

Wireless access point

WEP-550K

User manual

Firmware version 1.3.0

IP address: 192.168.1.10

Username: admin

Password: password

Contents

1	Introduction	6
1.1	Annotation.....	6
1.2	Symbols	6
2	Device description	7
2.1	Purpose.....	7
2.2	Device specification	7
2.3	Technical parameters	9
2.4	Radiation patterns	11
2.5	Design	12
2.5.1	Main panel	12
2.5.2	Top panel.....	13
2.6	Light indication	14
2.7	Restore the default configuration	14
2.8	Supply package.....	14
3	Rules and recommendations for device installation.....	15
3.1	Safety rules.....	15
3.2	Installation recommendations.....	15
3.3	Calculating the number of required access points	16
3.4	Channel selection for neighboring access points.....	16
4	Device installation	19
4.1	Device installation on a flat surface	19
4.2	Device installation on Armstrong ceiling.....	20
4.3	Device installation on a stud	23
4.4	Device installation on VESA100 bracket	25
5	Device management via the web interface	26
5.1	Getting started	26
5.2	Applying configuration and discarding changes.....	27
5.3	Web interface basic elements	28
5.4	"Monitoring" menu	29
5.4.1	"Wi-Fi Clients" submenu.....	29
5.4.2	"Traffic Statistics" submenu.....	30
5.4.3	"Events" submenu	32
5.4.4	"Network Information" submenu	33
5.4.5	"Radio Information" submenu	35
5.4.6	"Device Information" submenu	36
5.5	"Radio" menu.....	37
5.5.1	"Radio 2.4 GHz" submenu	37
5.5.2	"Radio 5 GHz" submenu	39
5.5.3	"Radio 6 GHz" submenu	41
5.5.4	"Advanced" submenu	43
5.6	"VAP" menu	44

5.6.1	"Summary" submenu	44
5.6.2	"VAP" submenu	45
5.6.3	"MLO" submenu	48
5.7	"Network Settings" menu	50
5.7.1	"System Configuration" submenu	50
5.7.2	"Access" submenu	51
5.8	"External Services" menu	52
5.8.1	"AirTune" submenu	52
5.9	"System" menu	53
5.9.1	"Device Firmware Upgrade" submenu	53
5.9.2	"Configuration" submenu	54
5.9.3	"Reboot" submenu	54
5.9.4	"Password" submenu	55
5.9.5	"Log" submenu	55
5.9.6	"Date and Time" submenu	56
5.9.7	"Troubleshooting" submenu	57
6	Managing the device using the command line.....	58
6.1	Connection to the device	58
6.2	Configuring network parameters	59
6.2.1	Configuring remote management	60
6.3	Configuring Wi-Fi virtual access points (VAP)	61
6.3.1	Configuring VAP without Encryption	62
6.3.2	Configuring VAP with OWE Encryption	63
6.3.3	Configuring VAP with WPA-Personal security mode	64
6.3.4	Configuring VAP with Enterprise authorization	65
6.3.5	Configuring VAP with external Captive Portal	66
6.3.6	Configuring an additional RADIUS server on VAP	69
6.3.7	Advanced VAP settings	69
6.4	Configuring MLO	75
6.4.1	Configuring MLO Group with OWE	75
6.4.2	Configuring MLO Group with WPA-Personal security mode	76
6.4.3	Configuring MLO Group with Enterprise authorization	76
6.5	Configuring AirTune	77
6.6	Radio settings	78
6.6.1	Advanced Radio settings	79
6.7	System settings	80
6.7.1	Device firmware update	80
6.7.2	Device configuration management	80
6.7.3	Device reboot	81
6.7.4	Configuring the authentication mode	81
6.7.5	Setting the date and time	81
6.7.6	Advanced system settings	82

6.8	Configuring Captive Portal parameters	83
6.9	Configuring DAS server	85
6.10	Monitoring	86
6.10.1	Wi-Fi clients	86
6.10.2	Device information.....	87
6.10.3	Network information	88
6.10.4	Wireless interfaces	90
6.10.5	Event logging.....	91
6.10.6	Environment scan	91
6.11	Obtaining troubleshooting information	92
7	Auxiliary utilities	93
7.1	traceroute utility	93
7.2	tcpdump utility.....	93
7.2.1	Capturing traffic from any active interface.....	93
7.3	iperf utility	93
8	The list of changes	94

1 Introduction

1.1 Annotation

Modern tendencies of telecommunication development necessitate operators to search for the most optimal technologies, allowing 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.

The main purpose of WEP-550K is indoor installation as an access point to various resources, creating a seamless wireless network from several identical access points (roaming), if the coverage area is large enough.

This manual specifies intended purpose, main technical parameters, design, safe operation rules, as well as installation and configuration recommendations for WEP-550K.

1.2 Symbols

Notes and warnings

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

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

2 Device description

2.1 Purpose

The WEP-550K wireless access points are designed to provide the user access to a high-speed and secure network.

The main purpose of the devices is to create a Layer 2 wireless data network at the junction with a wired network. WEP-550K connects to a wired network over the 100M/1G/2.5G/5G/10G Ethernet interface and uses radio interfaces to provide wireless high-speed access for devices that support Wi-Fi technology in the 2.4/5/6 GHz bands.

The devices contain 3 radio interfaces for organizing three physical wireless networks.

WEP-550K supports modern quality of service requirements and allows transmitting the most important traffic in higher priority queues compared to regular traffic. Prioritization is provided by the following QoS technologies: CoS (special tags in the VLAN packet field) and ToS (tags in the IP packet field).

The device is a flagship solution for building a wireless network with a large number of users and intensive traffic in offices, government institutions, hotels, conference rooms, laboratories, and classrooms. The ability to create virtual access points with different encryption types allows WEP-550K installation in organizations that require access rights separation between regular users and dedicated user groups.

2.2 Device specification

Interfaces:

- 1 port of 100M/1G/2.5G/5G/10G BASE-T (RJ-45) with PoE support;
- 1 port of 100M/1G/2.5G BASE-T (RJ-45) without PoE support;
- Wi-Fi 2.4 GHz IEEE 802.11b/g/n/ax/be;
- Wi-Fi 5 GHz IEEE 802.11a/n/ac/ax/be;
- Wi-Fi 6 GHz IEEE 802.11ax/be.

Functions:

WLAN capabilities:

- support for IEEE 802.11a/b/g/n/ac/ax/be standards;
- support for IEEE 802.11r/k/v user roaming;
- data aggregation, including A-MPDU and A-MSDU;
- WMM-based priorities and packet planning;
- Dynamic Frequency Selection (DFS);
- support for hidden SSID;
- automatic channel selection;
- 48 virtual access points.

Network functions:

- auto-negotiation of speed, duplex mode and switching between MDI and MDI-X modes;
- VLAN;
- C-VLAN;
- DHCP client;
- GRE;
- transmission of subscriber traffic without tunnels;
- NTP;
- Syslog;
- LLDP.

Security:

- centralized authorization via RADIUS server (802.1X WPA/WPA2/WPA3 Enterprise);
- WPA/WPA2/WPA3/OWE encryption;
- support for external authentication portal.

The WEP-550K equipment use case is shown in Figure 1.

