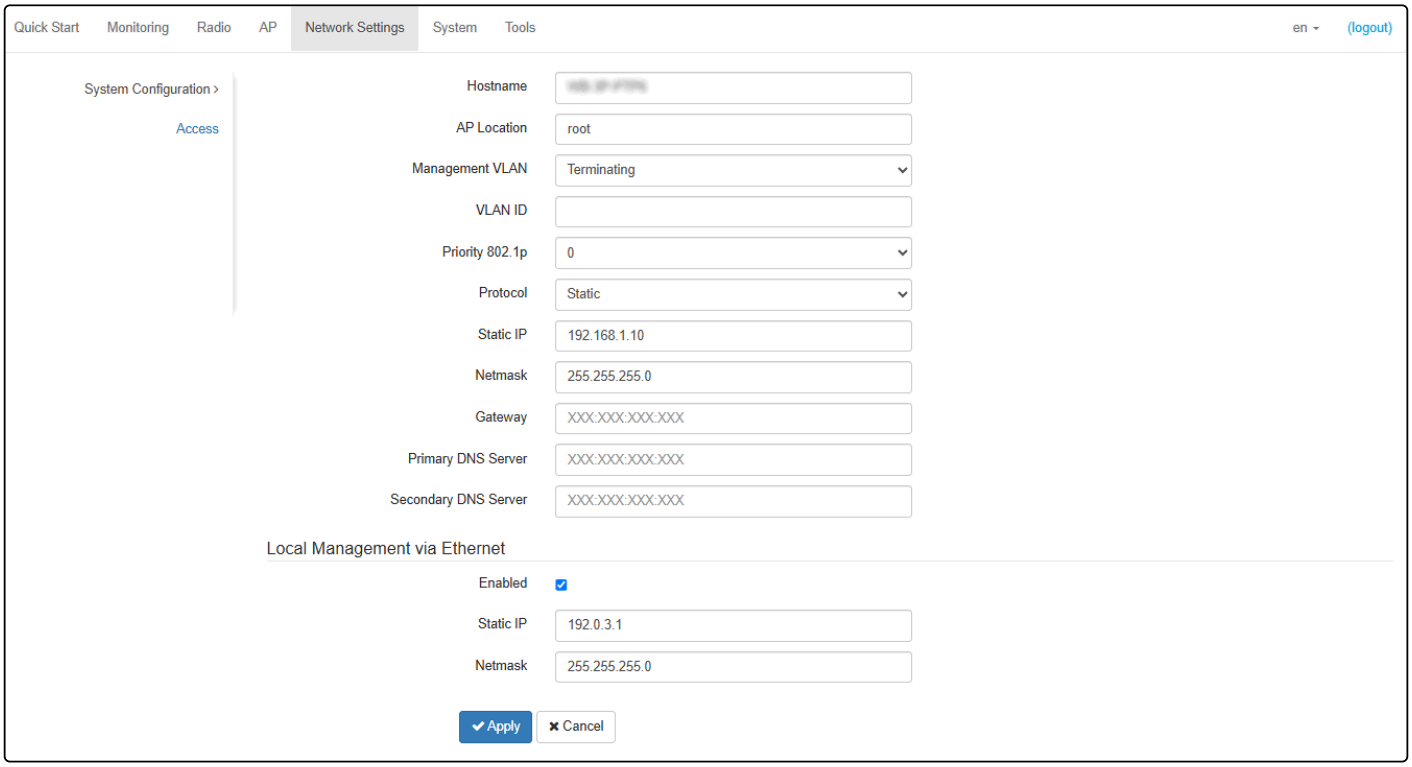
The following parameters are available for configuring restrictions:

- *Off* — bandwidth limiting is not applied;
- *kbps* — bandwidth limiting is applied in kbps;
- *pps* — bandwidth limiting is applied in packets/s.

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

10.11 "Network Settings" menu

10.11.1 "System Configuration" submenu



- *Hostname* — device network name, set as a string 1–63 characters: Latin uppercase and lowercase letters, digits, and the hyphen character "-" (a hyphen cannot be the last character in the name);
- *AP Location* — domain where the device is located;
- *Management VLAN*:
  - *Off* — Management VLAN is not used;
  - *Terminating* — mode in which Management VLAN is terminated on the device. In this case, remote devices connected via the radio interface have no access to the VLAN;
  - *Forwarding* — mode in which Management VLAN is also transmitted to the radio interface (with the appropriate AP settings).
- *VLAN ID* — VLAN identifier used for device access; accepts values 1–4094;
- *Priority 802.1p* — 802.1p priority number, assigned to packets outgoing from Management VLAN interface of the device;
- *Protocol* — select protocol for connecting a device via Ethernet interface to the service provider network:
  - *DHCP* — operating mode in which IP address, subnet mask, DNS server address, default gateway, and other parameters required for network operation will be obtained from the DHCP server automatically;
  - *Static* — operating mode in which IP address and all necessary parameters on WAN interface is assigned statically. When selecting the "Static" type, the following parameters become available for editing:
    - *Static IP* — IP address of WAN device interface in the provider network;
    - *Netmask* — external subnet mask;
    - *Gateway* — address to which a packet is sent if no route is found for it in the routing table.
- *Primary DNS Server, Secondary DNS Server* — IP Address of DNS servers. If addresses of DNS servers are not assigned automatically via the protocol DHCP, set them manually.

After "Management VLAN" configuration, access to the device may be lost.

Local Management via Ethernet:

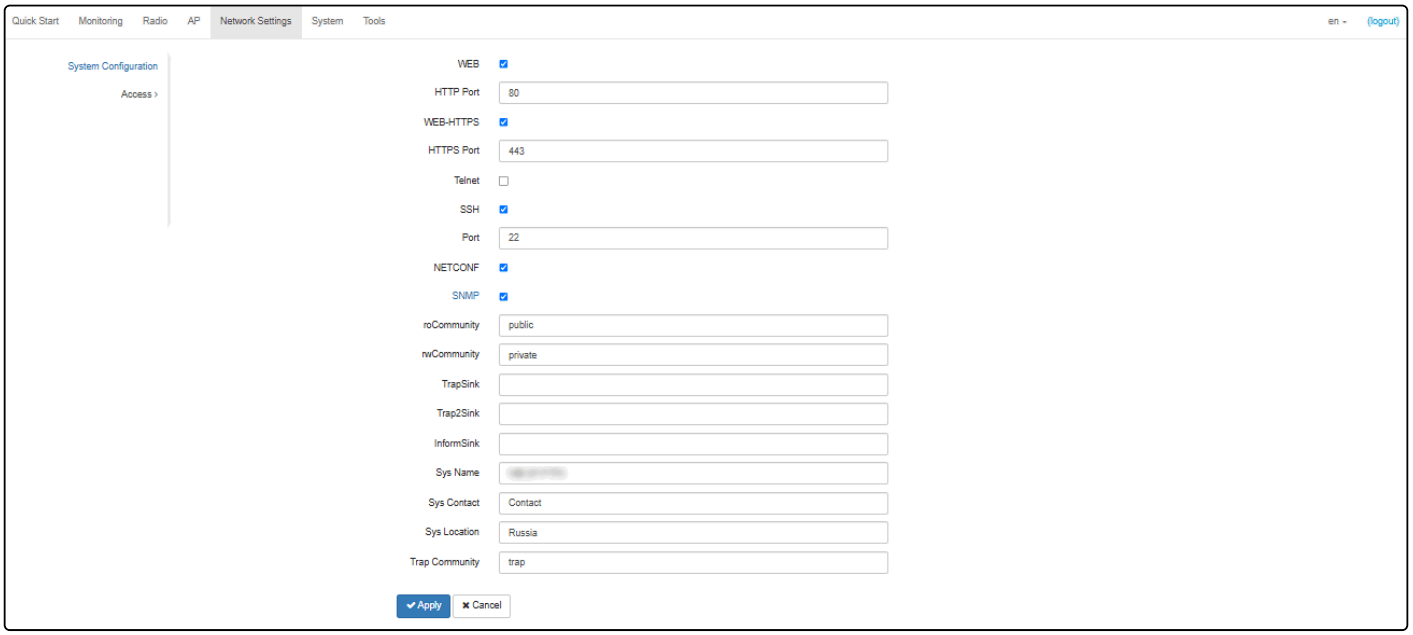
This subsection allows configuring untagged access to the device via Ethernet interface.

- *Enabled* — activates the setting;
- *Static IP* — IP address of device Ethernet interface in the local network (by default 192.0.3.1);
- *Netmask* — subnet mask.

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

10.11.2 "Access" submenu

The **"Access"** configures device access via web interface, Telnet, SSH, NETCONF and SNMP.

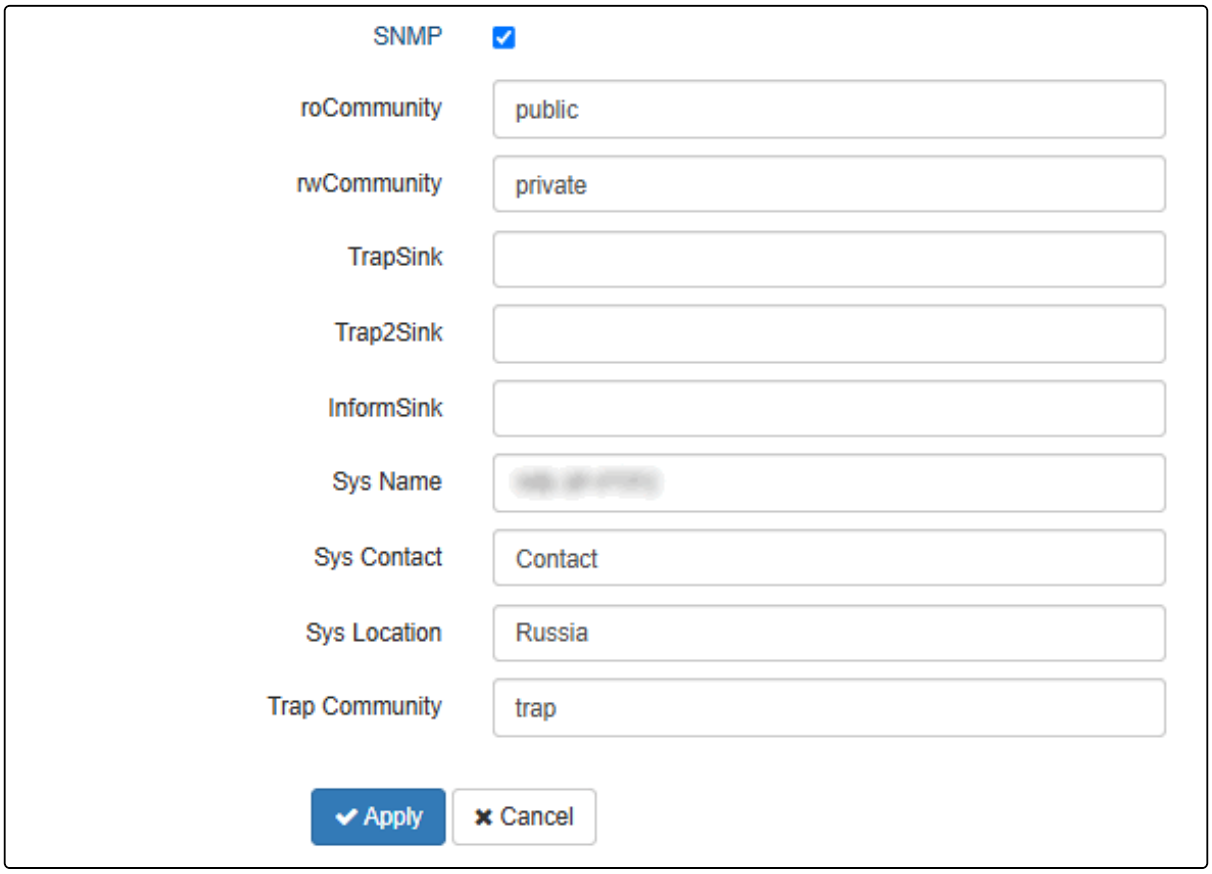


- To enable access to the device via the web interface via HTTP protocol, select the checkbox next to "WEB". In the window that appears, it is possible to change the HTTP port (by default: 80). The range of acceptable values of ports, in addition to the default, is from 1025 to 65535 inclusive;
- To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

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

- To enable access to the device via Telnet, select the checkbox next to "Telnet". In the window that appears, it is possible to change the Telnet port (23 by default). The range of acceptable port values, in addition to the default, is from 1025 to 65535 inclusive;
- To enable access to the device via SSH, select the checkbox next to "SSH". In the window that appears, it is possible to change the SSH port (22 by default). The range of acceptable port values, in addition to the default, is from 1025 to 65535 inclusive;
- To enable access to the device via NETCONF, select the checkbox next to "NETCONF".

The WB-3P-PTP6 software allows changing the device configuration, monitoring its status, as well as managing the device using the SNMP protocol.



The device supports SNMPv1, SNMPv2, SNMPv3 protocols.

To change the SNMP settings, select the checkbox next to "SNMP", the following SNMP agent options become available:

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

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

- eltexLtd.1.127.1 — monitoring of device parameters;
- eltexLtd.1.127.3 — device management;
- eltexLtd.1.127.5 — device configuring.

where eltexLtd — 1.3.6.1.4.1.35265 is Eltex Enterprise ID.

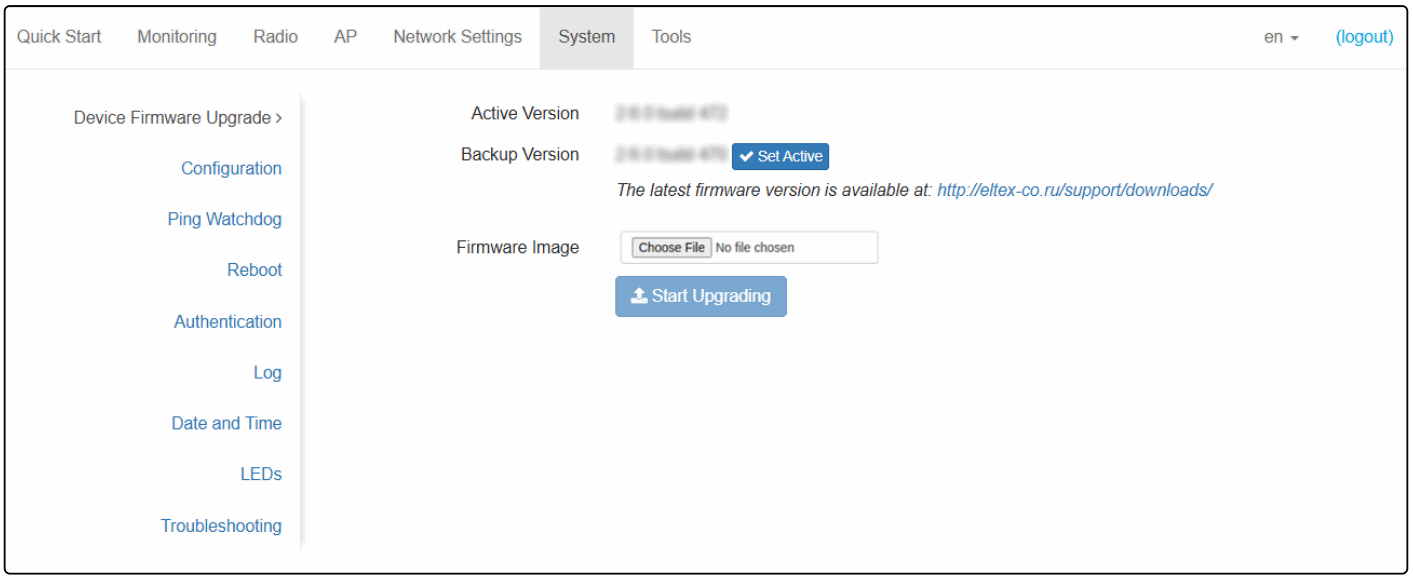
To apply a new configuration and save settings to non-volatile memory, click "Apply”. Click "Cancel" to discard the changes.

10.12 "System" menu

In the **"System"** menu, the user can configure the system, time, syslog, change the password, upload/download the configuration, upgrade the firmware, and reboot the device.

10.12.1 "Device Firmware Upgrade" submenu

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



- *Active Version* — installed firmware version, which is operating at the moment;
- *Backup Version* — installed firmware version that can be switched to without downloading a firmware file;
  - *Set active* — button that allows making a backup version of the firmware active, this will require a device reboot. The active firmware version will not be set as a backup.

Firmware upgrade

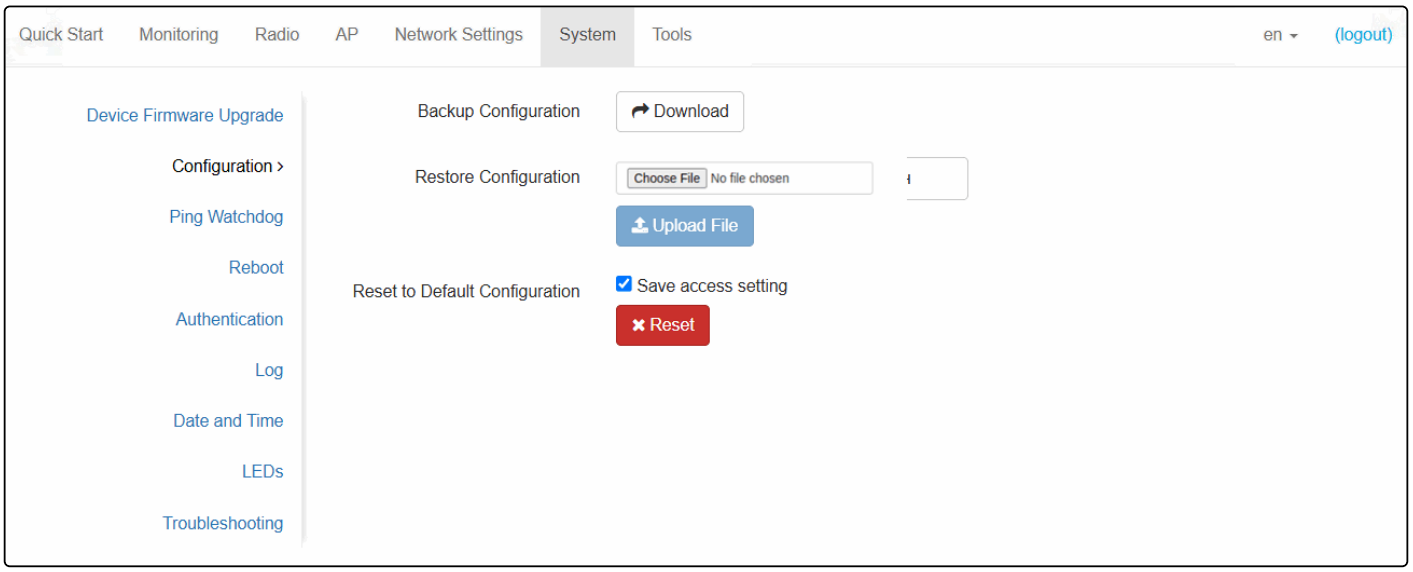
Download the firmware file from *http://eltex-co.com/support/downloads/* and save it on the PC. After that, click "Choose File" in the Firmware Image field and specify the path to the firmware file in .tar.gz format. To start the update process, click the "Start Upgrading" button. The process may take several minutes (its current status will be shown on the page). The device will be automatically rebooted when the upgrade is completed.

The firmware should be upgraded first on the client (STA) and then on the access point (AP).

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

10.12.2 "Configuration" submenu

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



Backup Configuration

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

Restore Configuration

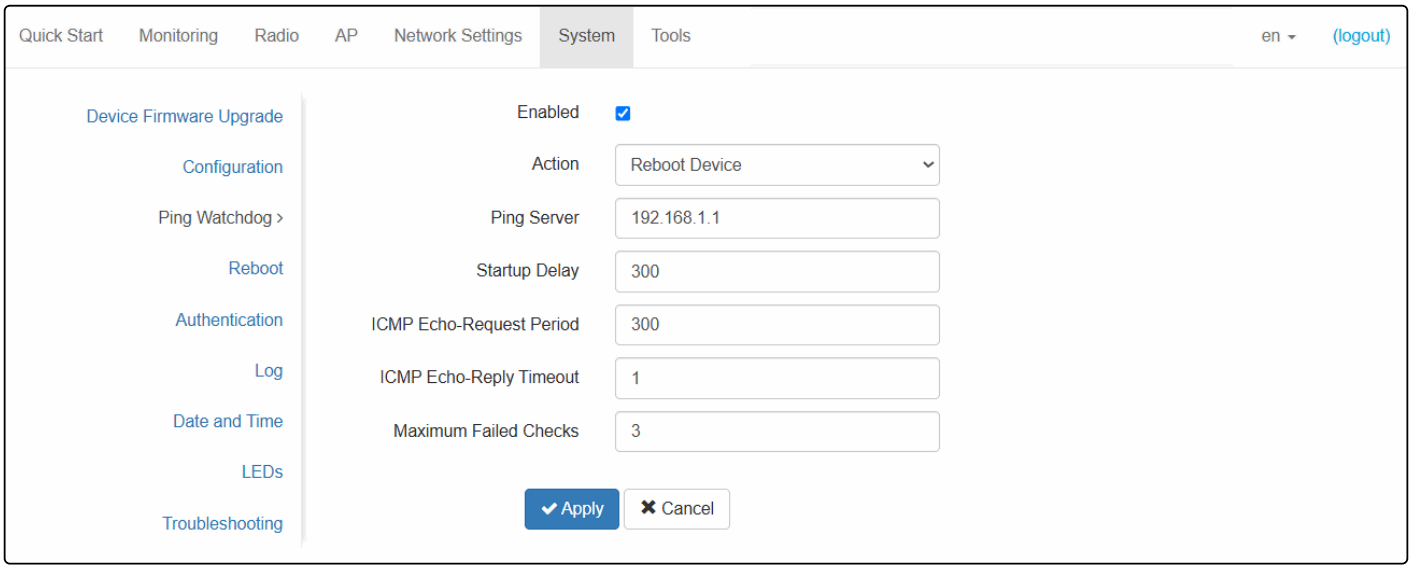
To upload the configuration file saved on the local computer, use the *Restore Configuration* item. To update the device configuration, click the "Chose File" button, specify a file (in .tar.gz format) and click the "Upload File" button. Uploaded configuration will be applied automatically and does not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

Reset to Default Configuration

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

10.12.3 "Ping Watchdog" submenu

The availability monitoring feature detects connectivity issues and reboots the device or its interfaces without user intervention. Restarting an interface also restarts the DHCP client on the current WAN interface.

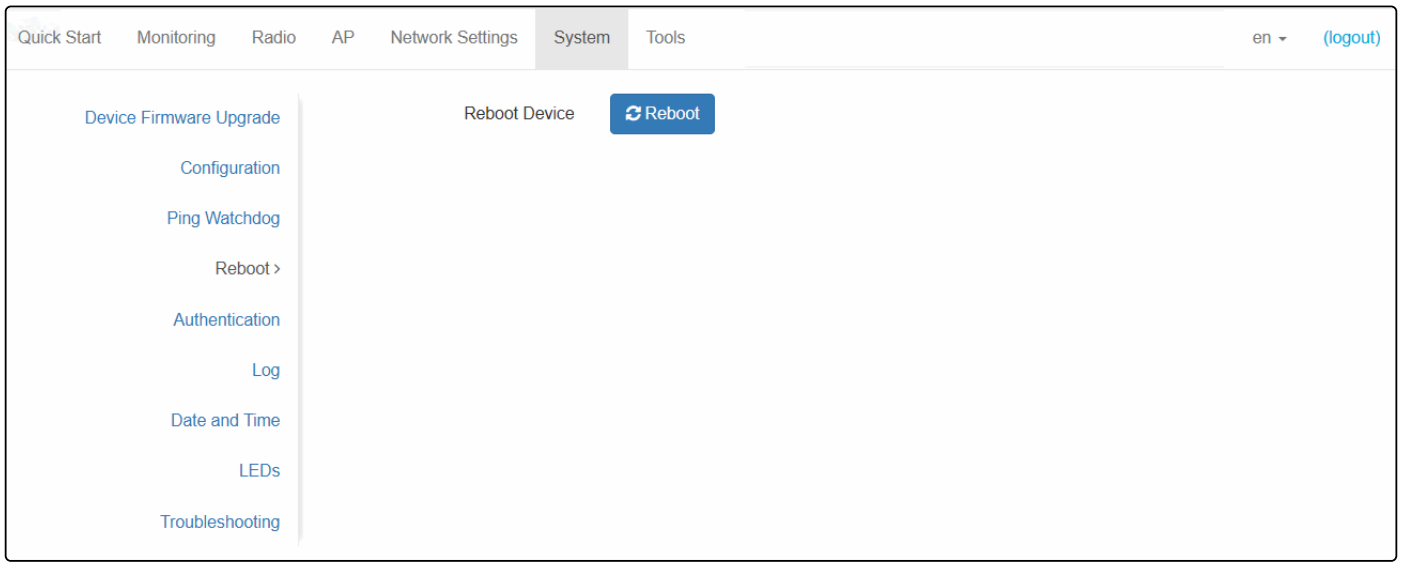


- *Enabled* — when checked, the ping watchdog feature is enabled, otherwise it is disabled;
- *Action:*
  - *Restart Ethernet Interface* — if the specified Ping server is unavailable, the device Ethernet interface will restart;
  - *Restart Wireless Interface* — if the specified Ping server is unavailable, the device wireless interface will restart;
  - *Reboot Device* — if the specified Ping server is unavailable, the device will reboot.
- *Ping Server* — IP address or host domain name, where ICMP requests will be sent;
- *Startup Delay* — time in seconds after the device is powered on or the previous trigger, during which the availability monitoring will not operate. Acceptable values: 60–86400 inclusive;
- *ICMP Echo-Request Period* — time in seconds after which an ICMP request will be sent when receiving an ICMP reply or deciding that the previous ICMP request was unsuccessful. Acceptable values: 1–86400 inclusive;
- *ICMP Echo-Reply Timeout* — time in seconds during which an ICMP reply is expected after sending an ICMP request. If an ICMP reply is not received within this time, the ICMP request is considered unsuccessful. Acceptable values: 1–10 inclusive;
- *Maximum Failed Checks* — maximum number of failed ICMP requests. If the number of failed ICMP requests reaches the specified value, the designated action is performed. Acceptable values: 1–86400 inclusive.