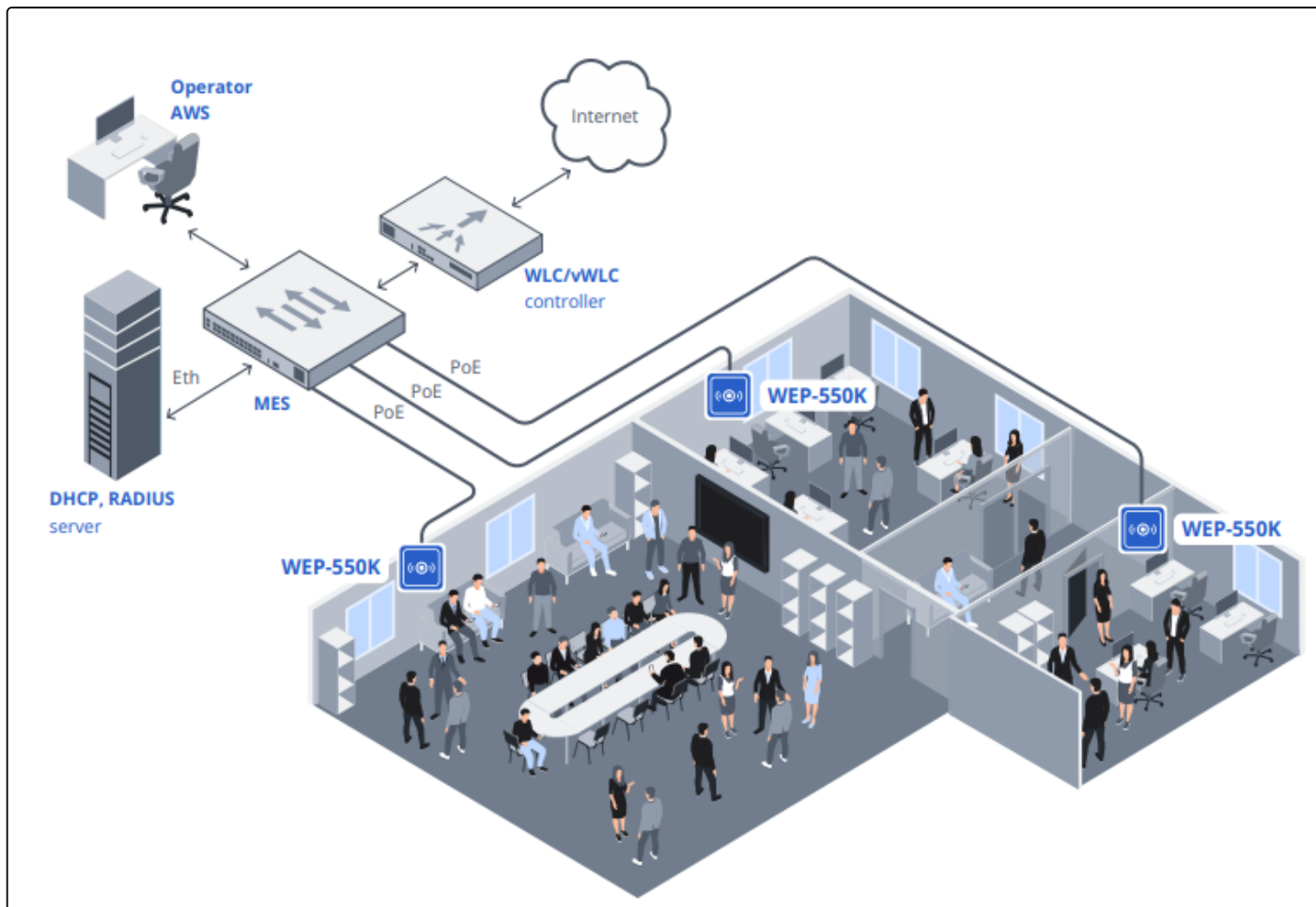


Figure 1 — WEP-550K use case

2.3 Technical parameters

Table 1 – Main specifications

Ethernet interface parameters	
Number of ports	2
Electrical connector	RJ-45
Data rate	100M/1G/2.5G/5G/10G/auto 100M/1G/2.5G/auto
Standards support	BASE-T
Wireless interface parameters	
Standards	802.11a/b/g/n/ac/ax/be
Frequency range	2400–2483.5 MHz; 5150–5350 MHz, 5470–5850 MHz, 5935–7125 MHz
Modulation	BPSK, QPSK, 16QAM, 64QAM, 256QAM, 1024QAM, 4096QAM
Operating channels	802.11b/g/n/ax/be: 1–13 (2401–2483 MHz) 802.11a/n/ac/ax/be: • 36–64 (5170–5330 MHz) • 100–144 (5490–5730 MHz) • 149–165 (5735–5835 MHz) 802.11ax/be: 1–233 (5935–7125 MHz)
Data rate	2.4 GHz, 802.11be: 1376 Mbit/s 5 GHz, 802.11be: 5765 Mbit/s 6 GHz, 802.11be: 11530 Mbit/s
Maximum number of simultaneous connections	1024
Maximum transmitter output power	2.4 GHz: 21 dBm 5 GHz: 21 dBm 6 GHz: 21 dBm
Built-in antenna gain	2.4 GHz: ~4 dBi 5 GHz: ~6 dBi 6 GHz: ~3 dBi
Receiver sensitivity	2.4 GHz: up to -93 dBm 5 GHz: up to -94 dBm 6 GHz: up to -94 dBm
Security	centralized authorization via RADIUS server (802.1X WPA/WPA2/WPA3 Enterprise) WPA/WPA2/WPA3/OWE data encryption support for external authentication portal
Radio interface with OFDMA and MU-MIMO 4×4 support	
Management	
Remote management	web interface, Telnet, SSH, CLI, NETCONF
Access restriction	by password

General parameters	
Flash memory	256 MB SPI-NAND Flash
RAM	1 GB DDR4 RAM
Power supply	PoE++ (IEEE 802.3bt-2018)
Power consumption	no more than 33 W
Operating temperature range	from +5 to +40 °C
Relative humidity at 25 °C	up to 80 %
Dimensions (diameter × height)	280 × 64.5 mm
Weight	1.8 kg
Service life	no less than 15 years

Table 2 – Power supply

Power supply unit	PoE class	Wi-Fi			Ethernet		Maximum power consumption, W
		2.4 GHz	5 GHz	6 GHz	10 GE	2.5 GE	
802.3bt (PoE++)	5	4×4	4×4	4×4	10G	2.5G	33
802.3at (PoE+)	4	2×2	2×2	2×2	2.5G	-	20
Unclassified	-	2×2	2×2	2×2	2.5G	-	20

⊗ Some PoE++ injectors may operate incorrectly; the PoE class must be matched with the powered device.
If an incorrect PoE class is supplied to the device, turn the injector off and on, or power the device from another injector/switch.

Table 3 – Compatibility table of network connection speeds and Ethernet cable categories

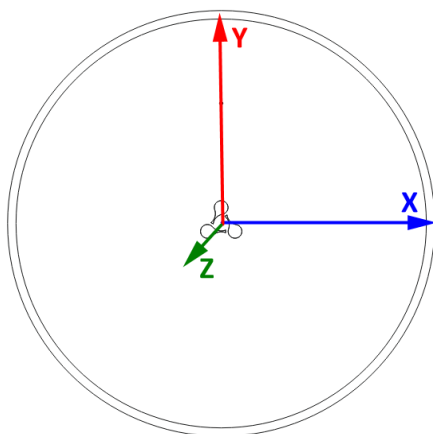
Speed	Cable category
10G	CAT6a (100 m)
	CAT6 (55 m)
	CAT5e (30 m)
5G	CAT6
	CAT5e (30 m)
2.5G	CAT5e
1G	CAT5e
100M	CAT5

2.4 Radiation patterns

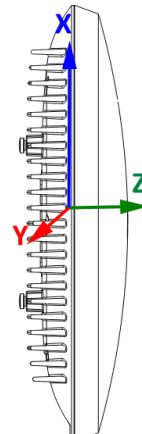
The figures below show the radiation patterns of the device.

Measurement position

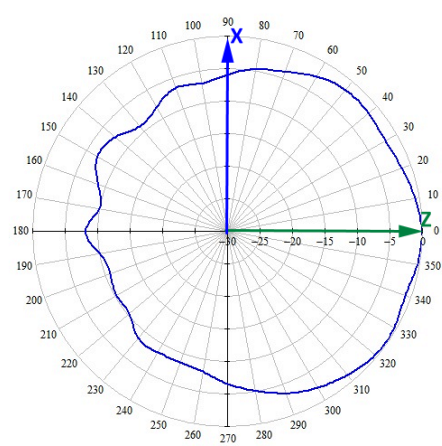
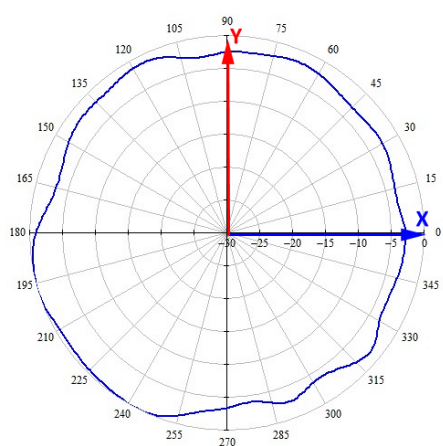
AZIMUTH (XY)



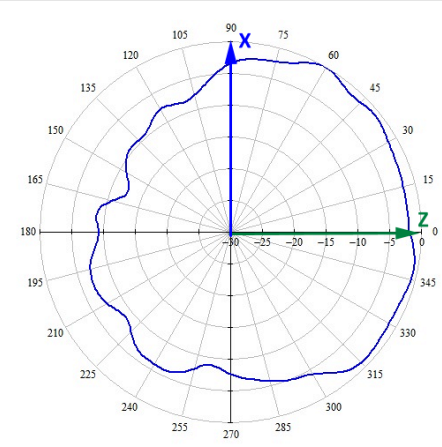
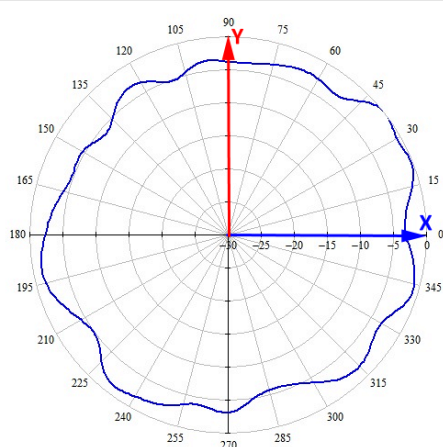
ELEVATION (XZ)



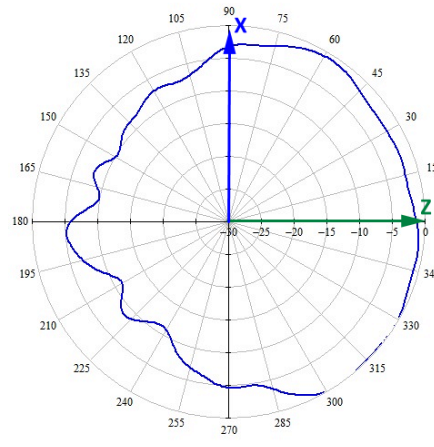
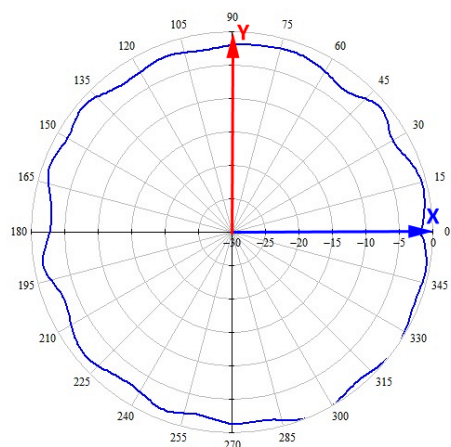
2.4 GHz band



5 GHz band



6 GHz band



2.5 Design

WEP-550K is enclosed in a plastic case.

2.5.1 Main panel

The main panel layout of the device is shown in Figure 2.

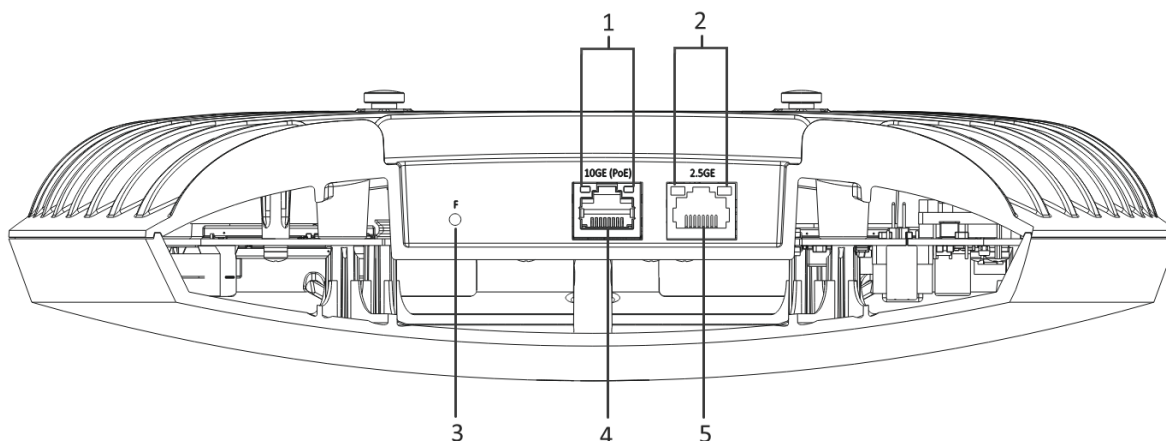


Figure 2 – WEP-550K main panel layout

The following indicator lights, connectors, and controls are placed on the main panel of WEP-550K (see table 4).

Table 4 – Description of indicators, ports and controls

Element		Description
1	LAN_1	10GE (PoE) port status LED
2	LAN_2	2.5GE port status LED
3	F	Factory reset button
4	10GE (PoE)	10GE port for Ethernet cable connection and PoE++
5	2.5GE	2.5GE port for Ethernet cable connection

2.5.2 Top panel

The top panel layout is shown in Figure 3.