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

10.12.4 "Reboot" submenu

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



10.12.5 "Authentication" submenu

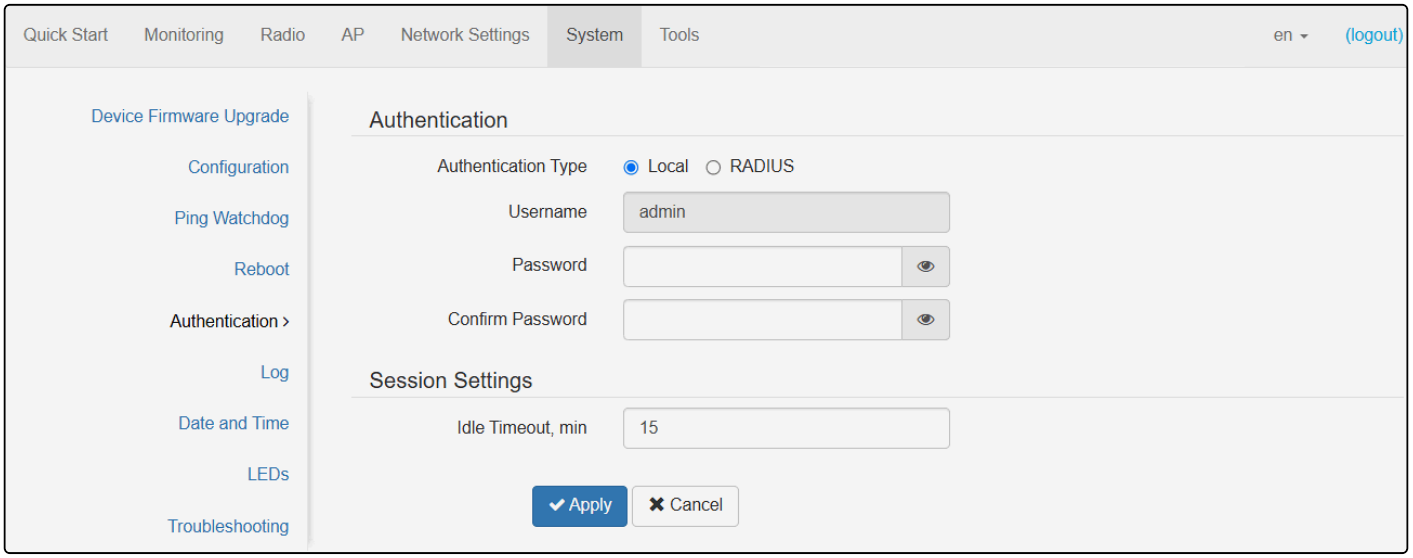
The **"Authentication"** submenu is used for configuring user authentication.

Authentication:

Factory account for device access: login: **admin**, password: **password**.

10.12.5.1 Local

When enabled, authentication is performed using an account stored on this device.

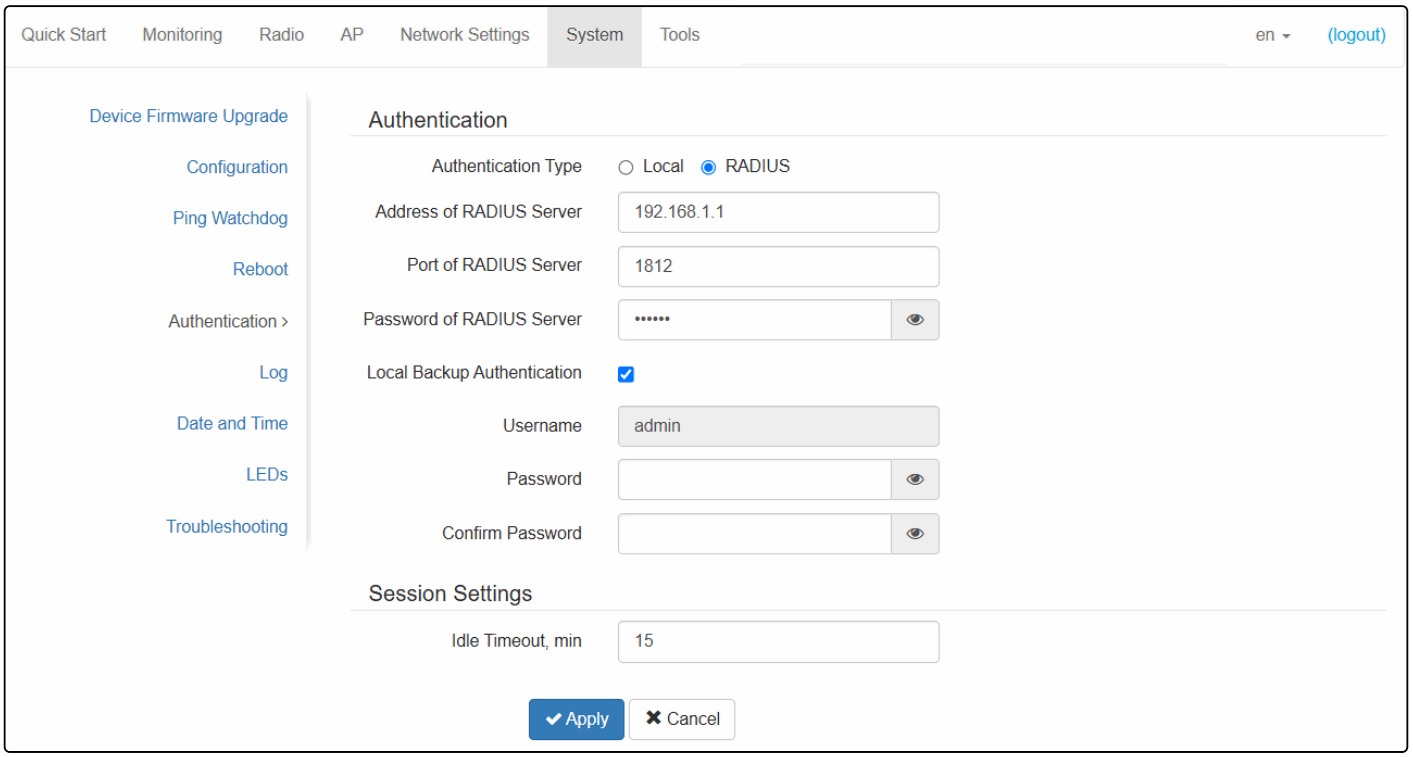


- *Username* — login of the configured account;
- *Password* — entering a new password;
- *Confirm Password* — confirming the new password.

Additional accounts with administrator or viewer roles can also be created (the setting is available only via CLI). Accounts with the administrator role have full access to the device: read and write access to any settings, full device status monitoring. Accounts with the viewer role have monitoring access only.

10.12.5.2 RADIUS

When enabled, authentication will be performed using an account on the RADIUS server.



- *Address of RADIUS server* — IP Address of RADIUS server;
- *Port of RADIUS server* — RADIUS server port used for authentication and authorization;
- *Password of RADIUS server* — RADIUS server key used for authentication and authorization;
- *Local Backup Authentication* — when enabled, local account authentication is activated **admin** when there is no connection with RADIUS server;
- *Username* — login of the configured account;
- *Password* — entering a new password;
- *Confirm Password* — confirming the new password.

With the **"Local Backup Authentication"** option disabled, authorization occurs only via RADIUS server. If the RADIUS server is unavailable or data is incorrect, authorization will fail.
With the **"Local Backup Authentication"** option enabled, if there is no connection with RADIUS server, authorization can be performed using a local **admin** account. Authorization through other local accounts will not be performed.

For authentication via RADIUS server, accounts with appropriate roles are created only on the server. Accounts can be assigned the following roles:
admin — user with this role will have full access device configuration and monitoring;
viewer — user with this role will only have access to device monitoring.
On the RADIUS server, the **Cisco-AVPair = "shell:role=<role>"** attribute is used to configure account roles (where **<role>** is either **admin** or **viewer**).

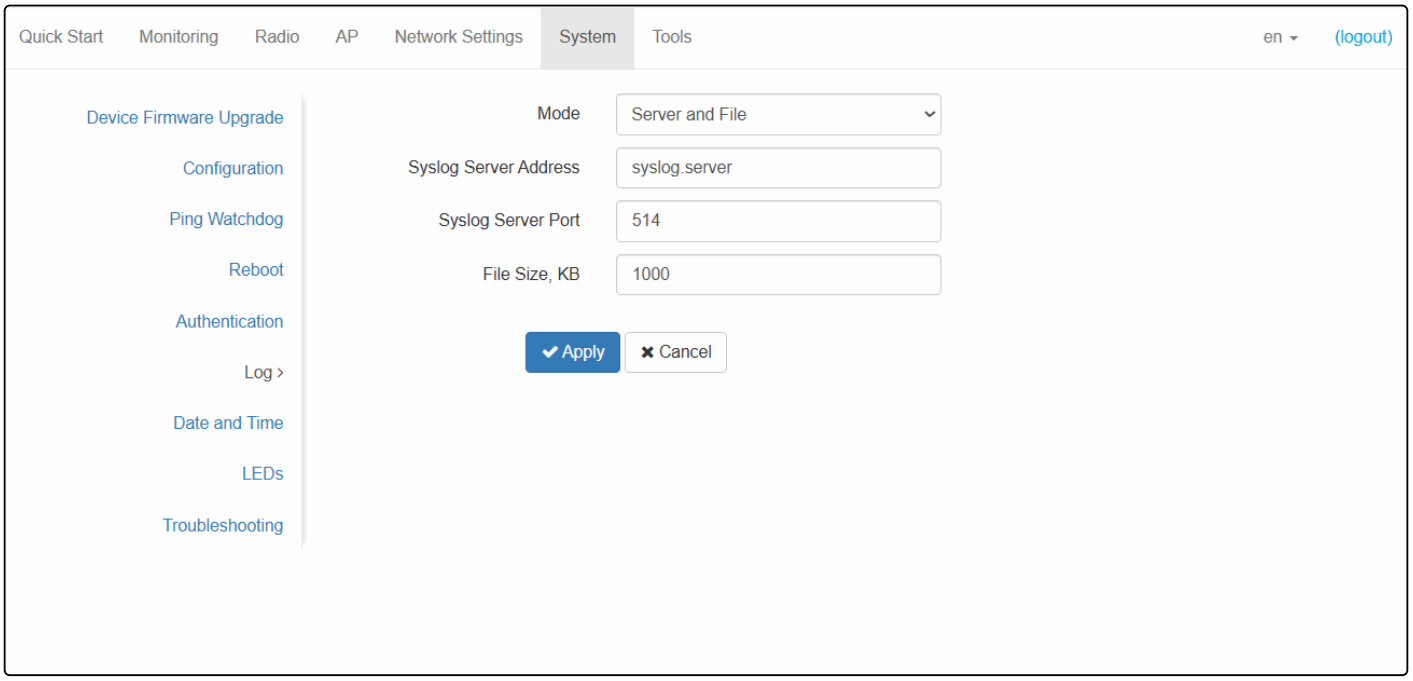
Session Settings:

- *Idle Timeout, min* — user idle time in minutes after which the session is terminated automatically.

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

10.12.6 "Log" submenu

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



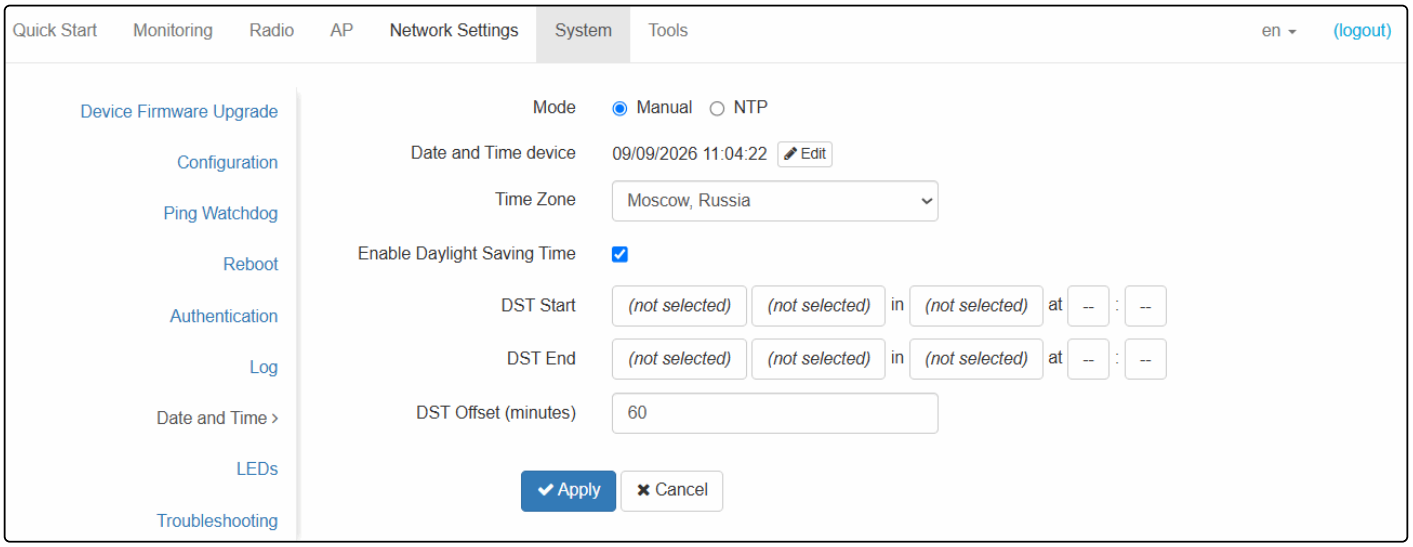
- *Mode* — Syslog agent operating mode:
  - *Local File* — log information is stored in a local file and is available in the "Events" submenu;
  - *Server and File* — log information is sent to a remote Syslog server and is saved to a local file.
- *Syslog Server Address* — IP address or domain name of the Syslog server;
- *Syslog Server Port* — port for incoming Syslog server messages (default: 514, acceptable values: from 1 to 65535);
- *File Size, KB* — maximum size of the log file (acceptable values: 1–1000 kB).

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

10.12.7 "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).

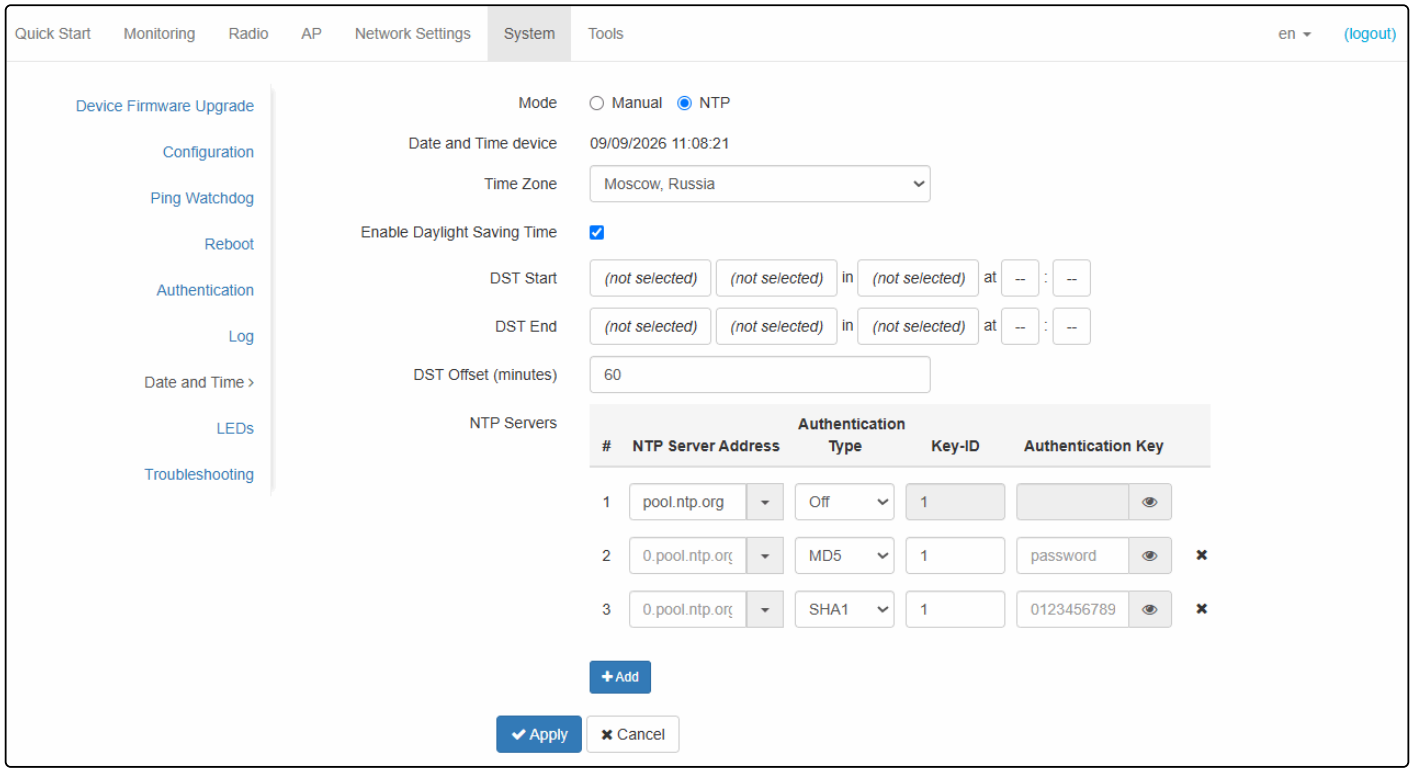
10.12.7.1 Manual



- *Date and Time device* — date and time on the device at the current moment. Click the "Edit" button to make corrections:
  - *Date, Time* — set the current date and time or click the "Set current date and time" button to synchronize with the device;
- *Time Zone* — allows to set the time zone according to the nearest city for your region from the list;
- *Enable daylight Saving Time* — when selected, automatic daylight saving change will be performed automatically within the defined time period:
  - *DST Start* — day and time, when daylight saving time starts;
  - *DST End* — day and time, when daylight saving time ends;
  - *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.

10.12.7.2 NTP Server

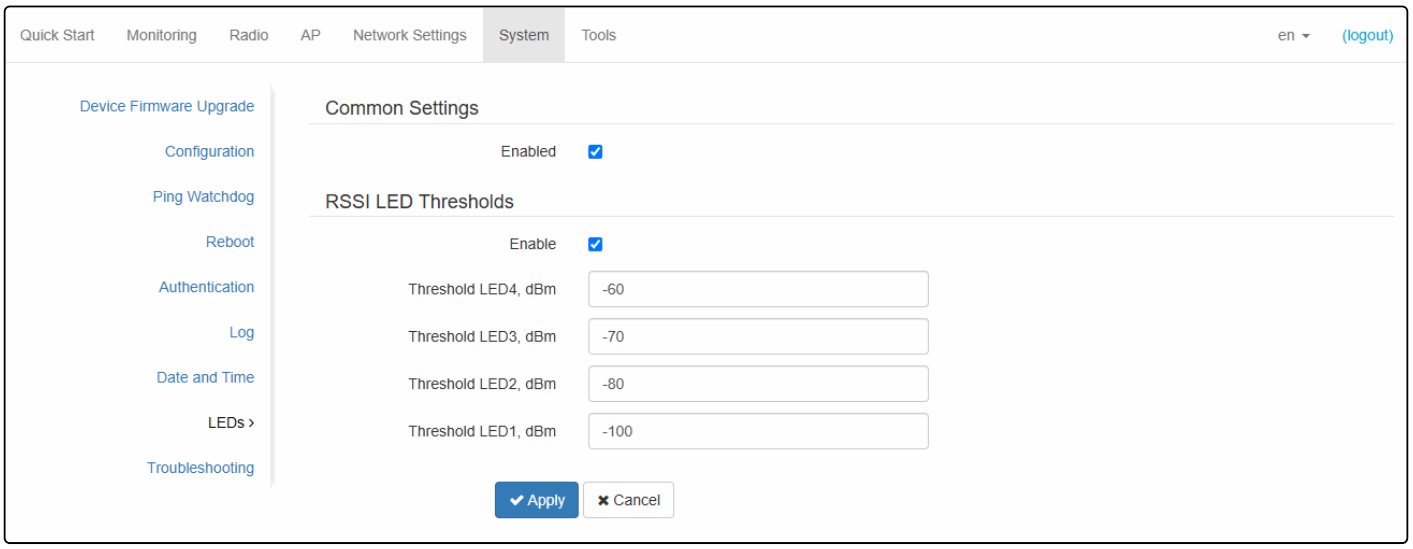


- *Date and Time devices* — current date and time on the device;
- *Time Zone* — sets the time zone according to the nearest city in your region from the given list;
- *Enable Daylight Saving Time* — when selected, automatic daylight saving change will be performed automatically within the defined time period:
  - *DST Start* — day and time, when daylight saving time starts;
  - *DST End* — day and time, when daylight saving time ends;
  - *DST Offset (minutes)* — time period in minutes, on which time offset is performing. The parameter can take a value from 0 to 720 minutes.
- *NTP Servers:*
  - *NTP Server Address* — IP address/domain name of the time synchronization server. An address can be specified or selected from the existing list;
  - *Authentication Type* — selection of a hashing algorithm for authentication of NTP packets. Possible values: Off, MD5, SHA1;
  - *Key-ID* — unique key number used for authentication during data exchange with NTP Server. Possible values: 1 to 65535;
  - *Authentication Key* — secret key for authentication in text format.

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

10.12.8 "LEDs" submenu

In the "**LEDs**" submenu, LEDs on the device can be customized.



Common settings:

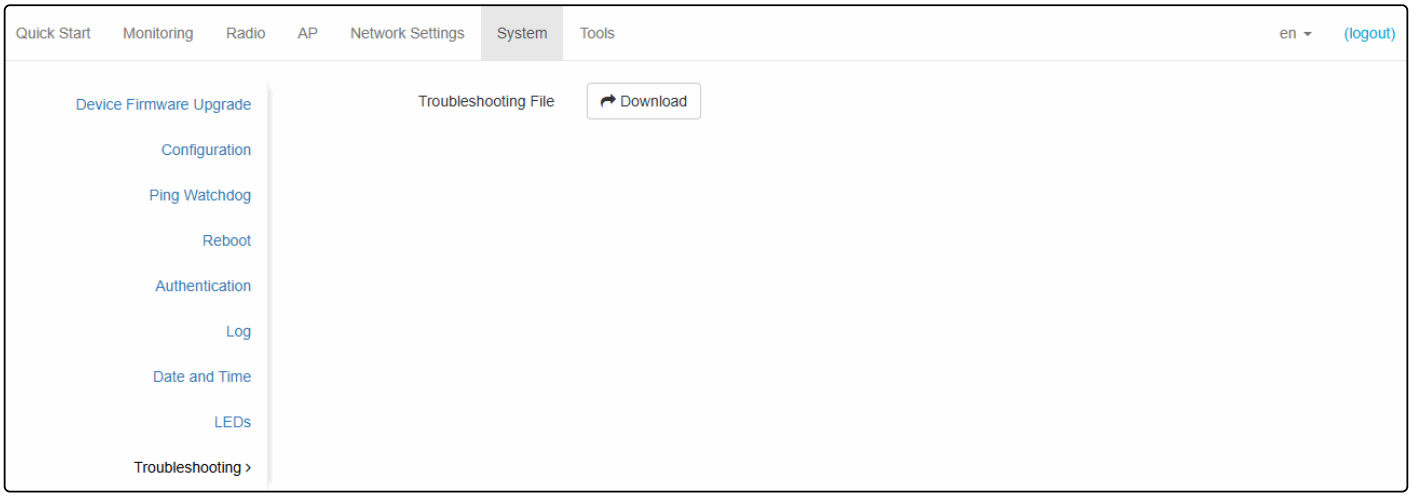
- *Enabled* — when checked, the indicators are enabled, otherwise they are disabled.