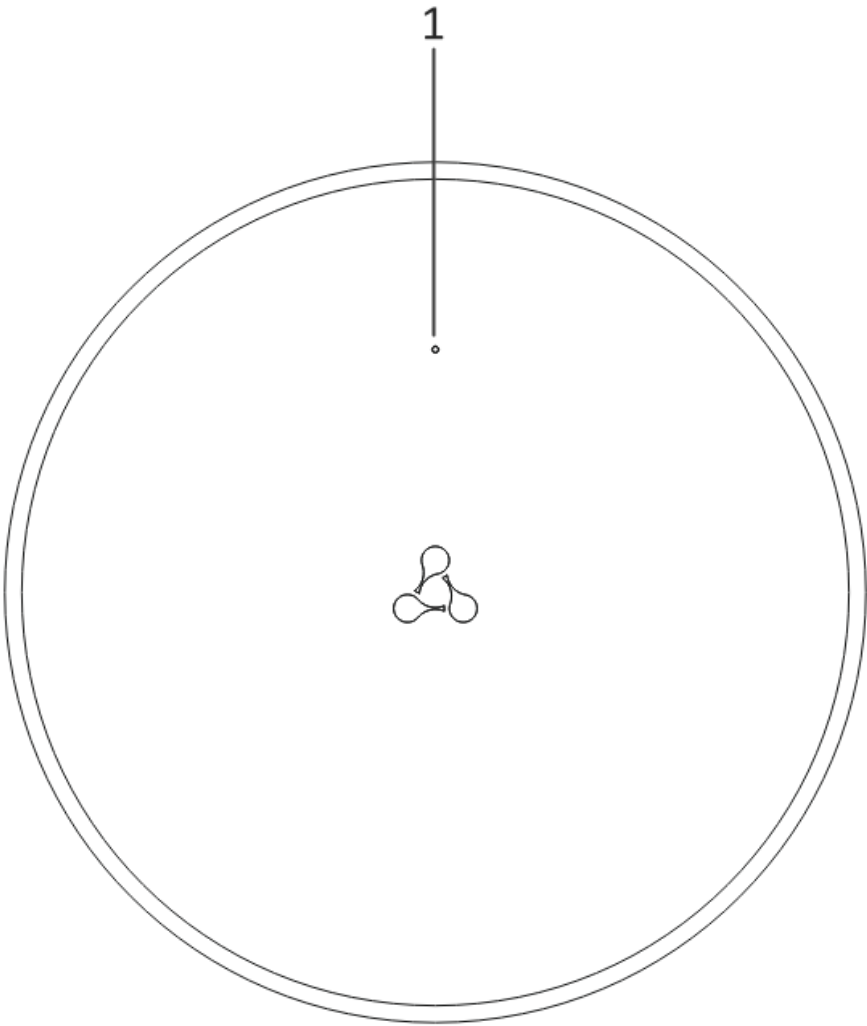


Figure 3 – WEP-550K top panel layout

Table 5 – Description of the top panel indicators

Panel element		Description
1	Power	Device operating status Indicator

2.6 Light indication

The current status of the device is displayed using the **LAN, Power** LEDs. The possible indicator states are described in Table 6.

Table 6 — Light indication of device status

LED	LED status	Description
LAN_1	Solid green (100 Mbps); Solid green, solid orange (1/2.5/5/10 Гбит/с)	The connection with a connected network device is established
	Flashing green	Packet data transmission over LAN interface
LAN_2	Solid green (100 Mbps); Solid green, solid orange (1/2.5/5/10 Gbps)	The connection with a connected network device is established
	Flashing green	Packet data transmission over LAN interface
Power	Solid green	The device power supply is enabled, normal operation
	Solid orange	The device is loaded but IP address is not received via DHCP
	Solid red	The device is loading

2.7 Restore the default configuration

The device can be reset to the factory configuration using the “F” button on the device. When the device is loaded, press and hold the “F” button (approximately 10–15 seconds) until “Power” indicator is flashing. The device will be rebooted automatically. DHCP client will be launched by default. If the address is not obtained via DHCP, the device will have the factory IP address — 192.168.1.10, and the following netmask — 255.255.255.0. Username/password for web interface: admin/password.

2.8 Supply package

The supply package includes:

- WEP-550K radio access equipment;
- mounting kit;
- user manual on a CD (optional);
- technical passport.

3 Rules and recommendations for device installation

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

3.1 Safety rules

1. Do not install the device near heat sources or in rooms and at places where temperature may reach values below 5 °C or above 40 °C.
2. Do not use the device in high-humidity areas. Do not expose the device to smoke, dust, water, mechanical vibration, or shock.
3. Do not open the device enclosure. There are no user serviceable parts inside.

✗ To prevent overheating of the device components and malfunction of the device, do not block the ventilation holes with foreign objects and do not place objects on the equipment surface.

3.2 Installation recommendations

1. The recommended installation position: horizontal, on the ceiling.
2. Before installing the device and turning it on, check the device for visible mechanical defects. If defects are observed, stop the device installation, fill in the corresponding act and contact the supplier.
3. If your device has been exposed to the cold for a long period of time, let it warm up at room temperature for two hours before starting work. If your device has been exposed to high humidity for a long period of time, let it stay under normal conditions for at least 12 hours before turning it on.
4. When placing your device, in order to provide the best Wi-Fi coverage consider the following rules:
 - Install the device at the center of a wireless network;
 - Minimize the number of barriers (walls, ceilings, furniture, and etc.) between the access point and other wireless network devices;
 - Do not install the device near electrical and radio devices (about 2 m);
 - It is not recommended to use radiophone and other equipment operating at the frequency of 2.4, 5 or 6 GHz, within the range of a Wi-Fi network;
 - Obstacles like glass/metal constructions, brick/concrete walls, water cans and mirrors can significantly reduce Wi-Fi action radius. It is not recommended to place the device inside a false ceiling as metal frame causes multipath signal propagation and signal attenuation.
5. When installing several access points, cell action radius must overlap with action radius of a neighboring cell at the level from -65 to -70 dBm. It is allowed to reduce the signal level to -75 dBm at cell boundaries, if it is not intended to use VoIP, video streaming and other sensitive to losses traffic in wireless network.

3.3 Calculating the number of required access points

To calculate the required number of access points, evaluate the required coverage zone. For more accurate assessment, it is necessary to make a radio examination of the room. Approximate radius of WEP-550K coverage area with a good-quality signal in case of mounting on a ceiling in typical office: 2.4 GHz – 40–50 m, 5 GHz/6 GHz – 20–30 m. In the absence of obstacles, the coverage radius: 2.4 GHz – up to 100 m, 5 GHz/6 GHz – up to 60 m.

Table 7 describes approximate attenuation values.