RSSI LED Threshold:

- *Enable* — when checked, the assignment of thresholds for each indicator is enabled, otherwise it is disabled;
- *Threshold LED4, dBm* — minimum signal level of a remote device (RSSI), at which LED4 turns on (by default: -60, acceptable values: -100–0);
- *Threshold LED3, dBm* — minimum signal level of a remote device (RSSI), at which LED3 turns on (by default: -70, acceptable values: -100–0);
- *Threshold LED2, dBm* — minimum signal level of a remote device (RSSI), at which LED2 turns on (by default: -80, acceptable values: -100–0);
- *Threshold LED1, dBm* — minimum signal level of a remote device (RSSI), at which LED1 turns on (by default: -100, acceptable values: -100–0).

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

10.12.9 "Troubleshooting" submenu



Troubleshooting File

To get *WB-3P-PTP6_SN_troubleshooting.tar.gz* archive from the device to a local computer, click "Download".

10.13 "Tools" menu

10.13.1 "Antenna Align" submenu

Alignment refers to adjusting the device antenna position in space to obtain the maximum signal.

To start alignment, click the "Start" button.

To stop alignment, click the "Stop" button.

Antenna Align:

- *SSID* — wireless network name;
- *Channel* — data channel;
- *RSSI, dBm* — received signal level, dBm;
- *Remote RSSI, dBm* — received signal level from the remote device, in dBm;
- *Estimated RSSI, dBm* — theoretical (expected) signal level value, dBm.



RSSI-H graph displays signal level changes on the first antenna in dBm over time in seconds.

RSSI-V graph displays signal level changes on the second antenna in dBm over time in seconds.

Remote RSSI-H graph displays signal level changes on the first antenna of the remote device in dBm over time in seconds.

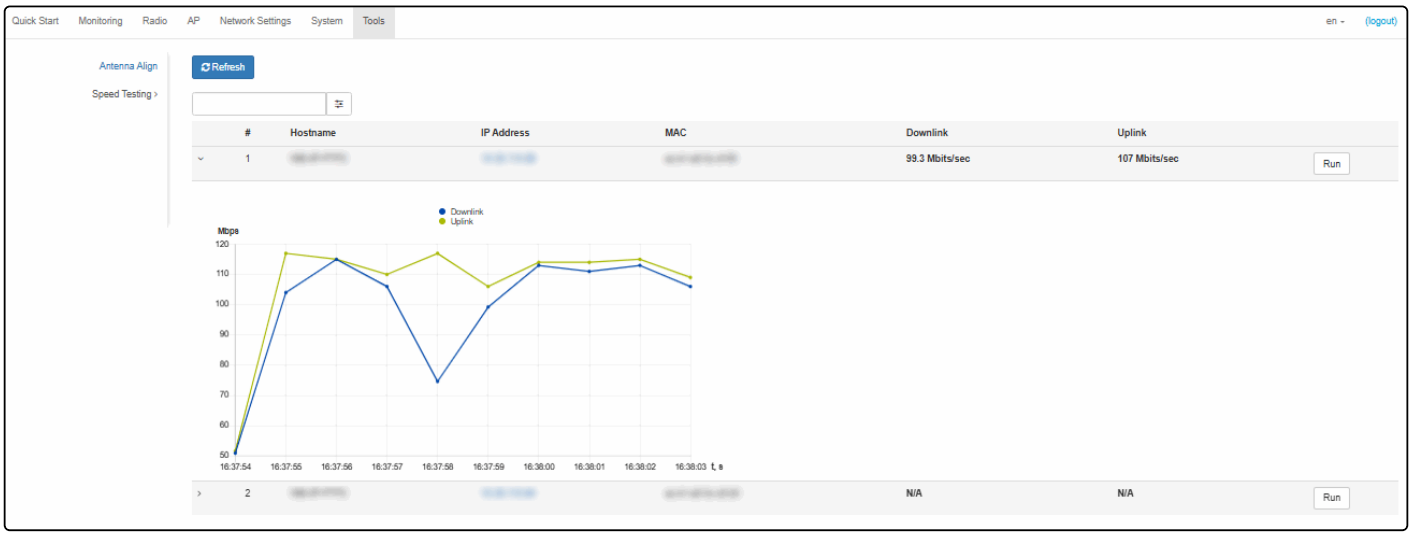
Remote RSSI-V graph displays signal level changes on the second antenna of the remote device in dBm over time in seconds.

Peak RSSI — maximum signal level in dBm during the measurement period. Red line.

Estimated RSSI — theoretical (expected) signal level value, dBm. Dashed green line.

10.13.2 "Speed Testing" submenu

The **"Speed Testing"** submenu is used for link speed testing.



The test operates in bidirectional mode (Downlink+Uplink). First, the inbound data flow rate is measured (Downlink), then outgoing (Uplink).

The test is performed with TCP traffic and lasts 10 seconds for one direction. At any given time, a test can only be run to one remote device.

To start, press the "Run" button. Upon test completion, the result will be displayed in the corresponding field and on the graph.

By default, the test uses VLAN 7 and subnet 192.0.4.0/24. If the network already uses such a subnet and VLAN, it is required to change the test settings so that they do not overlap with the existing networks. This can be done via the CLI. The process is described in more detail in the Perftest utility section .

The following filters are available for searching connected devices: by all fields, by hostname, by IP Address, by MAC. To select a filter, click on . The feature is available only in the "Access Point PMP" device mode.

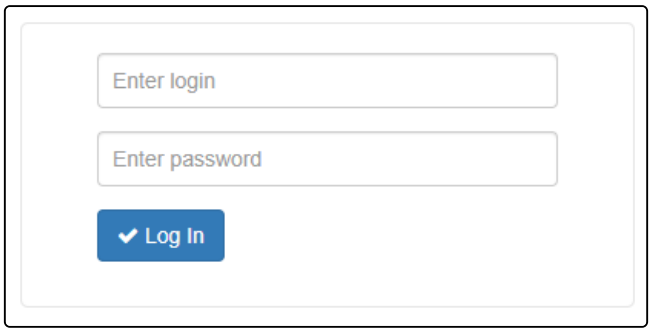
11 Example of device setup

This section provides an example of initial device setup for establishing a wireless bridge.



Figure 34 — WB-3P-PTP6 use case

In the browser address bar, enter the device IP address (by default **192.168.1.10**, if the device has not received an address via DHCP). Upon successful connection to the device, a window will appear asking for login and password. Fill in the fields and click the "Log In" button. By default — login: **admin**, password: **password**.



If this window does not appear, ensure the PC is on the same network as the device.

Configuring Access point (AP):

1. By default WB-3P-PTP6 is configured to receive an address via DHCP. If the address was not obtained, connect to the device using the factory IP Address: **192.168.1.10**, subnet mask: **255.255.255.0**.
2. The device firmware must be updated to the latest version as described in the Device Firmware Upgrade section.
3. In the "Radio" menu, perform preliminary radio interface configuration. Select the data channel and specify the distance between devices in kilometers.
4. Save the settings by clicking the "Apply" button.
5. In the "AP" menu in the "SSID" field, specify the wireless network identifier to which the client will connect (STA).
6. In the "Security Mode" field, select the security mode for network authentication and set the key if an encrypted network is used.
7. Save the settings by clicking the "Apply" button.

Configuring the client (STA) to connect to the access point (AP):

1. By default WB-3P-PTP6 is configured to receive an address via DHCP. If the address was not obtained, connect to the device using the factory IP Address: **192.168.1.10**, subnet mask: **255.255.255.0**.
2. The device firmware must be updated to the latest version as described in the section Device Firmware Upgrade.
3. If static or default settings are used to connect to the provider network, then in the "Network Settings" menu in the field "Protocol" you need to select a value "Static", fill in the fields "Static IP", "Network mask", "Gateway".
4. In the "STA" menu in the "SSID" field, specify the wireless network identifier to connect to.
5. In the "Security Mode" field, select the security mode for network authentication and set the key if an encrypted network is used.
6. After pressing the "Apply" button, client (STA) will search for the specified SSID in the air and will attempt to connect to the access point upon detection (AP) with the specified parameters.
7. Check that In the "Monitoring" menu in the "Wireless Peer" section an access point (AP) has appeared. Check the availability of the access point (AP) by entering the device's IP address into your browser's address bar.

If all the above items are completed successfully, the wireless connection between devices is configured.

12 Managing the device using the command line

To enter configuration mode, enter the command **configure.**
To display the current settings of a specific configuration section, enter the command **show-config.**
To get a hint about acceptable values for a device configuration parameter, press the key combination (in English keyboard layout) **[Shift + ?].**
To get a list of parameters available for editing in this configuration section, press the **Tab** key.
To save the settings, enter the **save** command.
To return to the previous configuration section, enter the **exit** command.
To exit configuration mode, enter the **end** command**.**

Configuration must begin with the client device to avoid losing connection to it.

12.1 Connection to the device

By default WB-3P-PTP6 is configured to receive an address via DHCP. If the address was not obtained, connect to the device using the factory IP Address.

The factory IP address for WB-3P-PTP6: **192.168.1.10**, subnet mask: **255.255.255.0**.

Connection to the device is performed using SSH:

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

12.2 Network parameters configuration

Configuring the static network parameters

WB-3P-PTP6(root):/# **configure**
WB-3P-PTP6(config):/# **interface**
WB-3P-PTP6(config):/interface# **br0**
WB-3P-PTP6(config):/interface/br0# **common**
WB-3P-PTP6(config):/interface/br0/common# **static-ip X.X.X.X** (where X.X.X.X — device IP address)
WB-3P-PTP6(config):/interface/br0/common# **netmask X.X.X.X** (where X.X.X.X — subnet mask)
WB-3P-PTP6(config):/interface/br0/common# **dns-server-1 X.X.X.X** (where X.X.X.X — IP address of the dns server №1)
WB-3P-PTP6(config):/interface/br0/common# **dns-server-2 X.X.X.X** (where X.X.X.X — IP address of the dns server №2)
WB-3P-PTP6(config):/interface/br0/common# **protocol static-ip** (changing the operating mode from DHCP to Static-IP)
WB-3P-PTP6(config):/interface/br0/common# **save** (saving settings)

Adding a static route

WB-3P-PTP6(config):/interface/br0/common# **exit**
WB-3P-PTP6(config):/interface/br0# **exit**
WB-3P-PTP6(config):/interface# **exit**
WB-3P-PTP6(config):/# **route**
WB-3P-PTP6(config):/route# **default**
WB-3P-PTP6(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)
WB-3P-PTP6(config):/route/default# **netmask X.X.X.X** (where X.X.X.X — destination network mask, for default route — 0.0.0.0)
WB-3P-PTP6(config):/route/default# **gateway X.X.X.X** (where X.X.X.X — gateway IP address)
WB-3P-PTP6(config):/interface/br0/common# **save** (saving settings)

Configuring the reception of network parameters via DHCP

WB-3P-PTP6(root):/# **configure**
WB-3P-PTP6(config):/# **interface**
WB-3P-PTP6(config):/interface# **br0**
WB-3P-PTP6(config):/interface/br0# **common**
WB-3P-PTP6(config):/interface/br0/common# **protocol dhcp** (changing the operating mode from Static-IP to DHCP)
WB-3P-PTP6(config):/interface/br0/common# **save** (saving settings)

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

Untagged access

Obtaining network settings via DHCP

WB-3P-PTP6(root):/# **set-management-vlan-mode off protocol dhcp**

Static settings

WB-3P-PTP6(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 network settings via DHCP

WB-3P-PTP6(root):/# **set-management-vlan-mode terminating vlan-id X protocol dhcp** (where X — VLAN ID, used for device access. Possible values: 1–4094)

Static settings

WB-3P-PTP6(root):/# **set-management-vlan-mode terminating vlan-id X protocol static-ip ip-addr X.X.X.X netmask Y.Y.Y.Y gateway Z.Z.Z.Z** (where X — VLAN ID, used for device access; possible values: 1–4094; X.X.X.X — static IP address; Y.Y.Y.Y — subnet mask; Z.Z.Z.Z — gateway)

Access via Management VLAN in Forwarding mode

Obtaining network settings via DHCP

WB-3P-PTP6(root):/# **set-management-vlan-mode forwarding vlan-id X protocol dhcp** (where X — VLAN ID, used for device access. Possible values: 1–4094)

Static settings

WB-3P-PTP6(root):/# **set-management-vlan-mode forwarding vlan-id X protocol static-ip ip-addr X.X.X.X netmask Y.Y.Y.Y gateway Z.Z.Z.Z** (where X — VLAN ID, used for device access; possible values: 1–4094; X.X.X.X — static IP address; Y.Y.Y.Y — subnet mask; Z.Z.Z.Z — gateway)

Completing and saving settings

WB-3P-PTP6(root):/# **save** (saving settings)

12.2.2 Configuring 802.1p priority for Management VLAN

802.1p priority in Terminating mode

WB-3P-PTP6(root):/# **configure**
WB-3P-PTP6(config):/# **interface**
WB-3P-PTP6(config):/interface# **management-vlan-terminating**
WB-3P-PTP6(config):/interface/management-vlan-terminating# **vlan**
WB-3P-PTP6(config):/interface/management-vlan-terminating/vlan# **priority X** (where X — 802.1p priority for Management VLAN. Possible values: 0–7)
WB-3P-PTP6(config):/interface/management-vlan-terminating/vlan# **save** (saving settings)

802.1p priority in Forwarding mode

WB-3P-PTP6(root):/# **configure**
WB-3P-PTP6(config):/# **interface**
WB-3P-PTP6(config):/interface# **management-vlan-forwarding**
WB-3P-PTP6(config):/interface/management-vlan-forwarding# **vlan**
WB-3P-PTP6(config):/interface/management-vlan-forwarding/vlan# **priority X** (where X — 802.1p priority for Management VLAN. Possible values: 0–7)
WB-3P-PTP6(config):/interface/management-vlan-forwarding/vlan# **save** (saving settings)

12.2.3 Remote management configuration

SSH configuration

WB-3P-PTP6(root):/# **configure**
WB-3P-PTP6(config):/# **ssh**
WB-3P-PTP6(config):/ssh# **enable true** (remote access management via SSH. To disable, enter **false**. By default: true)
WB-3P-PTP6(config):/ssh# **port X** (where X — SSH server port. By default: 22)
WB-3P-PTP6(config):/ssh# **save** (saving settings)

Telnet configuration

WB-3P-PTP6(root):/# **configure**
WB-3P-PTP6(config):/# **telnet**
WB-3P-PTP6(config):/telnet# **enable true** (remote access management via Telnet. To disable, enter **false**. By default: false)
WB-3P-PTP6(config):/telnet# **port X** (where X — port. By default: 23)
WB-3P-PTP6(config):/telnet# **save** (saving settings)

SNMPv2 configuration

WB-3P-PTP6(root):/# **configure**
WB-3P-PTP6(config):/# **snmp**
WB-3P-PTP6(config):/snmp# **enable true** (SNMP management. To disable, enter **false**. By default: true)
WB-3P-PTP6(config):/snmp# **rocommunity public** (where public — password for reading parameters)
WB-3P-PTP6(config):/snmp# **rwcommunity private** (where private — password for writing parameters)
WB-3P-PTP6(config):/snmp# **trapsink X.X.X.X** (where X.X.X.X — IP address or domain name of the SNMPv1-trap message receiver in format HOST [COMMUNITY [PORT]])
WB-3P-PTP6(config):/snmp# **trap2sink X.X.X.X** (where X.X.X.X — IP address or domain name of the SNMPv2-trap message receiver in format HOST [COMMUNITY [PORT]])
WB-3P-PTP6(config):/snmp# **informsink X.X.X.X** (where X.X.X.X — IP address or domain name of the Inform message receiver in format HOST [COMMUNITY [PORT]])
WB-3P-PTP6(config):/snmp# **sysname WB-3P-PTP6** (where WB-3P-PTP6 — device system name. By default: WB-3P-PTP6)
WB-3P-PTP6(config):/snmp# **syscontact Contact** (where Contact — contact information of the device manufacturer. By default: Contact)
WB-3P-PTP6(config):/snmp# **syslocation Russia** (where Russia — information about the device location. By default: Russia)
WB-3P-PTP6(config):/snmp# **trapcommunity trap** (where trap — password, contained in traps. By default: trap)
WB-3P-PTP6(config):/snmp# **save** (saving settings)

SNMPv3 configuration

WB-3P-PTP6(root):/# **configure**
WB-3P-PTP6(config):/# **snmp**
WB-3P-PTP6(config):/snmp# **enable true** (SNMP management. To disable, enter **false**. By default: true)
WB-3P-PTP6(config):/snmp# **view** (defines the range of OIDs available to specific user groups)
WB-3P-PTP6(config):/snmp/view# **add inc-all**
WB-3P-PTP6(config):/snmp/view# **inc-all**
WB-3P-PTP6(config):/snmp/view/inc-all# **rule** (defines access rights for different user groups to specific sections of the MIB configuration)
WB-3P-PTP6(config):/snmp/view/inc-all/rule# **add 1**
WB-3P-PTP6(config):/snmp/view/inc-all/rule# **1**
WB-3P-PTP6(config):/snmp/view/inc-all/rule/1# **type included** (where included — action type. Possible values: **included** — adding the specified OID, **excluded** — excluding the specified OID)
WB-3P-PTP6(config):/snmp/view/inc-all/rule/1# **subtree .1** (where .1 — given OID. If the group uses view with type = included and OID .1 as read-view, then OID .1 and all its children will be available for reading. If type = excluded, then all OIDs will be available except .1 and its children)
WB-3P-PTP6(config):/snmp/view/inc-all/rule/1# **exit**
WB-3P-PTP6(config):/snmp/view/inc-all/rule# **exit**
WB-3P-PTP6(config):/snmp/view/inc-all# **exit**
WB-3P-PTP6(config):/snmp/view# **exit**
WB-3P-PTP6(config):/snmp# **group** (set OID ranges for reading and writing, determines the security level)
WB-3P-PTP6(config):/snmp/group# **add rw** (where rw — group name. Used to bind users to a group)
WB-3P-PTP6(config):/snmp/group# **rw**
WB-3P-PTP6(config):/snmp/group/rw# **read-view inc-all** (where inc-all — view for reading parameters. Defines the range of OIDs available for reading)
WB-3P-PTP6(config):/snmp/group/rw# **write-view inc-all** (where inc-all — view for writing parameters. Defines the range of OIDs available for reading)
WB-3P-PTP6(config):/snmp/group/rw# **security-level priv** (where priv — security mode. Possible values: **noauth** — no security, **auth** — request authorization by username and password is used, **priv** — request

authorization by username and password is used, along with request and response encryption)
WB-3P-PTP6(config):/snmp/group/rw# **auth-type MD5** (where MD5 — authentication method. Possible values: **MD5**, **SHA**. It is used, if security-level = auth or priv. If not specified, then MD5 is used)
WB-3P-PTP6(config):/snmp/group/rw# **priv-type DES** (where DES — encryption method. Possible values: **DES**, **AES**. Used if security-level = priv. If not set, DES is used)
WB-3P-PTP6(config):/snmp/group/rw# **exit**
WB-3P-PTP6(config):/snmp/group# **exit**
WB-3P-PTP6(config):/snmp# **user** (user account. It is bound to a specific group and contains usernames and passwords for authorization and encryption)
WB-3P-PTP6(config):/snmp/user# **add admin** (where admin — username. Used for request authorization and can also be assigned for target)
WB-3P-PTP6(config):/snmp/user# **admin**
WB-3P-PTP6(config):/snmp/user/admin# **group rw** (where rw — group to which the user is added)
WB-3P-PTP6(config):/snmp/user/admin# **auth-password password** (where password — password for authorization. If the group security-level = auth or priv, and auth-password is not set, the user will not be available)
WB-3P-PTP6(config):/snmp/user/admin# **priv-password password** (where password — password for encryption. If the group security-level = priv, and priv-password is not set, the user will not be available)
WB-3P-PTP6(config):/snmp/user/admin# **exit**
WB-3P-PTP6(config):/snmp/user# **exit**
WB-3P-PTP6(config):/snmp# **target** (sends traps to the specified hosts. Added optionally. Analog trapsink and trap2sink for SNMPv3)
WB-3P-PTP6(config):/snmp/target# **add target1**
WB-3P-PTP6(config):/snmp/target# **target1**
WB-3P-PTP6(config):/snmp/target/target1# **host X.X.X.X** (where X.X.X.X — IP address host to which traps will be sent)
WB-3P-PTP6(config):/snmp/target/target1# **port X** (where X — port number to which traps will be sent)
WB-3P-PTP6(config):/snmp/target/target1# **user admin** (where admin — username used for sending trap messages. To change the radio channel, channel bandwidth, or other parameters. If an inactive user is specified (one of the required passwords is not set for it), then target will also be inactive)
WB-3P-PTP6(config):/snmp/target/target1# **exit**
WB-3P-PTP6(config):/snmp/target# **exit**
WB-3P-PTP6(config):/snmp# **snmpv3-only true** (enabling access denial to all OIDs via SNMPv1, SNMPv2. To disable, enter **false**. By default: false)
WB-3P-PTP6(config):/snmp# **save** (saving settings)

12.2.4 IPv6 network parameters configuration

By default access to the device via the protocol IPv6 is disabled on the device.

Enabling access to the device via IPv6 protocol

WB-3P-PTP6(root):/# **configure**
WB-3P-PTP6(config):/# **interface**
WB-3P-PTP6(config):/interface# **br0**
WB-3P-PTP6(config):/interface/br0# **common**
WB-3P-PTP6(config):/interface/br0/common# **ipv6**
WB-3P-PTP6(config):/interface/br0/common/ipv6# **protocol dhcp** (obtaining IPv6 network parameters via DHCP)
WB-3P-PTP6(config):/interface/br0/common/ipv6# **enabled true** (enabling access to the device via the IPv6 protocol. To disable, enter **false**)
WB-3P-PTP6(config):/interface/br0/common/ipv6# **save** (saving settings)

Configuring the static network parameters IPv6

WB-3P-PTP6(root):/# **configure**
WB-3P-PTP6(config):/# **interface**
WB-3P-PTP6(config):/interface# **br0**
WB-3P-PTP6(config):/interface/br0# **common**
WB-3P-PTP6(config):/interface/br0/common# **ipv6**
WB-3P-PTP6(config):/interface/br0/common/ipv6# **address XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX** (where XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX — static IPv6 address of the device)
WB-3P-PTP6(config):/interface/br0/common/ipv6# **address-prefix-length X** (where X — static IPv6 address prefix. Takes a value from 0 to 128. By default: 64)
WB-3P-PTP6(config):/interface/br0/common/ipv6# **gateway XXXX:XXXX:XXXX:XXXX::/64** (IPv6 prefix is specified, for example, 3211:0:0:1234::/64)
WB-3P-PTP6(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)
WB-3P-PTP6(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)
WB-3P-PTP6(config):/interface/br0/common/ipv6# **protocol static-ip** (enabling the use of static IPv6 networks parameters. To obtain IPv6 network parameters via DHCP enter **dhcp**)
WB-3P-PTP6(config):/interface/br0/common/ipv6# **enabled true** (enabling access to the device via the IPv6 protocol. To disable, enter **false**)
WB-3P-PTP6(config):/interface/br0/common/ipv6# **save** (saving settings)

12.3 Radio settings

To change the radio channel, channel bandwidth, or power, use the following commands:

Changing radio channel, bandwidth, and radio interface power

WB-3P-PTP6(root):/# **configure**
WB-3P-PTP6(config):/# **interface**
WB-3P-PTP6(config):/interface# **wlan0**
WB-3P-PTP6(config):/interface/wlan0# **wlan**
WB-3P-PTP6(config):/interface/wlan0/wlan# **radio**
WB-3P-PTP6(config):/interface/wlan0/wlan/radio# **tx-power X** (where X — power level in dBm)
WB-3P-PTP6(config):/interface/wlan0/wlan/radio# **channel X** (where X — static channel number on which the device will operate)
WB-3P-PTP6(config):/interface/wlan0/wlan/radio# **bandwidth X** (where X — channel width)
WB-3P-PTP6(config):/interface/wlan0/wlan/radio# **save** (saving settings)

Lists of available channels

In Radio 6 GHz for locations "Russia (RU)"/"Unlimited (ALL)" the following channels are available for selection:

- With channel bandwidth 20 MHz: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93.
- With channel bandwidth 40 MHz:
  - If "control-sideband" = lower: 1, 9, 17, 25, 33, 41, 49, 57, 65, 73, 81, 89.
  - If "control-sideband" = upper: 5, 13, 21, 29, 37, 45, 53, 61, 69, 77, 85, 93.
- With channel bandwidth 80 MHz: 1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61, 65, 69, 73, 77, 81, 85, 89, 93.
- With channel bandwidth 160 MHz: 1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61, 65, 69, 73, 77, 81, 85, 89, 93.