Table 7 – Attenuation values

Material	Change of signal level, dB		
	2.4 GHz	5GHz	6GHz
Drywall	3	3.2	3.5
Brick (9 cm wall)	5	7	8
Concrete (20 cm wall)	12	15	18
Reinforced concrete (30 cm wall)	20	25	30
Standard glass (window)	1	1,5	2
Furniture	1	1,5	2
Wood (hollow/door)	3	4	5
Wood (solid wood/wall)	10	15	20
Metal	25	30	35

3.4 Channel selection for neighboring access points

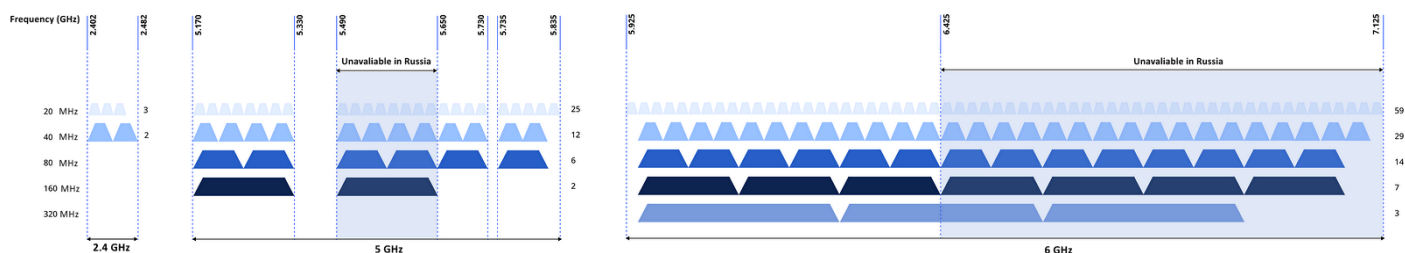


Figure 4 – Full Wi-Fi frequency spectrum

To avoid inter-channel interference between adjacent access points, it is recommended to set up non-overlapping channels.

When using a 40 MHz channel width in the 2.4 GHz band, there are no non-overlapping channels. In such cases, it is best to choose channels that are as far apart as possible.

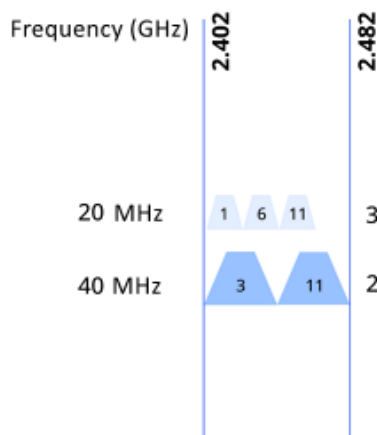


Figure 5 – Channels used in the 2.4 GHz band with channel widths of 20 and 40 MHz

Example of channel allocation scheme between adjacent access points in the 2.4 GHz band with channel width of 20 MHz is shown in Figure 6.

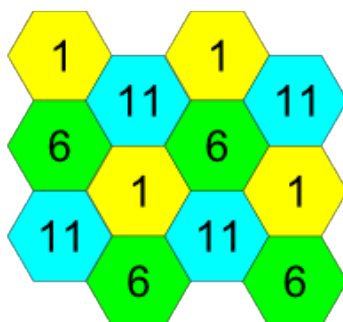


Figure 6 – Scheme of channel allocation between adjacent access points in the frequency range of 2.4 GHz when channel width is 20 MHz

Similarly, it is recommended to maintain this channel allocation mechanism when positioning access points between floors (Figure 7).

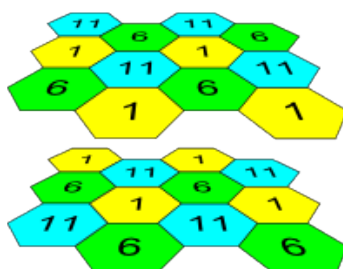


Figure 7 – Scheme of channel allocation between adjacent access points that are located between floors

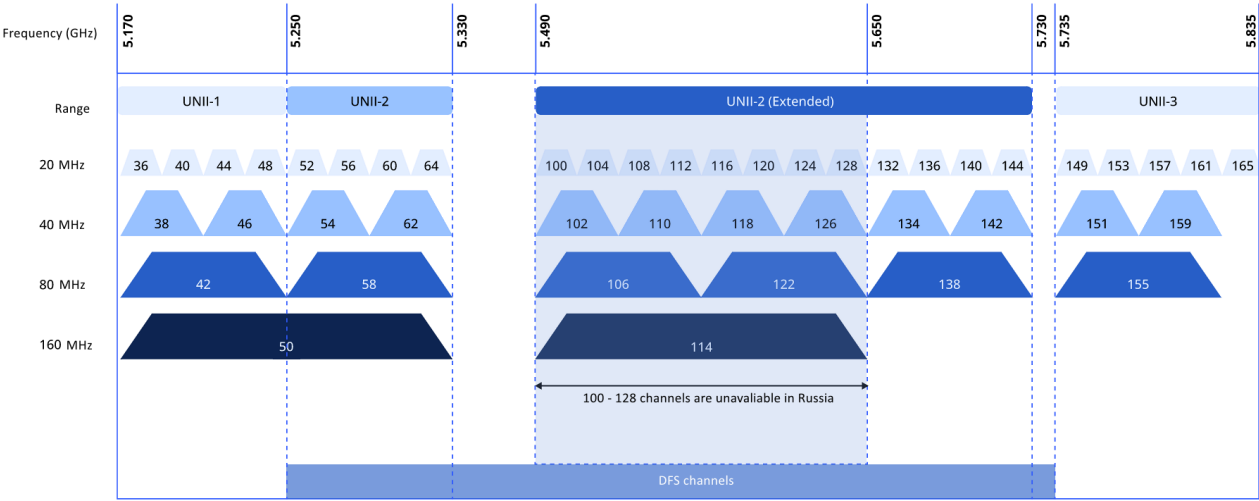


Figure 8 – Channels used in the 5 GHz band with channel widths of 20, 40, 80, and 160 MHz

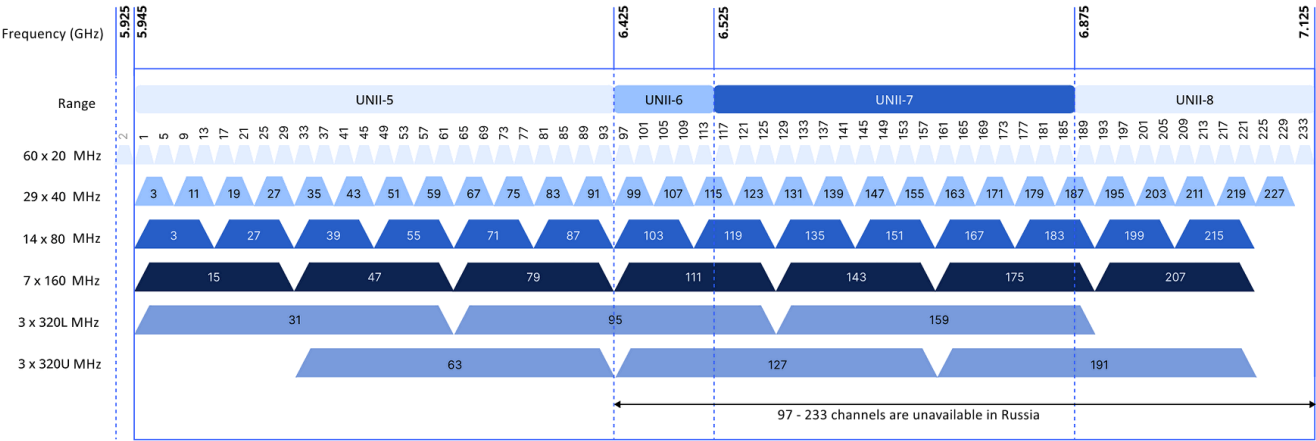


Figure 9 – Channels used in the 6 GHz band with channel widths of 20, 40, 80, 160, and 320 MHz

4 Device installation

The device can be installed on a ceiling profile, stud, flat surface, or VESA100 bracket in compliance with [the safety instructions and recommendations](#) listed above.