In Radio 6 GHz for locations "Russia (RU)"/"Unlimited (ALL)" the following channels are available for selection when fixed center frequency is enabled:

- With channel bandwidth 20 MHz: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93.
- With channel bandwidth 40 MHz: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91.
- With channel bandwidth 80 MHz: 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87.
- With channel bandwidth 160 MHz: 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79.

12.3.1 Advanced Radio settings

Changing the Country

WB-3P-PTP6(config):/interface/wlan0/wlan/radio# **country X** (parameter X can take a value: **RU**, **ALL**)

Changing the radio interface operating mode

WB-3P-PTP6(config):/interface/wlan0/wlan/radio# **work-mode X** (where X — radio interface operating mode in accordance with the IEEE 802.11 standard. Possible values: **ax**)

Changing the primary channel

WB-3P-PTP6(config):/interface/wlan0/wlan/radio# **control-sideband lower** (parameter can take the value: **lower**, **upper**. By default: lower)

Enabling fixed center frequency

WB-3P-PTP6(config):/interface/wlan0/wlan/radio# **center-frequency true** (enabling fixed center frequency. To disable, enter **false**)

Enabling the use of short guard interval

WB-3P-PTP6(config):/interface/wlan0/wlan/radio# **sgi true** (enabling the use of short guard interval for data transmission — 400 ns, instead 800 ns. To disable, enter **false**)

Configuring the limited list of channels

WB-3P-PTP6(config):/interface/wlan0/wlan/radio# **use-limit-channels true** (enabling the use of a limited channel list. To disable, enter **false**)
WB-3P-PTP6(config):/interface/wlan0/wlan/radio# **limit-channels '50 51 52'** (where 50 51 52 — are channels of range in which the configurable radio interface can operate)

Receiver sensitivity threshold

WB-3P-PTP6(config):/interface/wlan0/wlan/radio# **sensitivity-threshold-mode X** (where X — receiver sensitivity threshold mode. Takes values: **dynamic —** dynamic sensitivity adjustment; **fixed** — fixed receiver sensitivity threshold)
WB-3P-PTP6(config):/interface/wlan0/wlan/radio# **sensitivity-threshold X** (where X — receiver sensitivity threshold. Takes values: for 20 MHz channel bandwidth: from -95 dBm to -40 dBm; for 40 MHz channel bandwidth: from -92 dBm to -40 dBm; for 80 MHz channel bandwidth: from -89 dBm to -40 dBm; for 160 MHz channel bandwidth: from -86 dBm to -40 dBm)

Enabling STBC

WB-3P-PTP6(config):/interface/wlan0/wlan/radio# **stbc true** (enabling the Space-Time Block Coding (STBC) method, Designed to improve data transmission reliability. To disable, enter **false**)

Enabling aggregation

WB-3P-PTP6(config):/interface/wlan0/wlan/radio# **aggregation true** (enabling aggregation on Radio — support for AMPDU/AMSDU. To disable, enter **false**)

Enabling the use of short preamble

WB-3P-PTP6(config):/interface/wlan0/wlan/radio# **short-preamble true** (enabling the use of short packet preamble. To disable, enter **false**)

Enabling fixed channel data rate

WB-3P-PTP6(config):/interface/wlan0/wlan/radio# **fixed-rate X** (where X — modulation name in uppercase letters without spaces, for example, HE-NSS2-MCS10. Allowed values are determined by the radio interface operating mode and channel bandwidth)
WB-3P-PTP6(config):/interface/wlan0/wlan/radio# **enable-fixed-rate true** (enabling fixed channel data transfer rate. To disable, enter **false**)

Enabling maximum channel data transfer rate

WB-3P-PTP6(config):/interface/wlan0/wlan/radio# **maximal-rate-tx**
WB-3P-PTP6(config):/interface/wlan0/wlan/radio/maximal-rate-tx# **he X** (where X — modulation name in uppercase letters without spaces, for example, NSS2-MCS11. This parameter is used when connecting devices in IEEE 802.11ax mode)
WB-3P-PTP6(config):/interface/wlan0/wlan/radio/maximal-rate-tx# **enable true** (enabling maximum channel data transfer rate. To disable, enter **false**)
WB-3P-PTP6(config):/interface/wlan0/wlan/radio/qos# **save** (saving settings)

Enabling maximal channel data receive rate

WB-3P-PTP6(config):/interface/wlan0/wlan/radio# **maximal-rate-rx**
WB-3P-PTP6(config):/interface/wlan0/wlan/radio/maximal-rate-rx# **he X** (where X — modulation name in uppercase letters without spaces, for example, NSS2-MCS11. This parameter is used when connecting devices in IEEE 802.11ax mode)
WB-3P-PTP6(config):/interface/wlan0/wlan/radio/maximal-rate-rx# **enable true** (enabling maximal channel data receive rate. To disable, enter **false.** Access is only in **ap-ptp** and **sta** device modes)
WB-3P-PTP6(config):/interface/wlan0/wlan/radio/qos# **save** (saving settings)

Enabling minimal channel data receive rate

WB-3P-PTP6(config):/interface/wlan0/wlan/radio# **minimal-rate-rx**
WB-3P-PTP6(config):/interface/wlan0/wlan/radio/minimal-rate-rx# **he X** (where X — modulation name in uppercase letters without spaces, for example, NSS1-MCS0. This parameter is used when connecting devices in IEEE 802.11ax mode)
WB-3P-PTP6(config):/interface/wlan0/wlan/radio/minimal-rate-rx# **enable true** (enabling minimum channel data receive rate. To disable, enter **false**. Access is only in **ap-ptp** and **sta** device modes)
WB-3P-PTP6(config):/interface/wlan0/wlan/radio/qos# **save** (saving settings)

The maximal and minimal **receive** rate parameters are used to specify the maximal and minimal **transmit** rate to a remote device.
Therefore, when configuring maximal and/or minimal **receive** rate, for example, on a client (STA), there is no need to configure maximal and/or minimal **transmit** rate on an access point (AP).

Configuring Distance

WB-3P-PTP6(config):/interface/wlan0/wlan/radio# **auto-distance true** (enabling automatic distance calculation between devices. To disable, enter **false**)
WB-3P-PTP6(config):/interface/wlan0/wlan/radio# **max-distance X** (where X — distance between devices in kilometers. The parameter is used when auto-distance is disabled. Possible values: 0–34. By default: 0)

During the use of the antenna-align utility, automatic power control function is disabled.

Configuring ATPC

WB-3P-PTP6(config):/interface/wlan0/wlan/radio# **auto-tx-power**
WB-3P-PTP6(config):/interface/wlan0/wlan/radio/auto-tx-power# **enable true** (enabling automatic transmitter power control. To disable, enter **false**)
WB-3P-PTP6(config):/interface/wlan0/wlan/radio/auto-tx-power# **target-rssi X** (where X — target signal level. The parameter can take values from -100 to -40. By default: -50)

Configuring TDD

WB-3P-PTP6(config):/interface/wlan0/wlan/radio/tdd# **enable true** (enabling Time Division Duplex (TDD) technology, which synchronizes data transmission in both directions within a time frame. To disable, enter **false**)
WB-3P-PTP6(config):/interface/wlan0/wlan/radio/tdd# **flexible-mode true** (enabling automatic Downlink/Uplink ratio adjustment. To disable, enter **false**)
WB-3P-PTP6(config):/interface/wlan0/wlan/radio/tdd# **tx-ratio X** (where X — percentage of time slot in TDD frame, allocated for transmitting Downlink traffic. Possible values: 10, 20, 30, 40, 50, 60, 70, 80, 90. By default: 50)
WB-3P-PTP6(config):/interface/wlan0/wlan/radio/tdd# **frame-length X** (where X — TDD-frame duration in milliseconds. Possible values: 5, 10. By default: 10)
WB-3P-PTP6(config):/interface/wlan0/wlan/radio/tdd# **save** (saving settings)

Configuring the interval DTIM

WB-3P-PTP6(config):/interface/wlan0/wlan/radio# **dtim-interval X** (where X — DTIM interval. Possible values: 1–255. By default: 64)

Enabling QoS and changing parameters

WB-3P-PTP6(config):/interface/wlan0/wlan/radio# **qos**
WB-3P-PTP6(config):/interface/wlan0/wlan/radio/qos# **enable true** (when the option is enabled, the EDCA parameters are applied, specified in the configuration. To disable, enter **false**)
WB-3P-PTP6(config):/interface/wlan0/wlan/radio/qos# **edca-ap** (configuring device QoS parameters (traffic is transmitted in the direction to the client device))
WB-3P-PTP6(config):/interface/wlan0/wlan/radio/qos/edca-ap# **bk** (configuring EDCA parameters for the low-priority queue (priorities 802.1p: cs1, cs2))
WB-3P-PTP6(config):/interface/wlan0/wlan/radio/qos/edca-ap/bk# **aifs X** (where X — data frame waiting time, measured in slots. Takes values: 1–255)
WB-3P-PTP6(config):/interface/wlan0/wlan/radio/qos/edca-ap/bk# **cwmin X** (X — initial waiting time before retransmitting a frame, specified in milliseconds. Takes values: 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023. The cwMin value must not exceed the cwMax value)
WB-3P-PTP6(config):/interface/wlan0/wlan/radio/qos/edca-ap/bk# **cwmax X** (where X — maximal waiting time before retransmitting a frame, specified in milliseconds. Takes values: 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023. The cwMax value must be greater than the cwMin value)
WB-3P-PTP6(config):/interface/wlan0/wlan/radio/qos/edca-ap/bk# **txop X** (where X — time interval in milliseconds when the remote WME station has the right to initiate data transmission over the wireless medium to the device. Maximum value is 65535 milliseconds)
WB-3P-PTP6(config):/interface/wlan0/wlan/radio/qos/edca-ap/bk# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/radio/qos/edca-ap# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/radio/qos# **edca-sta** (configuring QoS parameters of a client device (traffic is transmitted in the direction from the client device))
WB-3P-PTP6(config):/interface/wlan0/wlan/radio/qos# **save** (saving settings)

The configuration method **edca-sta** is similar to the configuration method **edca-ap**.
Configuring parameters for queues **be**, **vi**, **vo** is similar to configuring parameters for the queue **bk**.

Configuring antenna parameters

WB-3P-PTP6(config):/interface/wlan0/wlan/radio/antenna-configuration# **type custom** (antenna type selection. The parameter can take the values: **internal** — integrated antenna; **custom** — custom antenna, **offset KU45/50CM** — offset parabolic antenna. By default: internal)
WB-3P-PTP6(config):/interface/wlan0/wlan/radio/antenna-configuration# **custom-gain X** (where X — antenna gain factor for the custom antenna type. Possible values: 0–40. By default: 0)
WB-3P-PTP6(config):/interface/wlan0/wlan/radio/antenna-configuration# **save** (saving settings)

12.4 Configuring DHCP option 82

Modes of operation DHCP snooping:

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

Changing the operating mode of DHCP options 82

WB-3P-PTP6(root):/# **configure**
WB-3P-PTP6(config):/# **interface**
WB-3P-PTP6(config):/interface# **wlan0**
WB-3P-PTP6(config):/interface/wlan0# **common**
WB-3P-PTP6(config):/interface/wlan0/common# **dhcp-snooping**
WB-3P-PTP6(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)
WB-3P-PTP6(config):/interface/wlan0/common/dhcp-snooping# **save** (saving settings)

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

Configuring option parameters 82

WB-3P-PTP6(config):/interface/wlan0/common/dhcp-snooping# **dhcp-option-82-CID-format custom** (where **custom** — replacing the CID content to the value specified in the **dhcp-option-82-customCID** parameter. The parameter can take the values: **APMAC-SSID** — replacing the CID content on <device MAC address>-<name SSID>. **SSID** — replacing the CID content to device SSID name. By default: APMAC-SSID)
WB-3P-PTP6(config):/interface/wlan0/common/dhcp-snooping# **dhcp-option-82-RID-format custom** (where **custom** — replacing the RID content to the value specified in the **dhcp-option-82-custom-RID** parameter. The parameter can take the values: **ClientMAC** — replacing the RID content on client device MAC. **APMAC** — replacing the RID content on device MAC address. **APdomain** — replacing the RID content to the domain where device is located. By default: ClientMAC)
WB-3P-PTP6(config):/interface/wlan0/common/dhcp-snooping# **dhcp-option-82-custom-CID longstring** (where **longstring** — value from 1 to 52 characters that will be transmitted to CID. If the parameter value **dhcp-option-82-custom-CID** is not set, the device will change CID to the default value: <device MAC address>-<SSID name>)
WB-3P-PTP6(config):/interface/wlan0/common/dhcp-snooping# **dhcp-option-82-custom-RID longstring** (where **longstring** — value from 1 to 63 characters that will be transmitted to RID. If the parameter value **dhcp-option-82-custom-RID** is not set, the device will change RID to the default value: <client device MAC >)
WB-3P-PTP6(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 character serves as a separator: AA-BB-CC-DD-EE-FF; **default** — a colon character serves as a separator: AA:BB:CC:DD:EE:FF)
WB-3P-PTP6(config):/interface/wlan0/common/dhcp-snooping# **save** (saving settings)

12.5 Configuring wireless network

Table 6 — Commands for configuring device mode

Device	Operating mode	Command for configuring the mode
Access Point (AP)	Access Point PTP	mode ap-ptp
Access Point (AP)	Access Point PMP	mode ap-pmp
Client (STA) / Station	Station / Client	mode sta

Table 7 — Commands for configuring security mode

Mode security	Command for configuring security mode
WPA3	mode WPA3
OWE	mode OWE
WPA3-Enterprise	mode WPA3_1X

12.5.1 Network settings for access point (AP)

Access point (AP) configuration with OWE

WB-3P-PTP6(root):/# **configure**
WB-3P-PTP6(config):/# **interface**
WB-3P-PTP6(config):/interface# **wlan0**
WB-3P-PTP6(config):/interface/wlan0# **wlan**
WB-3P-PTP6(config):/interface/wlan0/wlan# **mode ap-ptp** (device mode selection)
WB-3P-PTP6(config):/interface/wlan0/wlan# **ap**
WB-3P-PTP6(config):/interface/wlan0/wlan0/ap# **ssid WB-3P-PTP6** (change SSID name)
WB-3P-PTP6(config):/interface/wlan0/wlan0/ap# **ap-security** (enter the security mode settings)
WB-3P-PTP6(config):/interface/wlan0/wlan0/ap/ap-security# **mode OWE** (encryption mode OWE — encrypted connection without entering a password. Only Wi-Fi 6 clients will be able to connect in this mode)
WB-3P-PTP6(config):/interface/wlan0/wlan0/ap/ap-security# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan0/ap# **save** (saving settings)

Access point (AP) configuration with WPA-Personal security mode

WB-3P-PTP6(root):/# **configure**
WB-3P-PTP6(config):/# **interface**
WB-3P-PTP6(config):/interface# **wlan0**
WB-3P-PTP6(config):/interface/wlan0# **wlan**
WB-3P-PTP6(config):/interface/wlan0/wlan# **mode ap-ptp** (device mode selection)
WB-3P-PTP6(config):/interface/wlan0/wlan# **ap**
WB-3P-PTP6(config):/interface/wlan0/wlan0/ap# **ssid WB-3P-PTP6** (change SSID name)
WB-3P-PTP6(config):/interface/wlan0/wlan0/ap# **ap-security** (enter the security mode settings)
WB-3P-PTP6(config):/interface/wlan0/wlan0/ap/ap-security# **mode WPA3** (encryption mode — WPA3)
WB-3P-PTP6(config):/interface/wlan0/wlan0/ap# **key-wpa password123** (where password123 — key/password, required to connect to the wireless network. The key length must be from 8 to 63 characters)
WB-3P-PTP6(config):/interface/wlan0/wlan0/ap# **save** (saving settings)

Access point (AP) configuration with Enterprise authorization

WB-3P-PTP6(root):/# **configure**
WB-3P-PTP6(config):/# **interface**
WB-3P-PTP6(config):/interface# **wlan0**
WB-3P-PTP6(config):/interface/wlan0# **wlan**
WB-3P-PTP6(config):/interface/wlan0/wlan# **mode ap-ptp** (device mode selection)
WB-3P-PTP6(config):/interface/wlan0/wlan# **ap**
WB-3P-PTP6(config):/interface/wlan0/wlan0/ap# **ssid WB-3P-PTP6** (change SSID name)
WB-3P-PTP6(config):/interface/wlan0/wlan0/ap# **ap-security** (enter the security mode settings)
WB-3P-PTP6(config):/interface/wlan0/wlan0/ap/ap-security# **mode WPA3_1X** (encryption mode — WPA3-Enterprise)
WB-3P-PTP6(config):/interface/wlan0/wlan0/ap/ap-security# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan0/ap# **radius**
WB-3P-PTP6(config):/interface/wlan0/wlan0/ap/radius# **domain root** (where root — user domain)
WB-3P-PTP6(config):/interface/wlan0/wlan0/ap/radius# **auth-address X.X.X.X** (where X.X.X.X — IP Address of RADIUS server)
WB-3P-PTP6(config):/interface/wlan0/wlan0/ap/radius# **auth-port X** (where X — port of RADIUS server used for authentication and authorization. By default: 1812)
WB-3P-PTP6(config):/interface/wlan0/wlan0/ap/radius# **auth-password secret** (where secret — password for RADIUS server used for authentication and authorization)
WB-3P-PTP6(config):/interface/wlan0/wlan0/ap/radius# **acct-enable true** (enabling sending "Accounting" messages to the RADIUS server. By default: false)
WB-3P-PTP6(config):/interface/wlan0/wlan0/ap/radius# **acct-address X.X.X.X** (where X.X.X.X — IP Address of RADIUS server used for accounting)
WB-3P-PTP6(config):/interface/wlan0/wlan0/ap/radius# **acct-password secret** (where secret — password of RADIUS server used for accounting)
WB-3P-PTP6(config):/interface/wlan0/wlan0/ap/radius# **acct-periodic true** (enabling periodic sending "Accounting" message to RADIUS server. By default: false)
WB-3P-PTP6(config):/interface/wlan0/wlan0/ap/radius# **acct-interval 600** (interval for sending "Accounting" message" to RADIUS server)
WB-3P-PTP6(config):/interface/wlan0/wlan0/ap/radius# **save** (saving settings)

12.5.2 Advanced settings for access point (AP)

Destination VLAN-ID

WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **vlan-id X** (where X — VLAN-ID number)

Enabling VLAN trunk

WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **vlan-trunk true** (enabling VLAN Trunk. To disable, enter **false**)

Enabling General VLAN

WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **general-vlan-mode true** (enabling General VLAN on SSID. To disable, enter **false**)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **general-vlan-id X** (where X — General VLAN number)

Configuring C-VLAN

WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **customer-vlans**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/customer-vlans# **clients** (navigate to the clients section for configuring the matching list of user MAC address and VLAN-ID)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/customer-vlans/clients# **add XX:XX:XX:XX:XX:XX** (where XX:XX:XX:XX:XX:XX — MAC address of client device (STA), for which it is necessary to set C-VLAN. To remove an address from the list, use the command **del**)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/customer-vlans/clients# **XX:XX:XX:XX:XX:XX**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/customer-vlans/clients/XX:XX:XX:XX:XX:XX# **vlan-id X** (where X — VLAN-ID, which will be used as C-VLAN for the client devices (STA) with MAC XX:XX:XX:XX:XX:XX)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/customer-vlans/clients/XX:XX:XX:XX:XX:XX# **priority X** (where X — priority 802.1p value assigned to packets that are VLAN tagged using the C-VLAN functionality. Possible values: 0–7, auto. Default value: auto)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/customer-vlans/clients/XX:XX:XX:XX:XX:XX# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/customer-vlans/clients# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/customer-vlans# **enabled true** (enabling C-VLAN operation. To disable, enter **false**)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/customer-vlans# **save** (saving settings)

In case the access point is configured with Enterprise authorization and C-VLAN is specified for the client on RADIUS server, then this C-VLAN will be used for communication with this client, that means C-VLAN, configured on the access point, will be ignored. The VLAN value is transmitted to Tunnel-Private-Group-Id RADIUS attribute.

Configuring VLAN-ID 802.1p

WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **vlan-priority X** (where X — 802.1p priority value assigned to packets that are VLAN tagged using the VLAN-ID or General VLAN functionality. Possible values: 0–7, auto. Default value: auto)

Selecting the prioritization method

WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **priority-by-dscp false** (priority analysis from the CoS (Class of Service) field of tagged packets. Default value: true. In this case the priority from the field is analyzed DSCP header IP-packet)

Enabling hidden SSID

WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **hidden true** (enabling hidden SSID. To disable, enter **false**)

Enabling Minimal Signal and Roaming Signal

WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **check-signal-enable true** (enabling Minimal Signal. To disable, enter **false**)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **min-signal X** (where X — RSSI threshold value, upon reaching which client devices will be disconnected from the wireless network. The parameter can take values from -100 to -1)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **check-signal-timeout X** (where X — time period in seconds after which client devices are disconnected from the wireless network)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **roaming-signal X** (where X — RSSI threshold value, upon reaching which client devices will be switched to another device. The parameter can take values from -100 to -1. The roaming-signal parameter must be higher than min-signal: if min-signal = -75 dBm, then roaming-signal must be equal to, for example, -70 dBm)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **save** (saving settings)

Configuring data rate limit for the entire radio interface

Configuring the shaper in the direction from the client (STA) to the access point (AP):
WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **shaper-per-vap-rx**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/shaper-per-vap-rx# **value X** (where X — maximum speed in kbps or packets/s)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/shaper-per-vap-rx# **mode kbps** (enabling the shaper. Possible values: **kbps** — kbps, **pps** — packets/s, **off** — turned off)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/shaper-per-vap-rx# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **save** (saving settings)

Configuring the shaper in the direction from the access point (AP) to the client (STA):
WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **shaper-per-vap-tx**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/shaper-per-vap-tx# **value X** (where X — maximum speed in kbps or packets/s)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/shaper-per-vap-tx# **mode kbps** (enabling the shaper. Possible values: **kbps** — kbps, **pps** — packets/s, **off** — turned off)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/shaper-per-vap-tx# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **save** (saving settings)

Configuring data rate limit for each client (STA)

Configuring the shaper in the direction from the client (STA) to the access point (AP):

WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **shaper-per-sta-rx**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/shaper-per-sta-rx# **value X** (where X — maximum speed in kbps or packets/s)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/shaper-per-sta-rx# **mode kbps** (enabling the shaper. Possible values: **kbps** — kbps, **pps** — packets/s, **off** — turned off. Access is only in device mode **ap-pmp**)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/shaper-per-sta-rx# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **save** (saving settings)

Configuring the shaper in the direction from the access point (AP) to the client (STA):

WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **shaper-per-sta-tx**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/shaper-per-sta-tx# **value X** (where X — maximum speed in kbps or packets/s)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/shaper-per-sta-tx# **mode kbps** (enabling the shaper. Possible values: **kbps** — kbps, **pps** — packets/s, **off** — turned off. Access is only in device mode **ap-pmp**)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/shaper-per-sta-tx# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **save** (saving settings)

Configuring the broadcast traffic limit

Configuring the shaper in the direction from the client (STA) to the access point (AP):

WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **shaper-bcast-rx**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/shaper-bcast-rx# **value X** (where X — maximum speed in kbps or packets/s)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/shaper-bcast-rx# **mode kbps** (enabling the shaper. Possible values: **kbps** — kbps, **pps** — packets/s, **off** — turned off)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/shaper-bcast-rx# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **save** (saving settings)

Configuring the shaper in the direction from the access point (AP) to the client (STA):

WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **shaper-bcast-tx**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/shaper-bcast-tx# **value X** (where X — maximum speed in kbps or packets/s)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/shaper-bcast-tx# **mode kbps** (enabling the shaper. Possible values: **kbps** — kbps, **pps** — packets/s, **off** — turned off)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/shaper-bcast-tx# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **save** (saving settings)

Configuring the multicast traffic limit

Configuring the shaper in the direction from the access point (AP) to the client (STA):

WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **shaper-mcast-tx**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/shaper-mcast-tx# **value X** (where X — maximum speed in kbps or packets/s)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/shaper-mcast-tx# **mode kbps** (enabling the shaper. Possible values: **kbps** — kbps, **pps** — packets/s, **off** — disabled)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/shaper-mcast-tx# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **save** (saving settings)

Configuring the unknown traffic limit

Configuring the shaper in the direction from the access point (AP) to the client (STA):
WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **shaper-unknown-ucast-tx**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/shaper-unknown-ucast-tx:# **value X** (where X — maximum speed in kbps or packets/s)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/shaper-unknown-ucast-tx:# **mode kbps** (enabling the shaper. Possible values: **kbps** — kbps, **pps** — packets/s, **off** — disabled)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/shaper-unknown-ucast-tx:# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **save** (saving settings)

Configuring the unknown traffic limit

Configuring the shaper in the direction from the client (STA) to the access point (AP):
WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **shaper-unknown-ucast-rx**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/shaper-unknown-ucast-rx:# **value X** (where X — maximum speed in kbps or packets/s)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/shaper-unknown-ucast-rx:# **mode kbps** (enabling the shaper. Possible values: **kbps** — kbps, **pps** — packets/s, **off** — disabled)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/shaper-unknown-ucast-rx:# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **save** (saving settings)

Limiting the number of clients

WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **sta-limit X** (where X — maximum allowed number of client devices that can connect to the wireless network. Available only in **ap-pmp** device mode)

Enabling client isolation

WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **station-isolation true** (enabling traffic isolation between connected devices. To disable, enter **false**. Available only in **ap-pmp** device mode)

Configuring access control by MAC

WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **acl**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/acl# **mode local** (selecting the local mode — check by MAC list on the device)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/acl# **mac**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/acl/mac# **add XX:XX:XX:XX:XX:XX** (where XX:XX:XX:XX:XX:XX — MAC address of the device to which it is necessary to allow/deny access. To remove an address from the list, use the command **del**)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/acl/mac# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/acl# **policy allow** (selecting a policy. Possible values:
allow — allow connection only for devices with MAC addresses included in the list;
deny — to deny connection for devices with MAC addresses included in the list. By default: deny)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/acl# **enable true** (enabling access control by MAC. To disable, enter **false**)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/acl# **save** (saving settings)

Configuring access control by MAC via RADIUS-server

WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **acl**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/acll# **mode radius** (selecting the radius mode — check MACs via RADIUS server)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/acl# **policy allow** (selecting a policy. Possible values:
allow — allow connection only to clients approved by RADIUS server;
deny — deny connection to clients approved by RADIUS server. Default value: deny)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/acl# **enable true** (enabling access control by MAC via RADIUS server. To disable, enter **false**)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/acl# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/# **radius**
WB-3P-PTP6(config):/interface/wlan0/wlan0/ap/radius# **domain root** (where root — user domain)
WB-3P-PTP6(config):/interface/wlan0/wlan0/ap/radius# **auth-address X.X.X.X** (where X.X.X.X — IP Address of RADIUS server)
WB-3P-PTP6(config):/interface/wlan0/wlan0/ap/radius# **auth-port X** (where X — port of RADIUS server, used for authentication and authorization. By default: 1812)
WB-3P-PTP6(config):/interface/wlan0/wlan0/ap/radius# **auth-password secret** (where secret — password of RADIUS server, used for authentication and authorization)
WB-3P-PTP6(config):/interface/wlan0/wlan0/ap/radius# **acct-enable true** (enabling sending "Accounting" messages to RADIUS server. By default: false)
WB-3P-PTP6(config):/interface/wlan0/wlan0/ap/radius# **acct-address X.X.X.X** (where X.X.X.X — IP Address of RADIUS server used for accounting)
WB-3P-PTP6(config):/interface/wlan0/wlan0/ap/radius# **acct-password secret** (where secret — password of RADIUS server used for accounting)
WB-3P-PTP6(config):/interface/wlan0/wlan0/ap/radius# **acct-periodic true** (enabling periodic sending "Accounting" messages to RADIUS server. By default: false)
WB-3P-PTP6(config):/interface/wlan0/wlan0/ap/radius# **acct-interval 600** (interval of sending "Accounting" messages to RADIUS server)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/radius# **save** (saving settings)

Mapping VLAN

WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **vlan-mapping**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/vlan-mapping# **rule**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/vlan-mapping/rule# **add name1** (where name1 — mapping rule name. To remove a rule, use the command **del**)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/vlan-mapping/rule# **name1**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/vlan-mapping/rule/name1# **eth-vlan-id X** (where X — VLAN ID in Ethernet)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/vlan-mapping/rule/name1# **eth-priority X** (where X — 802.1p priority when transmitting to Ethernet. Possible values: 0–7, auto. If the priority is auto or not defined in this option — the original will be used)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/vlan-mapping/rule/name1# **wlan-vlan-id X** (where X — VLAN ID in WLAN)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/vlan-mapping/rule/name1# **wlan-priority X** (where X — 802.1p priority when transmitting in WLAN. Possible values: 0–7, auto. If the priority is auto or not defined in this option — the original will be used)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/vlan-mapping/rule/name1# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/vlan-mapping/rule# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/vlan-mapping# **enable true** (enabling vlan-mapping. To disable, enter **false**)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/vlan-mapping# **save** (saving settings)

There is a predefined rule in the vlan-mapping configuration — default-rule. It is used to change the 802.1p priority and WMM queue of all packets whose VLAN number does not match the user-defined rules.

Configuring default-rule

WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **vlan-mapping**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/vlan-mapping# **default-rule**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/vlan-mapping/default-rule# **eth-priority X** (where X — 802.1p priority when transmitting to Ethernet. Possible values: 0–7, auto. If the priority is auto or not defined in this option — the original will be used)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/vlan-mapping/default-rule# **wlan-priority X** (where X — 802.1p priority when transmitting in WLAN. Possible values: 0–7, auto. If the priority is auto or not defined in this option — the original will be used)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/vlan-mapping/default-rule# **wmm-queue X** (where X — WMM queue for this rule. Possible values: **bk**, **be**, **vi**, **vo**, **auto**. If the auto queue is not defined in this option, the DSCP priority will be analyzed in the packet)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/vlan-mapping/default-rule# **enable true** (enabling default-rule. To disable, enter **false**)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/vlan-mapping/default-rule# **save** (saving settings)

Priority by MAC

Configuring a rule for tagged traffic

WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **mac-priority**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/mac-priority# **rule**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/mac-priority/rule# **add name1** (where name1 — priority rule name by MAC. To remove a rule, use the command **del**)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/mac-priority/rule# **name1**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/mac-priority/rule/name1# **src-mac XX:XX:XX:XX:XX:XX** (where XX:XX:XX:XX:XX:XX — MAC address of source or client (STA) (more details about MAC configuration in the tip below). If the parameter is not set or its value is an empty string, it will not be used in matching)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/mac-priority/rule/name1# **dst-mac XX:XX:XX:XX:XX:XX** (where XX:XX:XX:XX:XX:XX — MAC address of recipient or client (STA) (more details about MAC configuration in the tip below). If the parameter is not set or its value is an empty string, it will not be used in matching)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/mac-priority/rule/name1# **wlan-priority X** (where X — 802.1p priority when transmitting in WLAN. Possible values: 0–7, auto. If the priority is auto or not defined in this option — the original will be used)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/mac-priority/rule/name1# **eth-priority X** (where X — 802.1p priority when transmitting to Ethernet. Possible values: 0–7, auto. If the priority is auto or not defined in this option — the original will be used)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/mac-priority/rule/name1# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/mac-priority/rule# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/mac-priority# **enable true** (enabling mac-priority. To disable, enter **false**)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/mac-priority# **save** (saving settings)

Configuring a rule for untagged traffic

WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **mac-priority**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/mac-priority# **rule**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/mac-priority/rule# **add name1** (where name1 — priority rule name by MAC. To remove a rule, use the command **del**)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/mac-priority/rule# **name1**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/mac-priority/rule/name1# **src-mac XX:XX:XX:XX:XX:XX** (where XX:XX:XX:XX:XX:XX — MAC address of source or client (STA) (more details about MAC configuration in the tip below). If the parameter is not set or its value is an empty string, it will not be used in matching)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/mac-priority/rule/name1# **dst-mac XX:XX:XX:XX:XX:XX** (where XX:XX:XX:XX:XX:XX — MAC address of recipient or client (STA) (more details about MAC configuration in the tip below). If the parameter is not set or its value is an empty string, it will not be used in matching)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/mac-priority/rule/name1# **wmm-queue X** (where X — WMM queue for this rule. Possible values: **bk**, **be**, **vi**, **vo**, **auto**. If the auto queue is not defined in this option, the DSCP priority will be analyzed in the packet)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/mac-priority/rule/name1# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/mac-priority/rule# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/mac-priority# **enable true** (enabling mac-priority. To disable, enter **false**)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/mac-priority# **save** (saving settings)

For packets going from the access point (AP) to the client (STA), **src-mac** parameter — source MAC address, **dst-mac** — MAC address of Client (STA).
For packets going from the client (STA) to the access point (AP), **src-mac** parameter — MAC address of client (STA), **dst-mac** — Recipient MAC address.

Priority by IP Address

Configuring a rule for tagged traffic

WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **ip-priority**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/ip-priority# **rule**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/ip-priority/rule# **add name1** (where name1 — priority rule name by IP. To remove a rule, use the command **del**)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/ip-priority/rule# **name1**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/ip-priority/rule/name1# **src-ip X.X.X.X** (where X.X.X.X — source IP Address: if the parameter is not set or its value is an empty string, it will not be used in matching)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/ip-priority/rule/name1# **dst-ip X.X.X.X** (where X.X.X.X — destination IP Address: if the parameter is not set or its value is an empty string, it will not be used in matching)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/ip-priority/rule/name1# **wlan-priority X** (where X — 802.1p priority when transmitting in WLAN. Possible values: 0–7, auto. If the priority is auto or not defined in this option — the original will be used)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/ip-priority/rule/name1# **eth-priority X** (where X — 802.1p priority when transmitting to Ethernet. Possible values: 0–7, auto. If the priority is auto or not defined in this option — the original will be used)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/ip-priority/rule/name1# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/ip-priority/rule# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/ip-priority# **enable true** (enabling ip-priority. To disable, enter **false**)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/ip-priority# **save** (saving settings)

Configuring a rule for untagged traffic

WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **ip-priority**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/ip-priority# **rule**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/ip-priority/rule# **add name1** (where name1 — priority rule name by IP. To remove a rule, use the command **del**)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/ip-priority/rule# **name1**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/ip-priority/rule/name1# **src-ip X.X.X.X** (where X.X.X.X — source IP Address: if the parameter is not set or its value is an empty string, it will not be used in matching)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/ip-priority/rule/name1# **dst-ip X.X.X.X** (where X.X.X.X — destination IP Address: if the parameter is not set or its value is an empty string, it will not be used in matching)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/ip-priority/rule/name1# **wmm-queue X** (where X — WMM queue for this rule. Possible values: **bk**, **be**, **vi**, **vo**, **auto**. If the auto queue is not defined in this option, the DSCP priority will be analyzed in the packet)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/ip-priority/rule/name1# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/ip-priority/rule# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/ip-priority# **enable true** (enabling ip-priority. To disable, enter **false**)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/ip-priority# **save** (saving settings)

If a packet matches more than one of the Vlan-Mapping, MAC-Priority, and IP-Priority rule types at the same time, the 802.1P priority assignment decision will be made based on the Priority-Order of the rule type, where 1 is the minimum priority and 100 is the maximum priority.
For example, if a packet matches a Vlan-Mapping rule with Priority-Order of 1, a MAC-priority with Priority-Order of 25, and an IP-priority with Priority-Order of 80, then this packet will be assigned a priority according to the IP-Priority rule, since it has the highest Priority-Order.

Priority order

WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **priority-order**
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/priority-order# **mac X** (where X — priority of this rule. Possible values: 1–100. The highest priority has the value 100)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/priority-order# **ip X** (where X — priority of this rule. Possible values: 1–100. The highest priority has the value 100)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/priority-order# **vlan X** (where X — priority of this rule. Possible values: 1–100. The highest priority has the value 100)
WB-3P-PTP6(config):/interface/wlan0/wlan/ap/priority-order# **save** (saving settings)

12.5.3 Network settings for client (STA)

In **sta** device mode, multiple access point (AP) connection profiles can be configured (up to 8 profiles).

Configuring the client (STA) with OWE

WB-3P-PTP6(root):/# **configure**
WB-3P-PTP6(config):/# **interface**
WB-3P-PTP6(config):/interface# **wlan0**
WB-3P-PTP6(config):/interface/wlan0# **wlan**
WB-3P-PTP6(config):/interface/wlan0/wlan# **mode sta** (device mode selection)
WB-3P-PTP6(config):/interface/wlan0/wlan# **sta**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta# **connection-profile**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/connection-profile# **profile**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/connection-profile/profile# **add profile1** (add a new profile. profile1 — connection profile name to AP. To remove a profile, use the command **del**)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/connection-profile/profile# **profile1**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/connection-profile/profile/profile1# **enable true** (enable profile)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/connection-profile/profile/profile1# **ssid WB-3P-PTP6** (change SSID name)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/connection-profile/profile/profile1# **security-mode OWE** (encryption mode OWE — encrypted connection without entering a password. Only Wi-Fi 6 clients will be able to connect in this mode)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/connection-profile/profile/profile1# **priority X** (where X — profile priority. Determines the order of profile usage. Possible values: 0–7. The highest priority has the value 7. When connecting a client (STA) the highest priority profile will be used first)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/connection-profile/profile/profile1# **save** (saving settings)

Configuring the client (STA) with WPA-Personal

WB-3P-PTP6(root):/# **configure**
WB-3P-PTP6(config):/# **interface**
WB-3P-PTP6(config):/interface# **wlan0**
WB-3P-PTP6(config):/interface/wlan0# **wlan**
WB-3P-PTP6(config):/interface/wlan0/wlan# **mode sta** (device mode selection)
WB-3P-PTP6(config):/interface/wlan0/wlan# **sta**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta# **connection-profile**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/connection-profile# **profile**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/connection-profile/profile# **add profile1** (add a new profile. profile1 — connection profile name to AP. To remove a profile, use the command **del**)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/connection-profile/profile# **profile1**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/connection-profile/profile/profile1# **enable true** (enable profile)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/connection-profile/profile/profile1# **ssid WB-3P-PTP6** (change SSID name)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/connection-profile/profile/profile1# **security-mode WPA3** (encryption mode — WPA3)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/connection-profile/profile/profile1# **key-wpa password123** (where password123 — key/password, required to connect to the wireless network. The key length must be from 8 to 63 characters)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/connection-profile/profile/profile1# **priority X** (where X — profile priority. Determines the order of profile usage. Possible values: 0–7. The highest priority has the value 7. When connecting a client (STA) the highest priority profile will be used first)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/connection-profile/profile/profile1# **save** (saving settings)

Configuring the client (STA) with Enterprise-authorization

WB-3P-PTP6(root):/# **configure**
WB-3P-PTP6(config):/# **interface**
WB-3P-PTP6(config):/interface# **wlan0**
WB-3P-PTP6(config):/interface/wlan0# **wlan**
WB-3P-PTP6(config):/interface/wlan0/wlan# **mode sta** (device mode selection)
WB-3P-PTP6(config):/interface/wlan0/wlan# **sta**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta# **connection-profile**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/connection-profile# **profile**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/connection-profile/profile# **add profile1** (add a new profile. profile1 — connection profile name to AP. To remove a profile, use the command **del**)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/connection-profile/profile# **profile1**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/connection-profile/profile/profile1# **enable true** (enable profile)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/connection-profile/profile/profile1# **ssid WB-3P-PTP6** (change SSID name)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/connection-profile/profile/profile1# **security-mode WPA3_1X** (encryption mode — WPA3-Enterprise)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/connection-profile/profile/profile1# **radius**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/connection-profile/profile/profile1/radius#
username user (where user — login, required for authorization on RADIUS server)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/connection-profile/profile/profile1/radius#
password password (where password — key/password, required for authorization on RADIUS server)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/connection-profile/profile/profile1# **priority X** (where X — profile priority. Determines the order of profile usage. Possible values: 0–7. The highest priority has the value 7. When connecting a client (STA) the highest priority profile will be used first)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/connection-profile/profile/profile1/radius# **save** (saving settings)

12.5.4 Advanced settings for client (STA)

Configuring VLAN-ID

WB-3P-PTP6(config):/interface/wlan0/wlan/sta# **vlan-id X** (where X — VLAN-ID number)

Enabling VLAN trunk

WB-3P-PTP6(config):/interface/wlan0/wlan/sta# **vlan-trunk true** (enabling VLAN Trunk. To disable, enter **false**)

Enabling General VLAN

WB-3P-PTP6(config):/interface/wlan0/wlan/sta# **general-vlan-mode true** (enabling General VLAN on SSID. To disable, enter **false**)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta# **general-vlan-id X** (where X — General VLAN number)

Enabling MVR

WB-3P-PTP6(config):/interface/wlan0/wlan/sta# **mvr-enable true** (enabling MVR. To disable, enter **false**)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta# **mvr-vlan-id X** (where X — VLAN number for Multicast traffic)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta# **mvr-vlan-priority X** (where X — 802.1p priority for IGMP packets from Ethernet devices behind the client (STA). Possible values: 0–7)

Configuring VLAN-ID 802.1p

WB-3P-PTP6(config):/interface/wlan0/wlan/ap# **vlan-priority X** (where X — 802.1p priority value assigned to packets that are VLAN tagged using the VLAN-ID or General VLAN functionality. Possible values: 0–7, auto. Default value: auto)

Selecting the prioritization method

WB-3P-PTP6(config):/interface/wlan0/wlan/sta# **priority-by-dscp false** (priority analysis from the field CoS (Class of Service) tagged packets. Default value: true. In this case, the priority from the DSCP field of the IP packet header is analyzed.

Configuring the speed limit

Configuring the shaper in the direction from the client (STA) to the access point (AP):
WB-3P-PTP6(config):/interface/wlan0/wlan/sta# **shaper-tx**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/shaper-tx# **value X** (where X — maximum speed in kbps or packets/s)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/shaper-tx# **mode kbps** (enabling the shaper. Possible values: **kbps** — kbps, **pps** — packets/s, **off** — disabled)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/shaper-tx# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta# **save** (saving settings)

Configuring the shaper in the direction from the access point (AP) to the client (STA):
WB-3P-PTP6(config):/interface/wlan0/wlan/sta# **shaper-rx**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/shaper-rx# **value X** (where X — maximum speed in kbps or packets/s)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/shaper-rx# **mode kbps** (enabling the shaper. Possible values: **kbps** — kbps, **pps** — packets/s, **off** — disabled)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/shaper-rx# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta# **save** (saving settings)

Configuring the broadcast traffic limit

Configuring the shaper in the direction from the access point (AP) to the client (STA):
WB-3P-PTP6(config):/interface/wlan0/wlan/sta# **shaper-bcast-rx**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/shaper-bcast-rx# **value X** (where X — maximum speed in kbps or packets/s)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/shaper-bcast-rx# **mode kbps** (enabling the shaper. Possible values: **kbps** — kbps, **pps** — packets/s, **off** — disabled)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/shaper-bcast-rx# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta# **save** (saving settings)

Configuring the shaper in the direction from the client (STA) to the access point (AP):
WB-3P-PTP6(config):/interface/wlan0/wlan/sta# **shaper-bcast-tx**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/shaper-bcast-rx# **value X** (where X — maximum speed in kbps or packets/s)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/shaper-bcast-rx# **mode kbps** (enabling the shaper. Possible values: **kbps** — kbps, **pps** — packets/s, **off** — disabled)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/shaper-bcast-rx# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta# **save** (saving settings)

Configuring the multicast traffic limit

Configuring the shaper in the direction from the access point (AP) to the client (STA):
WB-3P-PTP6(config):/interface/wlan0/wlan/sta# **shaper-mcast-rx**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/shaper-mcast-rx# **value X** (where X — maximum speed in kbps or packets/s)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/shaper-mcast-rx# **mode kbps** (enabling the shaper. Possible values: **kbps** — kbps, **pps** — packets/s, **off** — disabled)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/shaper-mcast-rx# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta# **save** (saving settings)

Configuring the unknown traffic limit

Configuring the shaper in the direction from the client (STA) to the access point (AP):
WB-3P-PTP6(config):/interface/wlan0/wlan/sta# **shaper-unknown-ucast-tx**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/shaper-unknown-ucast-tx:# **value X** (where X — maximum speed in kbps or packets/s)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/shaper-unknown-ucast-tx:# **mode kbps** (enabling the shaper. Possible values: **kbps** — kbps, **pps** — packets/s, **off** — disabled)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/shaper-unknown-ucast-tx:# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta# **save** (saving settings)

Configuring the unknown traffic limit

Configuring the shaper in the direction from the access point (AP) to the client (STA):
WB-3P-PTP6(config):/interface/wlan0/wlan/sta# **shaper-unknown-ucast-rx**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/shaper-unknown-ucast-rx:# **value X** (where X — maximum speed in kbps or packets/s)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/shaper-unknown-ucast-rx:# **mode kbps** (enabling the shaper. Possible values: **kbps** — kbps, **pps** — packets/s, **off** — disabled)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/shaper-unknown-ucast-rx:# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta# **save** (saving settings)

The remote device is configured similarly.

Increase MTU on interfaces

WB-3P-PTP6(config):/interface# **eth0**
WB-3P-PTP6(config):/interface/eth0# **common**
WB-3P-PTP6(config):/interface/eth0/common# **mtu X** (where X — MTU value. Maximum value is 2400)
WB-3P-PTP6(config):/interface/eth0/common# **exit**
WB-3P-PTP6(config):/interface/eth0# **exit**
WB-3P-PTP6(config):/interface# **wlan0**
WB-3P-PTP6(config):/interface/wlan0# **common**
WB-3P-PTP6(config):/interface/wlan0/common# **mtu X** (where X — MTU value. Maximum value is 2400)
WB-3P-PTP6(config):/interface/wlan0/common# **save** (saving settings)

Mapping VLAN

WB-3P-PTP6(config):/interface/wlan0/wlan/sta# **vlan-mapping**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/vlan-mapping# **rule**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/vlan-mapping/rule# **add name1** (where name1 — mapping rule name. To remove a rule, use the command **del**)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/vlan-mapping/rule# **name1**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/vlan-mapping/rule/name1# **eth-vlan-id X** (where X — VLAN ID in Ethernet)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/vlan-mapping/rule/name1# **eth-priority X** (where X — 802.1p priority when transmitting to Ethernet. Possible values: 0–7, auto. If the priority is auto or not defined in this option — the original will be used)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/vlan-mapping/rule/name1# **wlan-vlan-id X** (where X — VLAN ID in WLAN)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/vlan-mapping/rule/name1# **wlan-priority X** (where X — 802.1p priority when transmitting in WLAN. Possible values: 0–7, auto. If the priority is auto or not defined in this option — the original will be used)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/vlan-mapping/rule/name1# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/vlan-mapping/rule# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/vlan-mapping# **enable true** (enabling vlan-mapping. To disable, enter **false**)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/vlan-mapping# **save** (saving settings)

There is a predefined rule in the vlan-mapping configuration — default-rule. It is used to change the 802.1p priority and WMM queue of all packets whose VLAN number does not match the user-defined rules.