The device supply package includes required mounting kit to attach the device on a ceiling profile, stud, or flat surface.

4.1 Device installation on a flat surface

The holes for attaching the mounting plate to a flat surface are marked in Figure 10.

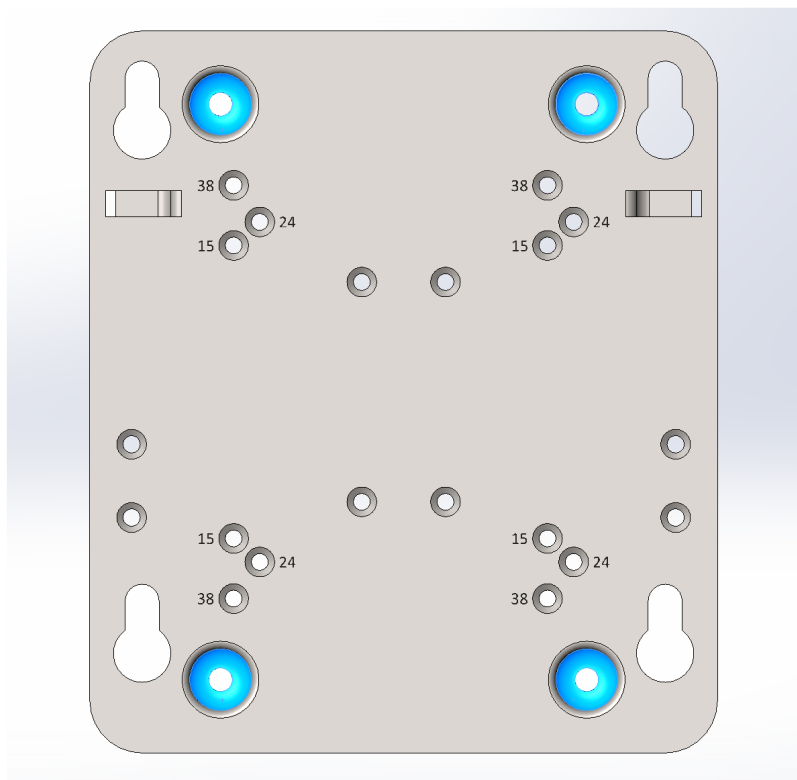


Figure 10 – Holes for attaching the mounting plate to a wall/ceiling

1. Secure the mounting plate to the surface using the fasteners from the supply package. The raised edges on the holes should face the mounting surface (Figure 11).



Figure 11 – Mounting plate attachment to surface

2. Connect the cables to the corresponding device connectors. The connector descriptions are provided in [Design](#). Install the device on the mounting plate by aligning the rubber feet with the holes on the plate, Figures 12 (a) and 12 (b).

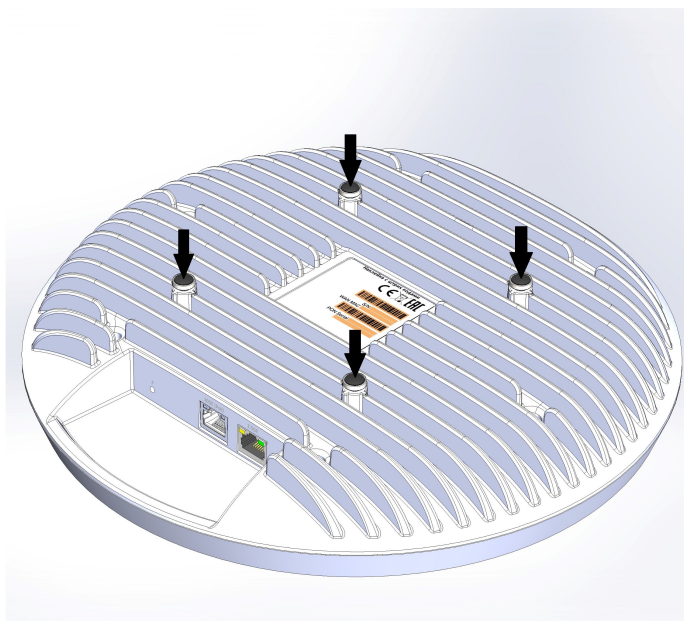


Figure 12 (a)

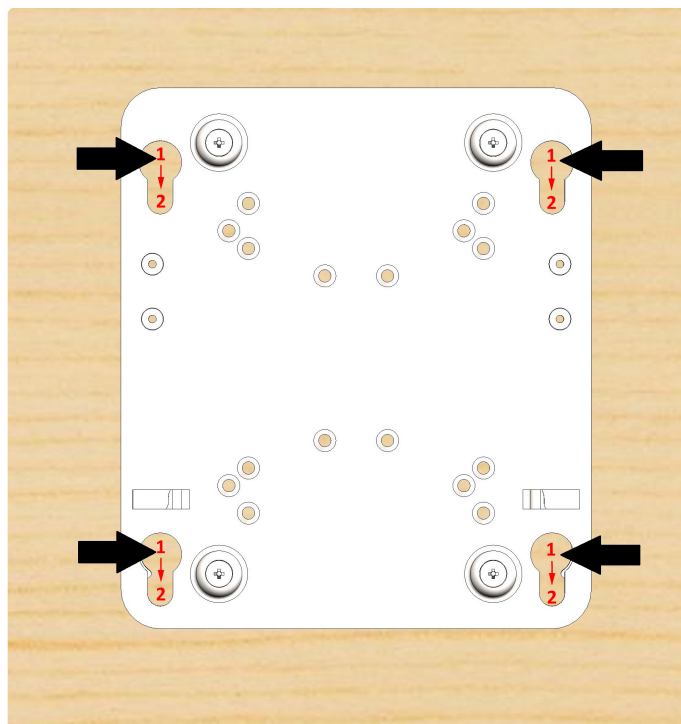


Figure 12 (b)

3. Secure the device on the mounting plate by sliding it from position 1 to position 2 (Figure 12 (b)).

4.2 Device installation on Armstrong ceiling

1. To install the device on a ceiling profile, use the ceiling clamp shown in Figure 13.

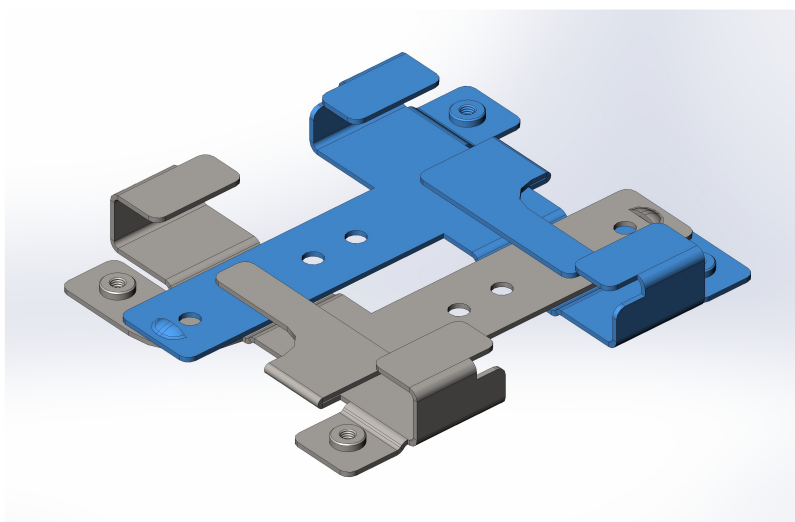


Figure 13 – Ceiling clamp

2. Spread the clamp to the extreme position and snap it onto the ceiling profile (Figure 14). The provided mounting option is designed for three types of profiles with widths of 15, 24, and 38 mm (see Figure 10).

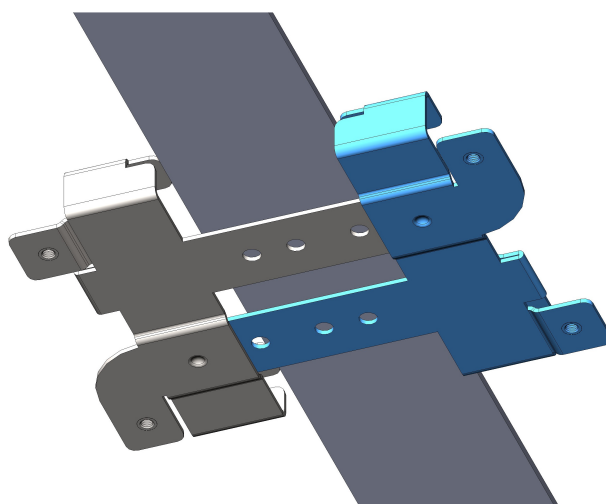


Figure 14 – Clamp attachment to ceiling profile

3. Secure the mounting plate to the ceiling clamp using M3×5 screws from the supply package, Figure 15.

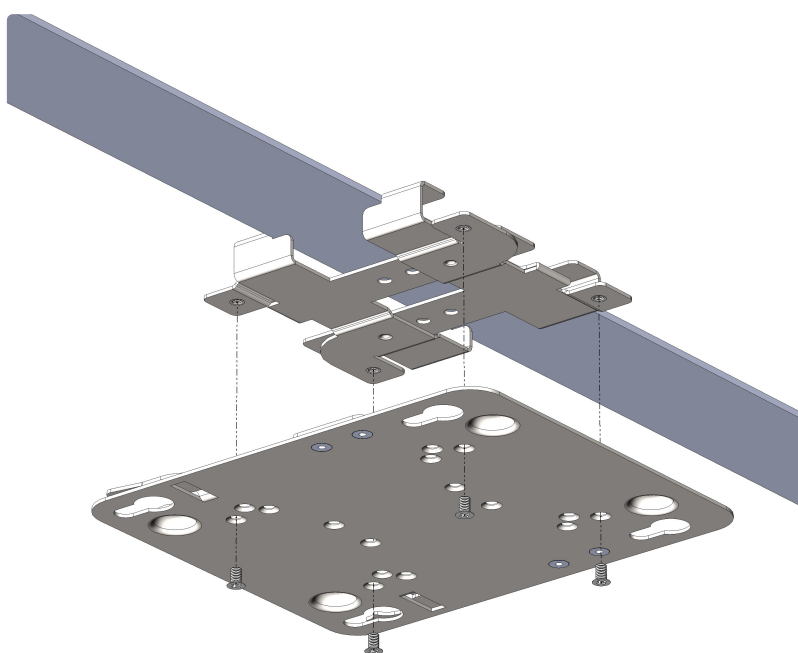


Figure 15 – Mounting plate attachment to clamp

4. Connect the cables to the corresponding device connectors. The connector descriptions are provided in [Design](#). Install the device on the mounting plate by aligning the rubber feet with the holes on the plate, Figure 16.

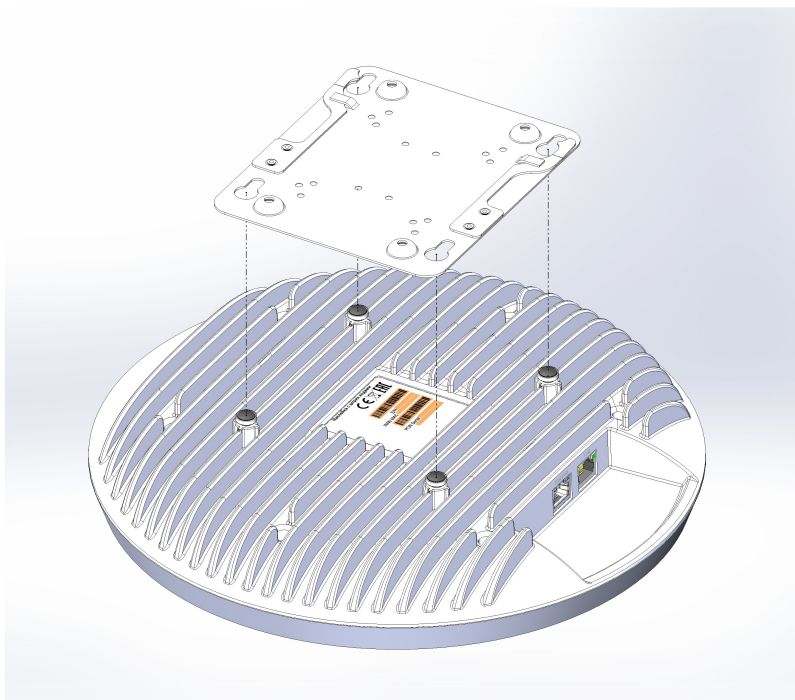


Figure 16 – Device installation on the mounting plate

5. Secure the device on the mounting plate by sliding it to the side in the direction of arrow 1, Figure 17 (a). Pay attention to the indicator position (arrow 2 direction) and connectors – they should be located along the profile direction, Figure 17 (b).