Configuration default-rule

WB-3P-PTP6(config):/interface/wlan0/wlan/sta# **vlan-mapping**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/vlan-mapping# **default-rule**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/vlan-mapping/default-rule# **eth-priority X** (where X — 802.1p priority when transmitting to Ethernet. Possible values: 0–7, auto. If the priority is auto or not defined in this option — the original will be used)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/vlan-mapping/default-rule# **wlan-priority X** (where X — 802.1p priority when transmitting in WLAN. Possible values: 0–7, auto. If the priority is auto or not defined in this option — the original will be used)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/vlan-mapping/default-rule# **wmm-queue X** (where X — WMM queue for this rule. Possible values: **bk**, **be**, **vi**, **vo**, **auto**. If the auto queue is not specified in this option, the DSCP priority in the packet will be analyzed)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/vlan-mapping/default-rule# **enable true** (enabling default-rule. To disable, enter **false**)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/vlan-mapping/default-rule# **save** (saving settings)

Priority by MAC

Configuring a rule for tagged traffic

WB-3P-PTP6(config):/interface/wlan0/wlan/sta# **mac-priority**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/mac-priority# **rule**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/mac-priority/rule# **add name1** (where name1 — priority rule name by MAC. To remove a rule, use the command **del**)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/mac-priority/rule# **name1**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/mac-priority/rule/name1# **src-mac XX:XX:XX:XX:XX:XX** (where XX:XX:XX:XX:XX:XX — MAC address of source or access point (AP) (more details about configuration MAC in the tip below). If the parameter is not set or its value is an empty string, it will not be used in matching)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/mac-priority/rule/name1# **dst-mac XX:XX:XX:XX:XX:XX** (where XX:XX:XX:XX:XX:XX — MAC address of recipient or access points (AP) (more details about configuration MAC in the tip below). If the parameter is not set or its value is an empty string, it will not be used in matching)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/mac-priority/rule/name1# **wlan-priority X** (where X — priority 802.1p when transmitting in WLAN. Possible values: 0–7, auto. If the priority auto or not defined in this option — the original will be used)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/mac-priority/rule/name1# **eth-priority X** (where X — priority 802.1p when transmitting to Ethernet. Possible values: 0–7, auto. If the priority auto or not defined in this option — the original will be used)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/mac-priority/rule/name1# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/mac-priority/rule# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/mac-priority# **enable true** (enabling mac-priority. To disable, enter **false**)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/mac-priority# **save** (saving settings)

Configuring a rule for untagged traffic

WB-3P-PTP6(config):/interface/wlan0/wlan/sta# **mac-priority**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/mac-priority# **rule**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/mac-priority/rule# **add name1** (where name1 — priority rule name by MAC. To remove a rule, use the command **del**)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/mac-priority/rule# **name1**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/mac-priority/rule/name1# **src-mac XX:XX:XX:XX:XX:XX** (where XX:XX:XX:XX:XX:XX — MAC source or access point (AP) (more details about MAC configuration is in the tip below). If the parameter is not set or its value is an empty string, it will not be used in matching)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/mac-priority/rule/name1# **dst-mac XX:XX:XX:XX:XX:XX** (where XX:XX:XX:XX:XX:XX — MAC recipient or access point (AP) (more details about MAC configuration is in the tip below). If the parameter is not set or its value is an empty string, it will not be used in matching)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/mac-priority/rule/name1# **wmm-queue X** (where X — WMM queue for this rule. Possible values: **bk**, **be**, **vi**, **vo**, **auto**. If the auto queue is not specified in this option, the DSCP priority in the packet will be analyzed)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/mac-priority/rule/name1# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/mac-priority/rule# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/mac-priority# **enable true** (enabling mac-priority. To disable, enter **false**)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/mac-priority# **save** (saving settings)

For packets going from access point (AP) to client (STA), **src-mac** is the MAC address of the access point (AP), **dst-mac** is the destination MAC address.
For packets going from client (STA) to access point (AP), **src-mac** is the source MAC address, **dst-mac** is the MAC address of the access point (AP).

Priority by IP Address

Configuring a rule for tagged traffic

WB-3P-PTP6(config):/interface/wlan0/wlan/sta# **ip-priority**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/ip-priority# **rule**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/ip-priority/rule# **add name1** (where name1 — priority rule name by IP. To remove a rule, use the command **del**)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/ip-priority/rule# **name1**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/ip-priority/rule/name1# **src-ip X.X.X.X** (where X.X.X.X — source IP Address: if the parameter is not set or its value is an empty string, it will not be used in matching)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/ip-priority/rule/name1# **dst-ip X.X.X.X** (where X.X.X.X — destination IP Address: if the parameter is not set or its value is an empty string, it will not be used in matching)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/ip-priority/rule/name1# **wlan-priority X** (where X — 802.1p priority when transmitting in WLAN. Possible values: 0–7, auto. If the priority is auto or not defined in this option — the original will be used)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/ip-priority/rule/name1# **eth-priority X** (where X — 802.1p priority when transmitting to Ethernet. Possible values: 0–7, auto. If the priority is auto or not defined in this option — the original will be used)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/ip-priority/rule/name1# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/ip-priority/rule# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/ip-priority# **enable true** (enabling ip-priority. To disable, enter **false**)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/ip-priority# **save** (saving settings)

Configuring a rule for untagged traffic

WB-3P-PTP6(config):/interface/wlan0/wlan/sta# **ip-priority**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/ip-priority# **rule**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/ip-priority/rule# **add name1** (where name1 — priority rule name by IP. To remove a rule, use the command **del**)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/ip-priority/rule# **name1**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/ip-priority/rule/name1# **src-ip X.X.X.X** (where X.X.X.X — source IP Address: if the parameter is not set or its value is an empty string, it will not be used in matching)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/ip-priority/rule/name1# **dst-ip X.X.X.X** (where X.X.X.X — destination IP Address: if the parameter is not set or its value is an empty string, it will not be used in matching)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/ip-priority/rule/name1# **wmm-queue X** (where X — WMM queue for this rule. Possible values: **bk**, **be**, **vi**, **vo**, **auto**. If the auto queue is not specified in this option, the DSCP priority in the packet will be analyzed)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/ip-priority/rule/name1# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/ip-priority/rule# **exit**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/ip-priority# **enable true** (enabling ip-priority. To disable, enter **false**)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/ip-priority# **save** (saving settings)

If a packet matches more than one of the Vlan-Mapping, MAC-Priority, and IP-Priority rule types at the same time, the 802.1P priority assignment decision will be made based on the Priority-Order of the rule type, where 1 is the minimum priority and 100 is the maximum priority.
For example, if a packet matches a Vlan-Mapping rule with Priority-Order of 1, a MAC-priority with Priority-Order of 25, and an IP-priority with Priority-Order of 80, then this packet will be assigned a priority according to the IP-Priority rule, since it has the highest Priority-Order.

Priority order

WB-3P-PTP6(config):/interface/wlan0/wlan/sta# **priority-order**
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/priority-order# **mac X** (where X — priority of this rule. Possible values: 1–100. The highest priority is 100)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/priority-order# **ip X** (where X — priority of this rule. Possible values: 1–100. The highest priority is 100)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/priority-order# **vlan X** (where X — priority of this rule. Possible values: 1–100. The highest priority is 100)
WB-3P-PTP6(config):/interface/wlan0/wlan/sta/priority-order# **save** (saving settings)

12.6 LoopBack Detection configuration

This functionality can be configured only in the **sta** device mode.

If a loop is detected on downstream equipment, the device blocks the Ethernet interface for the time specified in the configuration.

If the functionality is enabled, the client (STA) checks for loops on downstream equipment and, if any are detected, blocks the Ethernet interface for the time specified in the device configuration. The presence of loops is checked by sending special packets to the LAN network with the destination address cf:00:00:00:00:00.

Configuring LoopBack Detection

WB-3P-PTP6(root):/# **configure**
WB-3P-PTP6(config):/# **loopback-detection**
WB-3P-PTP6(config):/loopback-detection# **interval X** (where X — time interval between sending loop detection packets)
WB-3P-PTP6(config):/loopback-detection# **recovery-timer X** (where X — time during which the Ethernet interface will be locked)
WB-3P-PTP6(config):/loopback-detection# **vlan-id X** (where X — VLAN ID label, which will be attached to test packets. Possible values: 0–4094)
WB-3P-PTP6(config):/loopback-detection# **enabled true** (enabling LoopBack Detection. To disable, enter **false**)
WB-3P-PTP6(config):/loopback-detection# **save** (saving settings)

12.7 BPDU filter configuration

Configuring BPDU packet filtering for wlan0 interface

WB-3P-PTP6(root):/# **configure**
WB-3P-PTP6(config):/# **interface**
WB-3P-PTP6(config):/interface# **wlan0**
WB-3P-PTP6(config):/interface/wlan0# **common**
WB-3P-PTP6(config):/interface/wlan0/common# **bpdu-filter true** (enabling BPDU. To disable, enter **false**)
WB-3P-PTP6(config):/interface/wlan0/common# **save** (saving settings)

Configuring BPDU packet filtering for eth0 interface

WB-3P-PTP6(root):/# **configure**
WB-3P-PTP6(config):/# **interface**
WB-3P-PTP6(config):/interface# **eth0**
WB-3P-PTP6(config):/interface/eth0# **common**
WB-3P-PTP6(config):/interface/eth0/common# **bpdu-filter true** (enabling BPDU. To disable, enter **false**)
WB-3P-PTP6(config):/interface/eth0/common# **save** (saving settings)

12.8 MAC address learning limiting

Limiting the number of learned MACs

WB-3P-PTP6(root):/# **configure**
WB-3P-PTP6(config):/# **mac-learning**
WB-3P-PTP6(config):/mac-learning# **enabled true** (enabling the limit on the number of learned MACs. By default: false)
WB-3P-PTP6(config):/mac-learning# **mac-learning-limit X** (where X — global limit on the number of MACs (Wi-Fi + Ethernet). Possible values: 1–2048. By default: 2048, it is not recommended to change)
WB-3P-PTP6(config):/mac-learning# **wifi-mac-learning-limit X** (where X — limit on the number of MACs from Wi-Fi. Possible values: 1–2048. By default: 2048)
WB-3P-PTP6(config):/mac-learning# **eth-mac-learning-limit X** (where X — limit on the number of MACs from Ethernet. Possible values: 1–2048. By default: 2048)
WB-3P-PTP6(config):/mac-learning# **drop-unknown-unicast-src true** (enabling the restriction of traffic transmission from devices MAC addresses of which have not been learned due to exceeding any limitation of learned MAC addresses. To disable, enter **false**)
WB-3P-PTP6(config):/mac-learning# **drop-unknown-unicast true** (enabling the restriction of traffic forwarding to unknown MAC (only unicast). To disable, enter **false**)
WB-3P-PTP6(config):/mac-learning# **save** (saving settings)

12.9 Changing the MTU size on interfaces

The remote device is configured in a similar way.

Changing the MTU size on interfaces

WB-3P-PTP6(root):/# **configure**
WB-3P-PTP6(config):/# **interface**
WB-3P-PTP6(config):/interface# **eth0**
WB-3P-PTP6(config):/interface/eth0# **common**
WB-3P-PTP6(config):/interface/eth0/common# **mtu X** (where X — MTU size in bytes. Possible values: 68-2000. By default: 1500)
WB-3P-PTP6(config):/interface/eth0/common# **save** (saving settings)

The MTU value on the **br0**, **nas0** interfaces is set automatically, in accordance with the value on **eth0**. The MTU value on the **wlan0** interface is fixed and equals 2000.

12.10 System settings

12.10.1 Upgrading the device firmware

Device firmware update via TFTP

WB-3P-PTP6(root):/# **firmware upload tftp <IP Address of TFTP server><Firmware file name>** (example: firmware upload tftp 192.168.1.15 WB-3P-PTP6-2.6.1_build_X.tar.gz)
WB-3P-PTP6(root):/# **firmware upgrade**

Device firmware update via HTTP

WB-3P-PTP6(root):/# **firmware upload http <URL to download the firmware file>** (example: firmware upload https://eltex.ru/storage/upload_center/files/XX/WB-3P-PTP6-2.6.1_build_X.tar.gz)
WB-3P-PTP6(root):/# **firmware upgrade**

Switching to the firmware backup

WB-3P-PTP6(root):/# **firmware switch**

12.10.2 Device configuration management

Restore the default configuration without preserving the access parameters

WB-3P-PTP6(root):/# **manage-config reset-to-default**

Restore the default configuration while preserving access parameters

WB-3P-PTP6(root):/# **manage-config reset-to-default-without-management**

Download device configuration file to TFTP server

WB-3P-PTP6(root):/# **manage-config download tftp <IP Address of TFTP server>** (example: manage-config download tftp 192.168.1.15)

Download device configuration file to server/PC via SCP

scp <User>@<IP-device address>:/etc/config/config.json config.json (example: scp admin@192.168.1.15:/etc/config/config.json config.json. This command is executed on the server/PC)

Upload the configuration file to the device from TFTP server

WB-3P-PTP6(root):/# **manage-config upload tftp <IP Address of TFTP server> <configuration file name>** (example: manage-config upload tftp 192.168.1.15 config.json)
WB-3P-PTP6(root):/# **manage-config apply** (applying configuration)

12.10.3 Ping watchdog

The availability control feature (ping watchdog) allows one to detect a loss of network connectivity and reboot the device or its interfaces without user intervention. When an interface restarts, the DHCP client on the current WAN interface also restarts.

Configuring ping watchdog

WB-3P-PTP6(config):/ping-watchdog# **enable true** (enabling ping watchdog. By default: false)
WB-3P-PTP6(config):/ping-watchdog# **host X.X.X.X** (where X.X.X.X — IP Address of the recipient ICMP requests)
WB-3P-PTP6(config):/ping-watchdog# **ping-interval X** (where X — time in seconds after which an ICMP request will be sent after receiving an ICMP response or deciding that the previous ICMP request failed. Acceptable values: 1–86400. By default: 300)
WB-3P-PTP6(config):/ping-watchdog# **startup-delay X** (where X — time in seconds after the device is turned on or previously triggered, during which the ping watchdog will not work. Acceptable values: 60–86400. By default: 300)
WB-3P-PTP6(config):/ping-watchdog# **ping-timeout X** (where X — time in seconds during which an ICMP response to a sent ICMP request is expected. If no ICMP response is received after the time has elapsed, the ICMP request is considered unsuccessful. Acceptable values: 1–10. By default: 1)
WB-3P-PTP6(config):/ping-watchdog# **max-retry X** (where X — maximum number of failed ICMP requests. If the number of failed ICMP requests reaches the specified value, the defined action is performed. Possible values: 1–86400. By default: 3)
WB-3P-PTP6(config):/ping-watchdog# **action X** (where X — action. Possible values: **device-restart** — device reboot — if the specified ping server is unavailable, the device will restart; **ethernet-restart** — restart ethernet interface — if the specified ping server is unavailable, the device Ethernet interface will restart; **wireless-restart** — wireless interface restart — if the specified ping server is unavailable, the device wireless interface will restart)
WB-3P-PTP6(config):/ping-watchdog# **save** (saving settings)

12.10.4 Device reboot

Command to reboot the device

WB-3P-PTP6(root):/# **reboot**

Command for delayed device reboot

WB-3P-PTP6(root):/# **reboot delay X** (where X — time in seconds after which the scheduled device reboot will occur. Possible values: 0–86400)

Command for scheduling a device reboot at a specified time

WB-3P-PTP6(root):/# **reboot at hh:mm:ss** (where hh:mm:ss — time at which the scheduled device reboot will occur. Possible values: hh:mm, hh:mm:ss)

Command for canceling a scheduled device reboot

WB-3P-PTP6(root):/# **reboot cancel**

12.10.5 Configuring authentication mode

The device has a factory account **admin** with password **password**. This account cannot be deleted. The password can be changed using the commands below.

Changing the password for the account admin

WB-3P-PTP6(root):/# **configure**
WB-3P-PTP6(config):/# **authentication**
WB-3P-PTP6(config):/authentication# **admin-password <New password for account admin>**
from 1 to 64 characters, including Latin letters and digits)
WB-3P-PTP6(config):/authentication# **save** (saving settings)

Additional users can be created for local authentication and for authentication via RADIUS.

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

Additional users are created with the following commands:

Adding new users

WB-3P-PTP6(root):/# **configure**
WB-3P-PTP6(config):/# **authentication**
WB-3P-PTP6(config):/authentication# **user**
WB-3P-PTP6(config):/authentication/user# **add userX** (where userX — new account name. To remove, use the command **del**)
WB-3P-PTP6(config):/authentication/user# **userX**
WB-3P-PTP6(config):/authentication/user/userX# **login userX** (where userX — new account name)
WB-3P-PTP6(config):/authentication/user/userX# **password <Password for the account userX>** (from 1 to 64 characters, including Latin letters and digits)
WB-3P-PTP6(config):/authentication/user/userX# **role admin** (user is granted configuration privileges. Possible value: **viewer** — only monitoring will be available for the account)
WB-3P-PTP6(config):/authentication/user/userX# **save** (saving settings)

To authenticate via RADIUS server, access parameters should be configured:

Configuring access parameters to RADIUS server

WB-3P-PTP6(root):/# **configure**
WB-3P-PTP6(config):/# **authentication**
WB-3P-PTP6(config):/authentication# **radius**
WB-3P-PTP6(config):/authentication/radius# **auth-address X.X.X.X** (where X.X.X.X — IP Address of RADIUS server)
WB-3P-PTP6(config):/authentication/radius# **auth-port X** (where X — port of RADIUS server used for authentication and authorization. By default: 1812)
WB-3P-PTP6(config):/authentication/radius# **auth-password secret** (where secret — key for RADIUS server used for authentication and authorization)
WB-3P-PTP6(config):/authentication/radius# **exit**
WB-3P-PTP6(config):/authentication# **radius-local-fallback true** (enabling authorization via local account **admin** when there is no connection with RADIUS server. To disable, enter **false**. By default: false)
WB-3P-PTP6(config):/authentication# **radius-auth true** (enabling authentication mode via RADIUS server. To disable, enter **false**. By default: false)
WB-3P-PTP6(config):/authentication# **save** (saving settings)

With **radius-local-fallback** disabled, authorization occurs only via RADIUS server. If the server is unavailable or the credentials are incorrect, authorization will fail.
With **radius-local-fallback** enabled, if there is no connection to RADIUS server, authorization can be performed using the local **admin** account. Authorization through other local accounts will fail.

For authentication via RADIUS server: accounts with appropriate roles are created only on it.
Accounts can be assigned the following roles:
admin — a user with this role has full access to device configuration and monitoring;
viewer — a user with this role will have access only to device monitoring.
On RADIUS server: the following attribute is used to configure account roles **Cisco-AVPair = "shell:role=<role>"** (where **<role>** takes values **admin** or **viewer**).

Configuring the idle timeout

WB-3P-PTP6(root):/# **configure**
WB-3P-PTP6(config):/# **authentication**
WB-3P-PTP6(config):/authentication# **session-idle-timeout X** (where X — user idle time in minutes after which the session is terminated automatically. Possible values: 0–10080. To disable the feature, set the value **0**. By default: 15)
WB-3P-PTP6(config):/authentication# **save** (saving settings)

Configuring password validation

WB-3P-PTP6(root):/# **configure**
WB-3P-PTP6(config):/# **authentication**
WB-3P-PTP6(config):/authentication# **password-validation**
WB-3P-PTP6(config):/authentication/password-validation# **enable true** (where X — enabling password validation. To disable, enter **false**)
WB-3P-PTP6(config):/authentication/password-validation# **min-length X** (where X — minimum number of characters in a password. Possible values: 8–63. To disable the feature, set the value **0**. By default: 0)
WB-3P-PTP6(config):/authentication/password-validation# **character-classes-count X** (where X — minimum number of character classes that must be used in the password. Possible classes: lowercase letters, uppercase letters, digits, and special characters. Possible values: 1 — any single class is sufficient, 2 — any two classes are needed, 3 — any three classes are needed, 4 — all four classes are needed. By default: 1)
WB-3P-PTP6(config):/authentication# **save** (saving settings)

Configuring password expiration time limit

WB-3P-PTP6(root):/# **configure**
WB-3P-PTP6(config):/# **authentication**
WB-3P-PTP6(config):/authentication# **password-lifetime X** (where X — password validity period in days, after which a password change is required upon session termination. Possible values: 0–365. To disable the feature, set the value **0**. By default: 0)
WB-3P-PTP6(config):/authentication# **save** (saving settings)

12.10.6 Configuring DHCP-snooping

Commands for configuring DHCP snooping

WB-3P-PTP6(root):/# **configure**
WB-3P-PTP6(config):/# **dhcp-snooping**
WB-3P-PTP6(config):/dhcp-snooping# **enable true** (enabling DHCP snooping. To disable, enter **false**)
WB-3P-PTP6(config):/dhcp-snooping# **vlan** (configuring DHCP snooping for tagged traffic)
WB-3P-PTP6(config):/dhcp-snooping/vlan# **add vlan-group** (where vlan-group — VLAN group name, for which DHCP snooping will work)
WB-3P-PTP6(config):/dhcp-snooping/vlan# **vlan-group**
WB-3P-PTP6(config):/dhcp-snooping/vlan/vlan-group# **vid 'X;Y-Z'** (where X — VLAN number, Y–Z — range of VLANs that will be included in the vlan-group and for which DHCP snooping will work. Example of VLAN list configuration: vid '10;100-110')
WB-3P-PTP6(config):/dhcp-snooping/vlan/vlan-group# **exit**
WB-3P-PTP6(config):/dhcp-snooping/vlan# **exit**
WB-3P-PTP6(config):/dhcp-snooping# **untag true** (enabling DHCP snooping for untagged traffic. To disable, enter **false**)
WB-3P-PTP6(config):/dhcp-snooping# **save** (saving settings)

By default, only eth0 is considered a trusted port.

12.10.7 Configuring date and time

Commands for configuring time synchronization with NTP server

WB-3P-PTP6(root):/# **configure**
WB-3P-PTP6(config):/# **date-time**
WB-3P-PTP6(config):/date-time# **mode ntp** (enabling the operating mode with NTP. Possible value: **manual** — setting the time manually)
WB-3P-PTP6(config):/date-time# **ntp**
WB-3P-PTP6(config):/date-time/ntp# **servers**
WB-3P-PTP6(config):/date-time/ntp/servers# **add <name>** (adding NTP servers. Maximum number: 8. To remove, use the **del** command)
WB-3P-PTP6(config):/date-time/ntp/servers# **server1**
WB-3P-PTP6(config):/date-time/ntp/servers/server1# **address** (domain name/IP Address of NTP server in the configuration)
WB-3P-PTP6(config):/date-time/ntp/servers/server1# **key-id 1** (where 1 — unique key number used for authentication during data exchange with NTP server. Possible values: 1 to 65535)
WB-3P-PTP6(config):/date-time/ntp/servers/server1# **key-type MD5** (where MD5 — hash algorithm selection. Possible values: MD5, SHA1, off — disabling hash mode)
WB-3P-PTP6(config):/date-time/ntp/servers/server1# **key-value password** (where password — authentication secret key in text format)
WB-3P-PTP6(config):/date-time/ntp/servers/server1# **exit**
WB-3P-PTP6(config):/date-time/ntp/servers# **exit**
WB-3P-PTP6(config):/date-time/ntp# **exit**
WB-3P-PTP6(config):/date-time# **common**

WB-3P-PTP6(config):/date-time/common# **timezone 'Asia/Novosibirsk (Novosibirsk)'** (setting the time zone)
WB-3P-PTP6(config):/date-time/common# **save** (saving settings)

For the MD5 algorithm, the key length must be from 1 to 16 characters; the # character is not allowed. The SHA1 algorithm requires exactly 40 characters in hexadecimal format (digits 0–9 and letters a–f). key-id, key-type, and key-value are optional parameters. They are used only when connecting to an NTP server with authentication.

12.10.8 Advanced system settings

Changing the device name

WB-3P-PTP6(root):/# **configure**
WB-3P-PTP6(config):/# **system**
WB-3P-PTP6(config):/system# **hostname WB-3P-PTP6_2** (where WB-3P-PTP6_2 is a new device name. The parameter can contain from 1 to 63 characters: Latin uppercase and lowercase letters, digits, and the hyphen character "-" (a hyphen cannot be the last character in the name). By default: WB-3P-PTP6)
WB-3P-PTP6(config):/system# **save** (saving settings)

Changing the geographic domain

WB-3P-PTP6(root):/# **configure**
WB-3P-PTP6(config):/# **system**
WB-3P-PTP6(config):/system# **ap-location ap.test.root** (where ap.test.root — device tree node domain of the management system. By default: root)
WB-3P-PTP6(config):/system# **save** (saving settings)

Changing Radius NAS-ID

WB-3P-PTP6(root):/# **configure**
WB-3P-PTP6(config):/# **system**
WB-3P-PTP6(config):/system# **nas-id Lenina_1.Novovsibirsk.root** (where Lenina_1.Novovsibirsk.root — identifier of this device. This parameter is used to identify the device on the RADIUS server, in case if RADIUS expects a value other than MAC. By default: MAC devices)
WB-3P-PTP6(config):/system# **save** (saving settings)

Configuring LLDP

WB-3P-PTP6(root):/# **configure**
WB-3P-PTP6(config):/# **lldp**
WB-3P-PTP6(config):/lldp# **enabled true** (enabling LLDP functionality. To disable, enter **false**. By default: true)
WB-3P-PTP6(config):/lldp# **tx-interval X** (where X — changing the period for sending LLDP messages. Possible values: 1–86400. By default: 30)
WB-3P-PTP6(config):/lldp# **system-name WB-3P-PTP6_reserv** (where WB-3P-PTP6_reserv is a new device name. By default: WB-3P-PTP6)
WB-3P-PTP6(config):/lldp# **save** (saving settings)

Configuring indicators

WB-3P-PTP6(root):/# **configure**
WB-3P-PTP6(config):/# **led-manager**
WB-3P-PTP6(config):/led-manager# **enabled all** (enabling indicators. Can take values: **all** — all indicators are on, **none** — all indicators are off. By default: all)
WB-3P-PTP6(config):/led-manager# **enable-rssi-threshold-override true** (enabling control of RSSI indicator thresholds. To disable, enter **false**. By default: false)
WB-3P-PTP6(config):/led-manager# **led1-threshold X** (where X — minimum signal level from the remote device, at which the LED1 indicator turns on. Possible values: -100–0. By default: -100)
WB-3P-PTP6(config):/led-manager# **led2-threshold X** (where X — minimum signal level from the remote device, at which the LED2 indicator turns on. Possible values: -100–0. By default: -80)
WB-3P-PTP6(config):/led-manager# **led3-threshold X** (where X — minimum signal level from the remote device, at which the LED3 indicator turns on. Possible values: -100–0. By default: -70)
WB-3P-PTP6(config):/led-manager# **led4-threshold X** (where X — minimum signal level from the remote device, at which the LED4 indicator turns on. Possible values: -100–0. By default: -60)
WB-3P-PTP6(config):/led-manager# **save** (saving settings)

12.11 Monitoring

12.11.1 Wireless Peer/Wireless Clients

12.11.1.1 Device mode ap-ptp

Displaying useful information about the wireless peer status from the access point (AP):

WB-3P-PTP6(root):/# **monitoring wireless-peer**

```
 index                          | 0
hw-addr                         | ec:b1:e0:2d:a1:00
interface                       | wlan0
band                            | 6 GHz
state                           | ASSOC AUTH_SUCCESS
frequency                       | 5955 MHz
distance                        | 1 km
fbwa-mode                       | ptp-sta
serial-number                   | WP44000027
eltex-board-type                | WB-3P-PTP6
eltex-firmware-version          | 2.6.1 build X
factory-mac                     | EC:B1:E0:2D:A1:00
ssid                            | WB-3P-PTP6-AP
ip-addr                         | 192.168.1.15
hostname                        | WB-3P-PTP6-STA
rssi-h                          | -43 dBm
rssi-v                          | -53 dBm
snr-h                           | 22 dB
snr-v                           | 22 dB
noise-h                         | -65 dBm
noise-v                         | -75 dBm
rssi-remote-h                   | -46 dBm
rssi-remote-v                   | -48 dBm
snr-remote-h                    | 37 dB
snr-remote-v                    | 37 dB
link-quality-remote             | 100%
memory-usage-remote             | 61%
cpu-usage-remote                | 0.0%
noise-remote-h                  | -92 dBm
noise-remote-v                  | -92 dBm
tx-rate                         | HE NSS2 MCS9 LGI 195 Mbps
rx-rate                         | HE NSS2 MCS5 LGI 117 Mbps
tx-bw                           | 20M
rx-bw                           | 20M
uptime                          | 00:10:04
wireless-mode                   | ax
link-quality                    | 100%
link-quality-common             | 100%
actual-rx-pps                   | 0 pps
actual-tx-pps                   | 0 pps
actual-tx-rate                  | 0 Kbps
actual-rx-rate                  | 0 Kbps
link-capacity                   | 83 Mbps
```

Displaying brief information about the wireless peer status in horizontal view from the access point (AP):

WB-3P-PTP6(root):/# **monitoring wireless-peer brief**

```
Hostname         IP                RSSI, dBm  r-RSSI, dBm RX rate, Mbps           Uptime
                 MAC               SNR, dB    r-SNR, dB   TX rate, Mbps
---------------- ----------------- ---------- ----------- ----------------------  --------
WB-3P-PTP6-STA   192.168.1.15      -43/-54    -46/-48     HE NSS2 MCS7 LGI 146.3  00:02:42
                 ec:b1:e0:2d:a1:00 19/19      37/37       HE NSS2 MCS9 LGI 195
---------------- ----------------- ---------- ----------- ----------------------  --------
```

Displaying full information about the wireless peer status from the access point (AP):

WB-3P-PTP6(root):/# **monitoring wireless-peer detailed**

```
index                          | 0
hw-addr                        | ec:b1:e0:2d:a1:00
interface                      | wlan0
rfid                           | -1
wid                            | -1
band                           | 6 GHz
distance                       | 1 km
frequency                      | 5955 MHz
serial-number                  | WP44000027
eltex-board-type               | WB-3P-PTP6
eltex-firmware-version         | 2.6.1 build X
factory-mac                    | EC:B1:E0:2D:A1:00
state                          | ASSOC AUTH_SUCCESS
fbwa-mode                      | ptp-sta
ssid                           | WB-3P-PTP6-AP
vlan-id                        | 100
ip-addr                        | 192.168.1.15
channel                        | 1
hostname                       | WB-3P-PTP6-STA
dhcp-request-status            | obtained
eap-method                     | 0
rx-retry-count                 | 4
tx-fails                       | 0
tx-period-retry                | 0
tx-retry-count                 | 49
rssi-h                         | -42 dBm
rssi-v                         | -54 dBm
rssi                           | -54 dBm
max-rssi-h                     | -42 dBm
max-rssi-v                     | -51 dBm
max-rssi                       | -42 dBm
snr-h                          | 23 dB
snr-v                          | 23 dB
snr                            | 23 dB
noise-h                        | -65 dBm
noise-v                        | -77 dBm
noise                          | -65 dBm
rssi-remote-h                  | -46 dBm
rssi-remote-v                  | -48 dBm
rssi-remote                    | -48 dBm
snr-remote-h                   | 37 dB
snr-remote-v                   | 37 dB
snr-remote                     | 37 dB
link-quality-remote            | 100%
memory-usage-remote            | 61%
cpu-usage-remote               | 0.0%
tx-retry-ratio-remote          | 0%
rx-retry-ratio-remote          | 14%
utilization-remote             | 3
rx-utilization-remote          | 2
tx-utilization-remote          | 0
tx-power-remote                | 8 dBm
```

```
 system-uptime-remote               | 222:22:47
 link-capacity-remote               | 66 Mbps
 noise-remote-h                     | -93 dBm
 noise-remote-v                     | -93 dBm
 noise-remote                       | -93 dBm
 co-channel-interference-remote     | 0
 ap-interference-ratio-remote       | 3
 non-wifi-interference-remote       | 1
 packet-error-rate-remote           | 0
 tx-rate                            | HE NSS2 MCS11 LGI 243.8 Mbps
 tx-rate-numeric                    | 243.8
 rx-rate                            | HE NSS2 MCS7 LGI 146.3 Mbps
 rx-rate-numeric                    | 146.3
 rx-bw-all                          | 20M
 tx-bw                              | 20M
 rx-bw                              | 20M
 uptime                             | 00:03:56
 mfp                                | false
 wireless-mode                      | ax
 perftest-capable                   | true
 snr-rssi-capable                   | true
 link-quality                       | 91%
 link-quality-common                | 92%
 tx-retry-ratio                     | 0%
 rx-retry-ratio                     | 0%
 actual-tx-rate                     | 0 Kbps
 actual-rx-rate                     | 0 Kbps
 shaped-rx-rate                     | 0 Kbps
 actual-tx-pps                      | 1 pps
 actual-rx-pps                      | 0 pps
 shaped-rx-pps                      | 0 pps
 link-capacity                      | 91 Mbps
 multicast-groups-count             | 1
 using-802.11r                      | no
 using-802.11k                      | no
 using-802.11v                      | yes
 twt-support                        | none
 name                               | 0

Counter                 Transmitted               Received
----------------------  ------------------------  --------------------------
Total Packets:          627                       92
TX success:             100%                      0
Total Bytes:            51589                     5653
Data Packets:           541                       12
Data Bytes:             46962                     1616
Mgmt Packets:           86                        80
Mgmt Bytes:             4627                      4037
Dropped Packets:        0                         0
Dropped Bytes:          0                         0
Lost Packets:           0                         0

Rate             Transmitted                Received
---------------  ------------------------   -------------------------
mcs0             0              |   0%     4              |  33%
he-nss2-mcs3     0              |   0%     1              |   8%
he-nss2-mcs5     0              |   0%     1              |   8%
he-nss2-mcs7     4              |   0%     4              |  33%
```

```
he-nss2-mcs8      9              |   1%     2              |  16%
he-nss2-mcs9      127            |  23%     0              |   0%
he-nss2-mcs10     377            |  69%     0              |   0%
he-nss2-mcs11     24             |   4%     0              |   0%
-------------------------------------------------------------------------
   | Multicast groups                    | Clients                      |
-------------------------------------------------------------------------
   | MAC               | IP              | Count  | IP                  |
-------------------------------------------------------------------------
  0| 01:00:5e:00:00:6a |     xxx.0.0.106 |       1|   192.168.1.100(  0) |
-------------------------------------------------------------------------
```

12.11.1.2 Device mode ap-pmp

Displaying useful information about the wireless clients (STA) from the access point (AP):

WB-3P-PTP6(root):/# **monitoring clients**

```
index                          | 0
hw-addr                        | ec:b1:e0:2d:a1:00
interface                      | wlan0
band                           | 6 GHz
state                          | ASSOC AUTH_SUCCESS
frequency                      | 5955 MHz
distance                       | 1 km
fbwa-mode                      | pmp-sta
serial-number                  | WP44000027
eltex-board-type               | WB-3P-PTP6
eltex-firmware-version         | 2.6.1 build X
factory-mac                    | EC:B1:E0:2D:A1:00
ssid                           | WB-3P-PTP6-AP
ip-addr                        | 192.168.1.15
hostname                       | WB-3P-PTP6-STA
rssi-h                         | -43 dBm
rssi-v                         | -53 dBm
snr-h                          | 22 dB
snr-v                          | 22 dB
noise-h                        | -65 dBm
noise-v                        | -75 dBm
rssi-remote-h                  | -46 dBm
rssi-remote-v                  | -48 dBm
snr-remote-h                   | 37 dB
snr-remote-v                   | 37 dB
link-quality-remote            | 100%
memory-usage-remote            | 61%
cpu-usage-remote               | 0.0%
noise-remote-h                 | -92 dBm
noise-remote-v                 | -92 dBm
tx-rate                        | HE NSS2 MCS9 LGI 195 Mbps
rx-rate                        | HE NSS2 MCS5 LGI 117 Mbps
tx-bw                          | 20M
rx-bw                          | 20M
uptime                         | 00:10:04
wireless-mode                  | ax
link-quality                   | 100%
link-quality-common            | 100%
actual-rx-pps                  | 0 pps
actual-tx-pps                  | 0 pps
actual-tx-rate                 | 0 Kbps
actual-rx-rate                 | 0 Kbps
link-capacity                  | 83 Mbps
```

Displaying useful information about a wireless client (STA) from the access point side (AP):

WB-3P-PTP6(root):/# **monitoring clients station ec:b1:e0:2d:a1:00**

```
  index                          | 0
hw-addr                          | ec:b1:e0:2d:a1:00
interface                        | wlan0
band                             | 6 GHz
state                            | ASSOC AUTH_SUCCESS
frequency                        | 5955 MHz
distance                         | 1 km
fbwa-mode                        | pmp-sta
serial-number                    | WP44000027
eltex-board-type                 | WB-3P-PTP6
eltex-firmware-version           | 2.6.1 build X
factory-mac                      | EC:B1:E0:2D:A1:00
ssid                             | WB-3P-PTP6-AP
ip-addr                          | 192.168.1.15
hostname                         | WB-3P-PTP6-STA
rssi-h                           | -43 dBm
rssi-v                           | -53 dBm
snr-h                            | 22 dB
snr-v                            | 22 dB
noise-h                          | -65 dBm
noise-v                          | -75 dBm
rssi-remote-h                    | -46 dBm
rssi-remote-v                    | -48 dBm
snr-remote-h                     | 37 dB
snr-remote-v                     | 37 dB
link-quality-remote              | 100%
memory-usage-remote              | 61%
cpu-usage-remote                 | 0.0%
noise-remote-h                   | -92 dBm
noise-remote-v                   | -92 dBm
tx-rate                          | HE NSS2 MCS9 LGI 195 Mbps
rx-rate                          | HE NSS2 MCS5 LGI 117 Mbps
tx-bw                            | 20M
rx-bw                            | 20M
uptime                           | 00:10:04
wireless-mode                    | ax
link-quality                     | 100%
link-quality-common              | 100%
actual-rx-pps                    | 0 pps
actual-tx-pps                    | 0 pps
actual-tx-rate                   | 0 Kbps
actual-rx-rate                   | 0 Kbps
link-capacity                    | 83 Mbps
```

Displaying brief information about wireless clients (STA) in horizontal view from the access point side (AP):

WB-3P-PTP6(root):/# **monitoring clients brief**

```
Hostname         IP                RSSI, dBm  r-RSSI, dBm RX rate, Mbps           Uptime
                 MAC               SNR, dB    r-SNR, dB   TX rate, Mbps
---------------- ----------------- ---------- ----------- ----------------------  ---------
WB-3P-PTP6-STA   192.168.1.15      -43/-54    -46/-48     HE NSS2 MCS7 LGI 146.3  00:02:42
                 ec:b1:e0:2d:a1:00 19/19      37/37       HE NSS2 MCS9 LGI 195
---------------- ----------------- ---------- ----------- ----------------------  ---------
```

Displaying brief information about a wireless client (STA) in horizontal view from the access point side (AP):

WB-3P-PTP6(root):/# **monitoring clients station ec:b1:e0:2d:a1:00 brief**

```
Hostname         IP                RSSI, dBm  r-RSSI, dBm RX rate, Mbps           Uptime
                 MAC               SNR, dB    r-SNR, dB   TX rate, Mbps
---------------- ----------------- ---------- ----------- ----------------------  --------
WB-3P-PTP6-STA   192.168.1.15      -43/-54    -46/-48     HE NSS2 MCS7 LGI 146.3  00:02:42
                 ec:b1:e0:2d:a1:00 19/19      37/37       HE NSS2 MCS9 LGI 195
---------------- ----------------- ---------- ----------- ----------------------  --------
```

Displaying full information about wireless clients (STA) from the access point side (AP):

WB-3P-PTP6(root):/# **monitoring clients detailed**

```
 index                          | 0
hw-addr                         | ec:b1:e0:2d:a1:00
interface                       | wlan0
rfid                            | -1
wid                             | -1
band                            | 6 GHz
distance                        | 1 km
frequency                       | 5955 MHz
serial-number                   | WP44000027
eltex-board-type                | WB-3P-PTP6
eltex-firmware-version          | 2.6.1 build X
factory-mac                     | EC:B1:E0:2D:A1:00
state                           | ASSOC AUTH_SUCCESS
fbwa-mode                       | pmp-sta
ssid                            | WB-3P-PTP6-AP
vlan-id                         | 100
ip-addr                         | 192.168.1.15
channel                         | 1
hostname                        | WB-3P-PTP6-STA
dhcp-request-status             | obtained
eap-method                      | 0
rx-retry-count                  | 4
tx-fails                        | 0
tx-period-retry                 | 0
tx-retry-count                  | 49
rssi-h                          | -42 dBm
rssi-v                          | -54 dBm
rssi                            | -54 dBm
max-rssi-h                      | -42 dBm
max-rssi-v                      | -51 dBm
max-rssi                        | -42 dBm
snr-h                           | 23 dB
snr-v                           | 23 dB
snr                             | 23 dB
noise-h                         | -65 dBm
noise-v                         | -77 dBm
noise                           | -65 dBm
rssi-remote-h                   | -46 dBm
rssi-remote-v                   | -48 dBm
rssi-remote                     | -48 dBm
snr-remote-h                    | 37 dB
snr-remote-v                    | 37 dB
snr-remote                      | 37 dB
link-quality-remote             | 100%
memory-usage-remote             | 61%
cpu-usage-remote                | 0.0%
tx-retry-ratio-remote           | 0%
rx-retry-ratio-remote           | 14%
utilization-remote              | 3
rx-utilization-remote           | 2
tx-utilization-remote           | 0
tx-power-remote                 | 8 dBm
```

```
 system-uptime-remote               | 222:22:47
 link-capacity-remote               | 66 Mbps
 noise-remote-h                     | -93 dBm
 noise-remote-v                     | -93 dBm
 noise-remote                       | -93 dBm
 co-channel-interference-remote     | 0
 ap-interference-ratio-remote       | 3
 non-wifi-interference-remote       | 1
 packet-error-rate-remote           | 0
 tx-rate                            | HE NSS2 MCS11 LGI 243.8 Mbps
 tx-rate-numeric                    | 243.8
 rx-rate                            | HE NSS2 MCS7 LGI 146.3 Mbps
 rx-rate-numeric                    | 146.3
 rx-bw-all                          | 20M
 tx-bw                              | 20M
 rx-bw                              | 20M
 uptime                             | 00:03:56
 mfp                                | false
 wireless-mode                      | ax
 perftest-capable                   | true
 snr-rssi-capable                   | true
 link-quality                       | 91%
 link-quality-common                | 92%
 tx-retry-ratio                     | 0%
 rx-retry-ratio                     | 0%
 actual-tx-rate                     | 0 Kbps
 actual-rx-rate                     | 0 Kbps
 shaped-rx-rate                     | 0 Kbps
 actual-tx-pps                      | 1 pps
 actual-rx-pps                      | 0 pps
 shaped-rx-pps                      | 0 pps
 link-capacity                      | 91 Mbps
 multicast-groups-count             | 1
 using-802.11r                      | no
 using-802.11k                      | no
 using-802.11v                      | yes
 twt-support                        | none
 name                               | 0

Counter                 Transmitted               Received
----------------------  ------------------------  --------------------------
Total Packets:          627                       92
TX success:             100%                      0
Total Bytes:            51589                     5653
Data Packets:           541                       12
Data Bytes:             46962                     1616
Mgmt Packets:           86                        80
Mgmt Bytes:             4627                      4037
Dropped Packets:        0                         0
Dropped Bytes:          0                         0
Lost Packets:           0                         0

Rate             Transmitted                Received
---------------  ------------------------   -------------------------
mcs0             0              |   0%     4              |  33%
he-nss2-mcs3     0              |   0%     1              |   8%
he-nss2-mcs5     0              |   0%     1              |   8%
he-nss2-mcs7     4              |   0%     4              |  33%
```

```
he-nss2-mcs8      9              |   1%     2              |  16%
he-nss2-mcs9      127            |  23%     0              |   0%
he-nss2-mcs10     377            |  69%     0              |   0%
he-nss2-mcs11     24             |   4%     0              |   0%
-------------------------------------------------------------------------
   | Multicast groups                    | Clients                      |
-------------------------------------------------------------------------
   | MAC               | IP              | Count  | IP                  |
-------------------------------------------------------------------------
  0| 01:00:5e:00:00:6a |     xxx.0.0.106 |       1|   192.168.1.100(  0) |
-------------------------------------------------------------------------
```

Displaying full information about a wireless client (STA) from the access point side (AP):

WB-3P-PTP6(root):/# **monitoring clients station ec:b1:e0:2d:a1:00 detailed**

```
index                          | 0
hw-addr                        | ec:b1:e0:2d:a1:00
interface                      | wlan0
rfid                           | -1
wid                            | -1
band                           | 6 GHz
distance                       | 1 km
frequency                      | 5955 MHz
serial-number                  | WP44000027
eltex-board-type               | WB-3P-PTP6
eltex-firmware-version         | 2.6.1 build X
factory-mac                    | EC:B1:E0:2D:A1:00
state                          | ASSOC AUTH_SUCCESS
fbwa-mode                      | pmp-sta
ssid                           | WB-3P-PTP6-AP
vlan-id                        | 100
ip-addr                        | 192.168.1.15
channel                        | 1
hostname                       | WB-3P-PTP6-STA
dhcp-request-status            | obtained
eap-method                     | 0
rx-retry-count                 | 4
tx-fails                       | 0
tx-period-retry                | 0
tx-retry-count                 | 49
rssi-h                         | -42 dBm
rssi-v                         | -54 dBm
rssi                           | -54 dBm
max-rssi-h                     | -42 dBm
max-rssi-v                     | -51 dBm
max-rssi                       | -42 dBm
snr-h                          | 23 dB
snr-v                          | 23 dB
snr                            | 23 dB
noise-h                        | -65 dBm
noise-v                        | -77 dBm
noise                          | -65 dBm
rssi-remote-h                  | -46 dBm
rssi-remote-v                  | -48 dBm
rssi-remote                    | -48 dBm
snr-remote-h                   | 37 dB
snr-remote-v                   | 37 dB
snr-remote                     | 37 dB
link-quality-remote            | 100%
memory-usage-remote            | 61%
cpu-usage-remote               | 0.0%
tx-retry-ratio-remote          | 0%
rx-retry-ratio-remote          | 14%
utilization-remote             | 3
rx-utilization-remote          | 2
tx-utilization-remote          | 0
tx-power-remote                | 8 dBm
```

```
 system-uptime-remote               | 222:22:47
 link-capacity-remote               | 66 Mbps
 noise-remote-h                     | -93 dBm
 noise-remote-v                     | -93 dBm
 noise-remote                       | -93 dBm
 co-channel-interference-remote     | 0
 ap-interference-ratio-remote       | 3
 non-wifi-interference-remote       | 1
 packet-error-rate-remote           | 0
 tx-rate                            | HE NSS2 MCS11 LGI 243.8 Mbps
 tx-rate-numeric                    | 243.8
 rx-rate                            | HE NSS2 MCS7 LGI 146.3 Mbps
 rx-rate-numeric                    | 146.3
 rx-bw-all                          | 20M
 tx-bw                              | 20M
 rx-bw                              | 20M
 uptime                             | 00:03:56
 mfp                                | false
 wireless-mode                      | ax
 perftest-capable                   | true
 snr-rssi-capable                   | true
 link-quality                       | 91%
 link-quality-common                | 92%
 tx-retry-ratio                     | 0%
 rx-retry-ratio                     | 0%
 actual-tx-rate                     | 0 Kbps
 actual-rx-rate                     | 0 Kbps
 shaped-rx-rate                     | 0 Kbps
 actual-tx-pps                      | 1 pps
 actual-rx-pps                      | 0 pps
 shaped-rx-pps                      | 0 pps
 link-capacity                      | 91 Mbps
 multicast-groups-count             | 1
 using-802.11r                      | no
 using-802.11k                      | no
 using-802.11v                      | yes
 twt-support                        | none
 name                               | 0

Counter                 Transmitted               Received
----------------------  ------------------------  --------------------------
Total Packets:          627                       92
TX success:             100%                      0
Total Bytes:            51589                     5653
Data Packets:           541                       12
Data Bytes:             46962                     1616
Mgmt Packets:           86                        80
Mgmt Bytes:             4627                      4037
Dropped Packets:        0                         0
Dropped Bytes:          0                         0
Lost Packets:           0                         0

Rate             Transmitted                Received
---------------  ------------------------   -------------------------
mcs0             0              |   0%     4              |  33%
he-nss2-mcs3     0              |   0%     1              |   8%
he-nss2-mcs5     0              |   0%     1              |   8%
he-nss2-mcs7     4              |   0%     4              |  33%
```

```
he-nss2-mcs8      9              |   1%     2              |  16%
he-nss2-mcs9      127            |  23%     0              |   0%
he-nss2-mcs10     377            |  69%     0              |   0%
he-nss2-mcs11     24             |   4%     0              |   0%
-------------------------------------------------------------------------
   | Multicast groups                    | Clients                      |
-------------------------------------------------------------------------
   | MAC               | IP              | Count  | IP                  |
-------------------------------------------------------------------------
  0| 01:00:5e:00:00:6a |     xxx.0.0.106 |       1|   192.168.1.100(  0) |
-------------------------------------------------------------------------
```

12.11.1.3 Device mode sta

Displaying information about the wireless peer status from the client (STA):

WB-3P-PTP6(root):/# **monitoring wireless-peer**

```
index                          | 0
hw-addr                        | ec:b1:e0:2d:a1:f0
interface                      | wlan0
band                           | 6 GHz
state                          | ASSOC STATION
frequency                      | 5955 MHz
distance                       | 1 km
fbwa-mode                      | ptp-ap
serial-number                  | WP44000027
eltex-board-type               | WB-3P-PTP6
eltex-firmware-version         | 2.6.1 build X
factory-mac                    | EC:B1:E0:2D:A1:F0
ssid                           | WB-3P-PTP6-AP
ip-addr                        | 192.168.1.20
hostname                       | WB-3P-PTP6-AP
rssi-h                         | -46 dBm
rssi-v                         | -48 dBm
snr-h                          | 37 dB
snr-v                          | 37 dB
noise-h                        | -83 dBm
noise-v                        | -85 dBm
rssi-remote-h                  | -42 dBm
rssi-remote-v                  | -54 dBm
snr-remote-h                   | 23 dB
snr-remote-v                   | 23 dB
link-quality-remote            | 95%
memory-usage-remote            | 63%
cpu-usage-remote               | 0.0%
noise-remote-h                 | -80 dBm
noise-remote-v                 | -80 dBm
tx-rate                        | HE NSS2 MCS8 LGI 175.5 Mbps
rx-rate                        | HE NSS2 MCS10 LGI 219.4 Mbps
tx-bw                          | 20M
rx-bw                          | 20M
uptime                         | 00:04:40
wireless-mode                  | ax
link-quality                   | 90%
link-quality-common            | 97%
actual-rx-pps                  | 3 pps
actual-tx-pps                  | 1 pps
actual-tx-rate                 | 1 Kbps
actual-rx-rate                 | 3 Kbps
link-capacity                  | 71 Mbps
```

Displaying brief information about the wireless peer status in horizontal view from the client (STA):

WB-3P-PTP6(root):/# **monitoring wireless-peer brief**

```
Hostname         IP                RSSI, dBm  r-RSSI, dBm RX rate, Mbps           Uptime
                 MAC               SNR, dB    r-SNR, dB   TX rate, Mbps
---------------- ----------------- ---------- ----------- ----------------------  --------
WB-3P-PTP6-AP    192.168.1.20     -46/-49    -42/-53     HE NSS2 MCS9 LGI 195    00:06:40
                 ec:b1:e0:2d:a1:f0 38/38      20/20       HE NSS2 MCS8 LGI 175.5
---------------- ----------------- ---------- ----------- ----------------------  --------
```

Displaying full information about the wireless peer status from the client (STA):

WB-3P-PTP6(root):/# **monitoring wireless-peer detailed**

```
index                          | 0
hw-addr                        | ec:b1:e0:2d:a1:f0
interface                      | wlan0
rfid                           | -1
wid                            | -1
band                           | 6 GHz
distance                       | 1 km
frequency                      | 5955 MHz
state                          | ASSOC STATION
fbwa-mode                      | ptp-ap
serial-number                  | WP44000027
eltex-board-type               | WB-3P-PTP6
eltex-firmware-version         | 2.6.1 build X
factory-mac                    | EC:B1:E0:2D:A1:F0
ssid                           | WB-3P-PTP6-AP
vlan-id                        | 100
ip-addr                        | 192.168.1.20
channel                        | 1
hostname                       | WB-3P-PTP6-AP
rx-retry-count                 | 104
tx-fails                       | 0
tx-period-retry                | 0
tx-retry-count                 | 11
rssi-h                         | -46 dBm
rssi-v                         | -48 dBm
rssi                           | -48 dBm
max-rssi-h                     | -45 dBm
max-rssi-v                     | -45 dBm
max-rssi                       | -45 dBm
snr-h                          | 38 dB
snr-v                          | 38 dB
snr                            | 38 dB
noise-h                        | -84 dBm
noise-v                        | -86 dBm
noise                          | -84 dBm
rssi-remote-h                  | -42 dBm
rssi-remote-v                  | -53 dBm
rssi-remote                    | -53 dBm
snr-remote-h                   | 19 dB
snr-remote-v                   | 19 dB
snr-remote                     | 19 dB
link-quality-remote            | 100%
memory-usage-remote            | 62%
cpu-usage-remote               | 0.0%
tx-retry-ratio-remote          | 0%
rx-retry-ratio-remote          | 0%
utilization-remote             | 59
rx-utilization-remote          | 18
tx-utilization-remote          | 0
tx-power-remote                | 8 dBm
system-uptime-remote           | 222:33:05
link-capacity-remote           | 84 Mbps
```

```
 noise-remote-h                    | -84 dBm
 noise-remote-v                    | -84 dBm
 noise-remote                      | -84 dBm
 co-channel-interference-remote    | 20
 ap-interference-ratio-remote      | 55
 non-wifi-interference-remote      | 21
 packet-error-rate-remote          | 3
 tx-rate                           | HE NSS2 MCS6 LGI 131.6 Mbps
 tx-rate-numeric                   | 131.6
 rx-rate                           | HE NSS2 MCS9 LGI 195 Mbps
 rx-rate-numeric                   | 195
 rx-bw-all                         | 20M
 tx-bw                             | 20M
 rx-bw                             | 20M
 uptime                            | 00:08:02
 mfp                               | false
 wireless-mode                     | ax
 perftest-capable                  | true
 snr-rssi-capable                  | true
 link-quality                      | 100%
 link-quality-common               | 96%
 tx-retry-ratio                    | 0%
 rx-retry-ratio                    | 0%
 actual-tx-rate                    | 1 Kbps
 actual-rx-rate                    | 5 Kbps
 shaped-rx-rate                    | 6 Kbps
 actual-tx-pps                     | 1 pps
 actual-rx-pps                     | 6 pps
 shaped-rx-pps                     | 7 pps
 link-capacity                     | 71 Mbps
 multicast-groups-count            | 1
 using-802.11r                     | no
 using-802.11k                     | no
 using-802.11v                     | no
 twt-support                       | none
 name                              | 0

Counter                 Transmitted              Received
----------------------  -----------------------  -------------------------
Total Packets:          287                      5808
TX success:             100%                     0
Total Bytes:            21029                    640457
Data Packets:           80                       1279
Data Bytes:             11228                    205290
Mgmt Packets:           207                      4529
Mgmt Bytes:             9801                     435167
Dropped Packets:        0                        0
Dropped Bytes:          0                        0
Lost Packets:           0                        0

Rate             Transmitted               Received
---------------  -----------------------   -------------------------
mcs0             0              |   0%     631            |  49%
he-nss2-mcs6     6              |   7%     3              |   0%
he-nss2-mcs7     21             |  26%     12             |   0%
he-nss2-mcs8     33             |  41%     68             |   5%
he-nss2-mcs9     20             |  25%     314            |  24%
he-nss2-mcs10    0              |   0%     246            |  19%
```

```
he-nss2-mcs11     0              |   0%     5              |   0%
-------------------------------------------------------------------------------
   | Multicast groups                    | Clients                       |
-------------------------------------------------------------------------------
   | MAC               | IP              | Count  | IP                   |
-------------------------------------------------------------------------------
  0| 01:00:5e:00:00:6a |     xxx.0.0.106 |       1|   192.168.1.100(  0) |
-------------------------------------------------------------------------------
```

12.11.2 Device information

WB-3P-PTP6(root):/# **monitoring information**

```
system-time                  | 10:11:07 25.04.2025
uptime                       | 03:31:02
hostname                     | WB-3P-PTP6
software-version             | 2.6.1 build X
secondary-software-version   | 2.6.1 build X
boot-version                 | 2.6.1 build X
memory-usage                 | 49
memory-free                  | 120
memory-used                  | 117
memory-total                 | 237
cpu-load                     | 1.2
cpu-average                  | 1.22
is-default-config            | false
vendor                       | Eltex
device-type                  | Wireless Bridge
board-type                   | WB-3P-PTP6
hw-platform                  | WB-3P-PTP6
factory-wan-mac              | EC:B1:E0:xx:xx:xx
factory-lan-mac              | EC:B1:E0:xx:xx:xx
factory-serial-number        | WP5C000030
hw-revision                  | 1v0
session-password-initialized | false
ott-mode                     | false
last-reboot-reason           | firmware update
test-changes-mode            | false
```

12.11.3 Network information

WB-3P-PTP6(root):/# **monitoring wan-status**

```
Common information:

 interface               | br0.100
 mac                     | ec:b1:e0:xx:xx:xx
 vlan                    | 1000
 rx-bytes                | 38604853
 rx-packets              | 519072
 tx-bytes                | 17376843
 tx-packets              | 101871

IPv4 information:

 protocol                | dhcp
 ip-address              | 192.168.1.15
 netmask                 | 255.255.255.0
 gateway                 | 192.168.1.1
 DNS-1                   | 192.168.1.100
 DNS-2                   | 8.8.8.8
```

WB-3P-PTP6(root):/# **monitoring ethernet**

```
 link: up
 speed: 1000M
 duplex: enabled
 media-type: copper
 rx-bytes: 665533857
 rx-packets: 4341734
 tx-bytes: 105542200
 tx-packets: 230002
```

WB-3P-PTP6(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
```

WB-3P-PTP6(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
```

WB-3P-PTP6(root):/# **monitoring lldp**

```
System capability legend:
        B - Bridge; R - Router; W - Wlan Access Point; T - Telephone;
        D - DOCSIS Cable Device; H - Host; r - Repeater; O - Other;

Port         Device ID           Port ID             System Name     Capabilities   TTL
---------    -----------------   -----------------   -------------   ------------   ---
eth0         50:eb:e3:xx:xx:xx   gi 0/10             PC-16487        B,W,R,H        120
```

12.11.4 Wireless interfaces

WB-3P-PTP6(root):/# **monitoring radio-interface**

```
    name                      | wlan0
    rfid                      | 0
    status                    | on
    band                      | 6 GHz
    hwaddr                    | EC:B1:E0:xx:xx:xx
    tx-power                  | 26 dBm
    auto-tx-power             | off
    antenna-gain              | 9 dBi
    eirp                      | 35 dBm
    connection-status         | AP mode
    operation-mode            | ap-pmp
    noise-h                   | -93 dBm
    noise-v                   | -93 dBm
    noise threshold (dBm)     | -92 -89 -86 -83 -80 -75 -70 -65 -60 -55  -1
    noise ratio (%)           |  96   2   0   1   1   0   0   0   0   0   0
    utilization               | 7%
    rx-utilization            | 7%
    tx-utilization            | 0%
    co-channel-interference   | 0%
    ap-interference-ratio     | 2%
    non-wifi-interference     | 0%
    packet-error-rate         | 0%
    channel                   | 1
    frequency                 | 5995 MHz
    bandwidth                 | 20 MHz
    mode                      | ax
    thermal                   | 47 °C
```

12.11.5 Event logs

WB-3P-PTP6(root):/# **monitoring events**

```
Apr 25 10:21:07 WB-3P-PTP6 daemon.info configd[171]: The AP running configuration was
updated successfully by admin
Apr 25 10:21:07 WB-3P-PTP6 daemon.info configd[171]: The AP startup configuration was
updated successfully by admin
Apr 25 10:22:01 WB-3P-PTP6 user.info monitord: start spectrum analyzer on interface 'wlan0'
Apr 25 10:22:57 WB-3P-PTP6 user.info monitord: spectrum analyzer on interface 'wlan0'
 finished
Apr 25 10:23:38 WB-3P-PTP6 daemon.info scanwlan[1320]: start scan on interface 'wlan0'
Apr 25 10:26:36 WB-3P-PTP6 daemon.info scanwlan[1320]: scan on interface 'wlan0' finished
Apr 25 10:28:44 WB-3P-PTP6 daemon.info monitord[596]: event: 'authenticated' ip: 0.0.0.0
 mac: EC:B1:E0:2E:68:50 ssid: 'WB-3P-PTP6' interface: wlan0 channel: 1 rssi-1: -43 rssi-2:
-31 location: 'root' auth-method: 'Personal' captive-portal: 'disabled'
Apr 25 10:35:17 WB-3P-PTP6 daemon.info monitord[596]: event: 'deauthenticated by AP' ip:
192.168.1.20 mac: EC:B1:E0:2E:68:50 ssid: 'WB-3P-PTP6' interface: wlan0 channel: 1 rssi-1:
-22 rssi-2: -19 location: 'root' reason: 4 description: 'Inactivity'
```

12.11.6 Environment scan

While scanning the environment, the device radio interface will be disabled, which will make it impossible to transfer data to client devices during scanning.

WB-3P-PTP6(root):/# **monitoring scan-wifi**

SSID	Mode	Security	BSSID	Channel	RSSI, dBm	Bandwidth, MHz
[redacted]	PTP	wpa3	EC:B1:E0:27:AC:C0	5	-65	20
[redacted]	AP	wpa3	00:11:22:33:44:75	37	-65	160
[redacted]	PTP	wpa3	EC:B1:E0:27:AC:50	1	-85	20

12.11.7 Spectrum analyzer

The spectrum analyzer provides information on channel congestion. The analysis time for all radio channels in the range is approximately 1 minute.

While the spectrum analyzer is running, client devices disconnect. The client devices will only reconnect when the spectrum analyzer has finished its work.

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

WB-3P-PTP6(root):/# **monitoring spectrum-analyzer**

```
Channel| CCA
  1| 0%
  5| 0%
  9| 0%
 13| 0%
 17| 0%
 21| 0%
 25| 0%
 29| 0%
 33| 0%
 37| 1%
 41| 0%
 45| 0%
 49| 0%
 53| 0%
 57| 0%
 61| 0%
 65| 0%
 69| 0%
 73| 0%
 77| 0%
 81| 0%
 85| 0%
 89| 0%
 93| 0%
```

12.11.8 Obtaining troubleshooting information

Command for collecting debug information
WB-3P-PTP6(root):/# **get-troubleshooting-file**

After executing the command, the *troubleshooting.tar.gz* archive will be created, containing troubleshooting data and device status information.

Get the *troubleshooting.tar.gz* archive from the device to a server or PC using the TFTP protocol:

This protocol is unavailable to created users; available only to admin.

WB-3P-PTP6(root):/# **tftp upload <IP Address TFTP-of the server>troubleshooting.tar.gz**

Get the *troubleshooting.tar.gz* archive from the device to a server or PC using the SCP protocol:

This protocol is unavailable to created users; available only to admin.

scp <User>@<IP-device address>:troubleshooting.tar.gztroubleshooting.tar.gz (example: scp admin@192.168.1.15:troubleshooting.tar.gztroubleshooting.tar.gz. This command is executed on the server/PC)

13 Auxiliary utilities

13.1 Perftest utility

The perftest utility performs a built-in radio link speed test.

Configuring perftest

WB-3P-PTP6(root):/# **configure**
WB-3P-PTP6(config):/# **perftest**
WB-3P-PTP6(config):/perftest# **server-ip X.X.X.X** (where X.X.X.X — IP Address, which will be assigned to the remote device interface for the duration of the test. By default: 192.0.4.1. It is recommended to configure a subnet not used on the active network)
WB-3P-PTP6(config):/perftest# **client-ip X.X.X.X** (where X.X.X.X — IP Address, which will be assigned to the device interface where the utility is run, for the duration of the test. By default: 192.0.4.2. It is recommended to configure a subnet not used on the active network)
WB-3P-PTP6(config):/perftest# **netmask X.X.X.X** (where X.X.X.X — subnet mask, which is used for the test. By default: 255.255.255.0)
WB-3P-PTP6(config):/perftest# **vlan-id X** (where X — VLAN ID, used for the test. By default: 7. It is recommended to configure VLAN ID, which is not used on the active network)
WB-3P-PTP6(config):/perftest# **save** (saving settings)

The perftest utility can be run with the following commands:

Commands to start perftest

Perf-test station <MAC remote device> downlink — initiates speed testing to the remote device (Downlink)
perf-test station <MAC remote device > uplink — initiates speed testing from the remote device (Uplink)
perf-test station <MAC remote device> bidirectional — device (Downlink + Uplink)

13.2 Manage-remote utility

The manage-remote utility allows running commands from access point (AP) on client (STA).

These commands can be executed when there is no access to the client (STA) via IP address.

13.2.1 Rebooting

For device mode **ap-ptp**:

Command for rebooting a remote device

WB-3P-PTP6(root):/# **manage-remote reboot**

For device mode **ap-pmp**:

Command for rebooting a remote device
WB-3P-PTP6(root):/# **manage-remote reboot station XX:XX:XX:XX:XX:XX** (where XX:XX:XX:XX:XX:XX — MAC address of the device to be rebooted)

13.2.2 Scan environment

For device mode **ap-ptp**:

Command for air scanning from a remote device
WB-3P-PTP6(root):/# **manage-remote scan-wifi**

For device mode **ap-pmp**:

Command for air scanning from a remote device
WB-3P-PTP6(root):/# **manage-remote scan-wifi station XX:XX:XX:XX:XX:XX** (where XX:XX:XX:XX:XX:XX — MAC address of the device on which air scanning will be performed)

13.2.3 Spectrum Analyzer

For device mode **ap-ptp**:

Command to run on a remote device
WB-3P-PTP6(root):/# **manage-remote spectrum-analyzer**

For device mode **ap-pmp**:

Command to run on a remote device
WB-3P-PTP6(root):/# **manage-remote spectrum-analyzer station XX:XX:XX:XX:XX:XX** (where XX:XX:XX:XX:XX:XX — MAC address of the device on which spectrum analysis will be performed)

13.2.4 Obtaining troubleshooting information

For device mode **ap-ptp**:

Commands to run for a remote device
WB-3P-PTP6(root):/# **manage-remote upload-troubleshooting** WB-3P-PTP6(root):/# **manage-remote upload-troubleshooting-checksum**

For device mode **ap-pmp**:

Commands to run on a remote device

WB-3P-PTP6(root):/# **manage-remote upload-troubleshooting station XX:XX:XX:XX:XX:XX** (where XX:XX:XX:XX:XX:XX — MAC address of the device from which troubleshooting information will be obtained)
WB-3P-PTP6(root):/# **manage-remote upload-troubleshooting-checksum station XX:XX:XX:XX:XX:XX** (where XX:XX:XX:XX:XX:XX — MAC address of the device from which troubleshooting information will be obtained)

The **upload-troubleshooting-checksum** command verifies the integrity of the received data. It is used for more reliable data transfer but may require more time.

A specified channel on which the spectrum scan will be performed */tmp/troubleshooting/* with received data, *troubleshooting_remote.tar.gz* and *troubleshooting_remote_checksum.tar.gz* respectively.
After the commands are executed, archives containing the collected data — *troubleshooting_remote.tar.gz* and *troubleshooting_remote_checksum.tar.gz*, respectively — will be created in the */tmp/troubleshooting/* directory.

Uploading files from the device:

These commands are unavailable to created users; available only to admin.

Upload archive from device to TFTP server

WB-3P-PTP6(root):/# **tftp upload <IP address of TFTP server> /tmp/troubleshooting/ troubleshooting_remote.tar.gz**
WB-3P-PTP6(root):/#**tftp upload <IP address of TFTP server> /tmp/troubleshooting/ troubleshooting_remote_checksum.tar.gz**

Upload archive from device to server/PC via SCP

Scp <User>@<IP-device address>: /tmp/troubleshooting/ troubleshooting_remote.tar.gztroubleshooting_remote.tar.gz (example: scp admin@192.168.1.15: */tmp/troubleshooting/*troubleshooting_remote.tar.gztroubleshooting_remote.tar.gz. This command is executed on the server/PC)
scp <User>@<IP-device address>: /tmp/troubleshooting/ troubleshooting_remote_checksum.tar.gztroubleshooting_remote_checksum.tar.gz (example: scp admin@192.168.1.15: */tmp/troubleshooting/* troubleshooting_remote_checksum.tar.gztroubleshooting_remote_checksum.tar.gz. This command is executed on the server/PC)

13.3 Traceroute utility

The utility shows the nodes (routers) a packet passes through and the time it takes to process the packet at each node.

This utility is unavailable to created users; available only to admin.

Command to start tracing

WB-3P-PTP6(root):/# **traceroute <test host>**

13.4 Tcpdump utility

The tcpdump utility allows capturing packets on a specified interface.

This utility is unavailable to created users; available only to admin.

13.4.1 Traffic capture from the active interface

Capturing Ethernet interface packets.

WB-3P-PTP6(root):/# **tcpdump interface eth0**

Capturing Ethernet interface packets and saving them to a file.

WB-3P-PTP6(root):/# **tcpdump interface eth0 file <filename>**

13.4.2 Air Sniffer

It is necessary to enable a special interface on the device's operating channel that captures packets from the air.

Commands

WB-3P-PTP6(root):/# **configure**
WB-3P-PTP6(config):/# **interface**
WB-3P-PTP6(config):/interface# **radio0**
WB-3P-PTP6(config):/interface/radioX# **common**
WB-3P-PTP6(config):/interface/radioX/common# **enabled true**

Capturing air packets on radio0-interface.

WB-3P-PTP6(root):/# **tcpdump interface radio0**

Capturing air packets on radio0-interface with saving to file.

WB-3P-PTP6(root):/# **tcpdump interface radio0 file <filename>**

13.4.3 Uploading the file from device to server

This command is executed on the server/PC.

scp <User>@<IP-device address>:tcpdump.pcap tcpdump.pcap (example: scp admin@192.168.1.15:tcpdump.pcap tcpdump.pcap)

13.5 Iperf/iperf3 utility

This utility is used to initiate a traffic stream from one device to another. The sending side is referred to as the client, and the receiving side as the server.

13.5.1 iperf

Example of initiating a traffic stream from device to server:

Configuring the server to receive traffic

WB-3P-PTP6(root):/# **iperf server**

Initiating traffic from the device towards the server

WB-3P-PTP6(root):/# **iperf client X.X.X.X** (where X.X.X.X — IP Address of the server)

13.5.2 iperf3

Example of launching a traffic stream from device to server:

Configuring the server to receive traffic

WB-3P-PTP6(root):/# **iperf3 server**

Initiating traffic from device towards server

WB-3P-PTP6(root):/# **iperf3 client X.X.X.X** (where X.X.X.X — IP Address of the server)

13.6 Antenna Align

Alignment refers to adjusting the device antenna position in space to obtain the maximum signal.

WB-3P-PTP6(root):/# **antenna-align**

```
ssid                    | WB-3P-PTP6
channel                 | 1
frequency               | 5955
estimated-rssi          | -48 dBm
rssi-h                  | -47
rssi-v                  | -48
rssi-remote-h           | -47
rssi-remote-v           | -48
```

14 List of changes

Document Version	Release Date	List of changes
Version 1.6	08.2026	Synchronization with firmware version 2.6.1
Version 1.5	06.2026	Synchronization with firmware version 2.6.0 Added: 10.12.9 "Troubleshooting" submenu 12.11.8 Obtaining troubleshooting information Modified: 10.7.7 "Radio Information" submenu 10.8.1 "Radio" submenu 10.9 "AP" menu 10.10 "STA" menu 10.12.7.2 NTP Server 10.13.1 "Antenna Align" submenu 10.13.2 "Speed Testing" submenu 12.3.1 Advanced Radio settings 12.5.2 Advanced settings for access point (AP) 12.5.4 Advanced settings for client (STA) 12.10.7 Configuring date and time 12.11 Monitoring 13.2.4 Obtaining troubleshooting information 13.5 Iperf/iperf3 utility 13.6 Antenna Align
Version 1.4	03.2026	Synchronization with firmware version 2.5.1 Added: 13.2.4 Obtaining troubleshooting information Modified: 10.6 "Quick Start" menu 10.7.7 "Radio Information" submenu 10.8 "Radio" menu 10.9 "AP" menu 10.10 "STA" menu 10.12.5 "Authentication" submenu 12.2.2 Configuring 802.1p priority for Management VLAN 12.3.1 Advanced Radio settings 12.10.5 Configuring authentication mode 12.11 Monitoring

Document Version	Release Date	List of changes
Version 1.3	12.2025	Synchronization with firmware version 2.4.4 Modified: 12.5.2 Advanced settings for access point (AP) 12.5.4 Advanced settings for client (STA)
Version 1.2	10.2025	Synchronization with firmware version 2.4.1 Added: 10.4 Test mode 10.12.3 "Ping Watchdog" submenu 10.12.5 "Authentication" submenu 12.10.3 Ping watchdog 12.10.5 Configuring authentication mode 13.4.1 Traffic capture from the active interface 13.4.3 Uploading the file from the device to the server Modified: 12.3.1 Advanced Radio settings
Version 1.1	07.2025	Synchronization with firmware version 2.3.1 Added: 10.11.7 "LEDs" submenu 10.12.2 "Speed Testing" submenu 12.7 BPDU filter configuration 12.8 MAC address learning limiting Modified: 10.6.1 "Wireless Peer/Wireless Clients" submenu 10.6.3 "Scan Environment" submenu 10.8.1 "Access Point" submenu 10.9.1 "Station / Client" submenu 12.2.3 Remote management configuration 12.3 Radio Settings 12.3.1 Advanced Radio settings 12.5 Configuring the wireless network 12.5.2 Advanced settings for AP 12.5.3 Network settings for STA 12.5.4 Advanced settings for STA 12.10.4 Device reboot 12.10.5 Configuring authentication mode 12.10.8 Advanced system settings
Version 1.0	05.2025	First issue
Software version 2.6.1		

TECHNICAL SUPPORT

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

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

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

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

https://eltex-co.com/download/