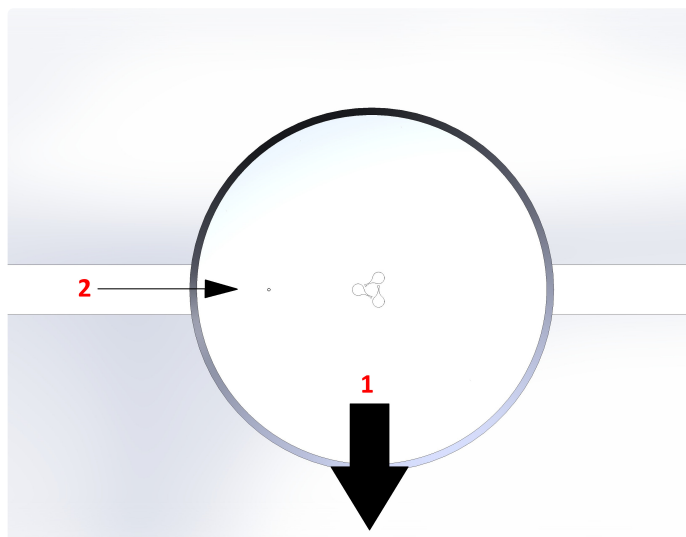


Figure 17 (a) – Securing the device on the mounting plate

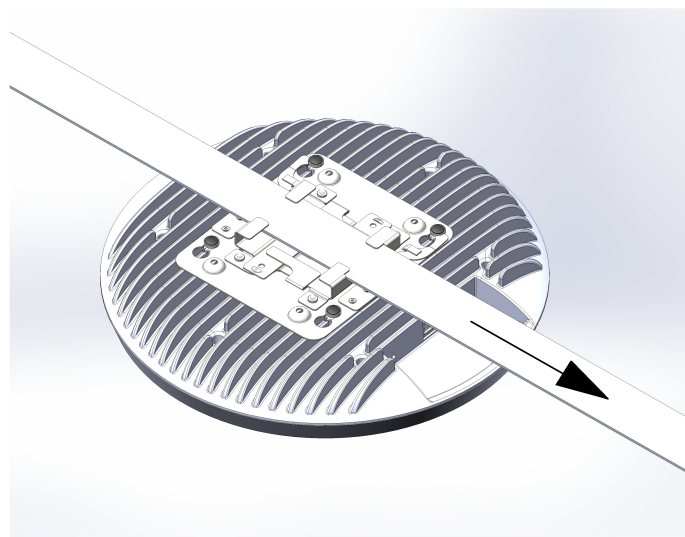


Figure 17 (b) – Connector arrangement

4.3 Device installation on a stud

1. Install the bracket from the supply package onto the mounting plate using M3×5 screws, Figure 18.

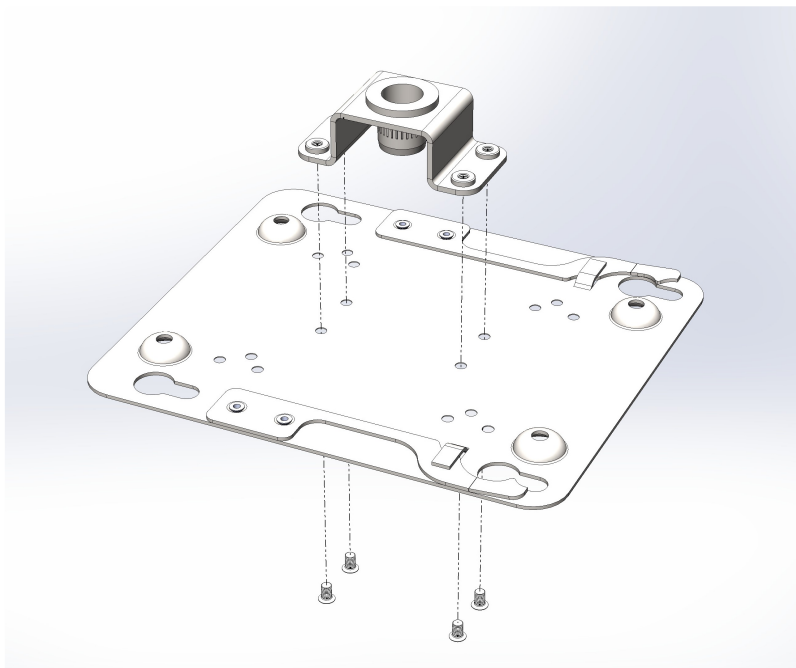


Figure 18 — Bracket installation on mounting plate

2. Screw the mounting plate onto the M10 stud until tight, Figure 19.

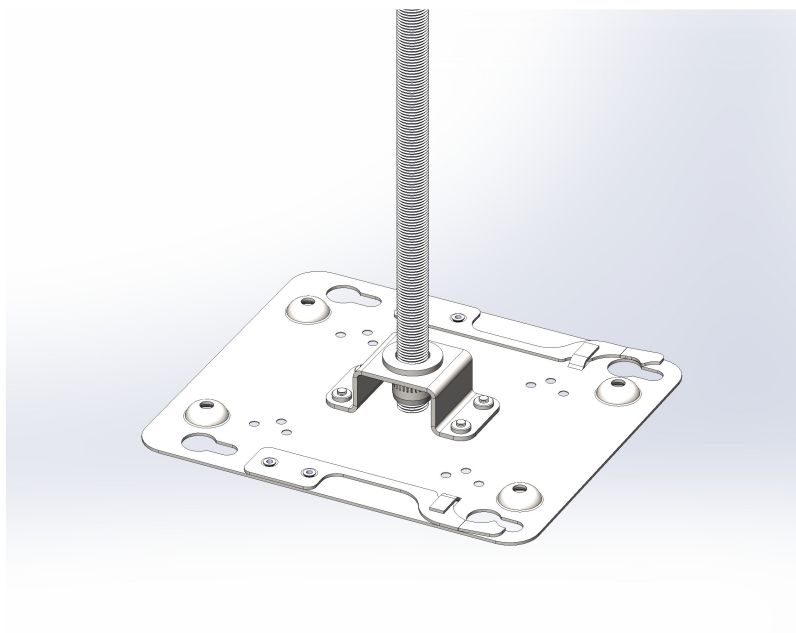


Figure 19 — Mounting plate installation on stud

3. Connect the cables to the corresponding device connectors. The connector descriptions are provided in [Design](#). Install the device on the mounting plate by aligning the rubber feet with the holes on the plate, Figure 20.

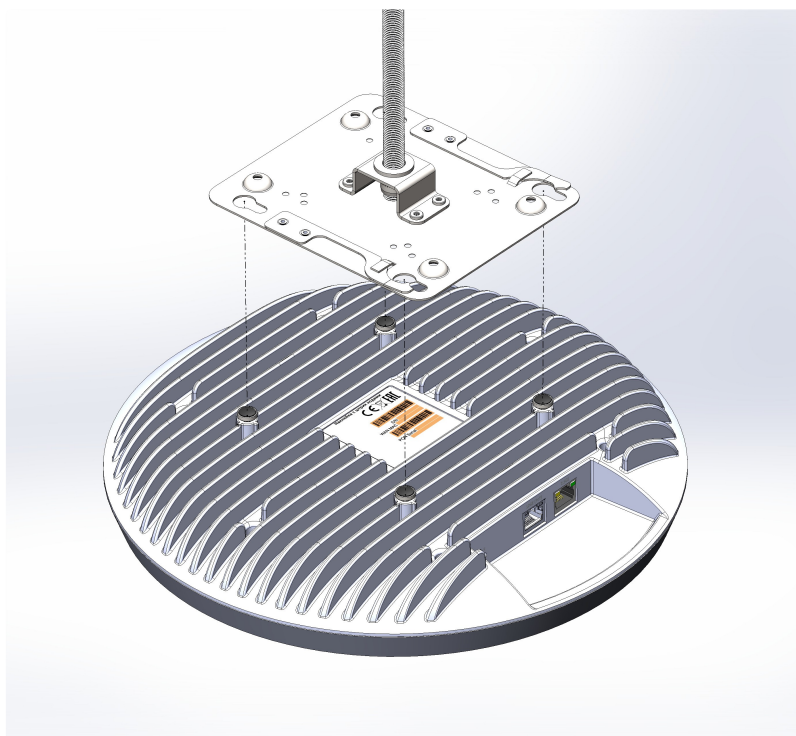


Figure 20 — Device installation on the mounting plate

4. Secure the device on the plate by sliding it to the side, Figure 21.

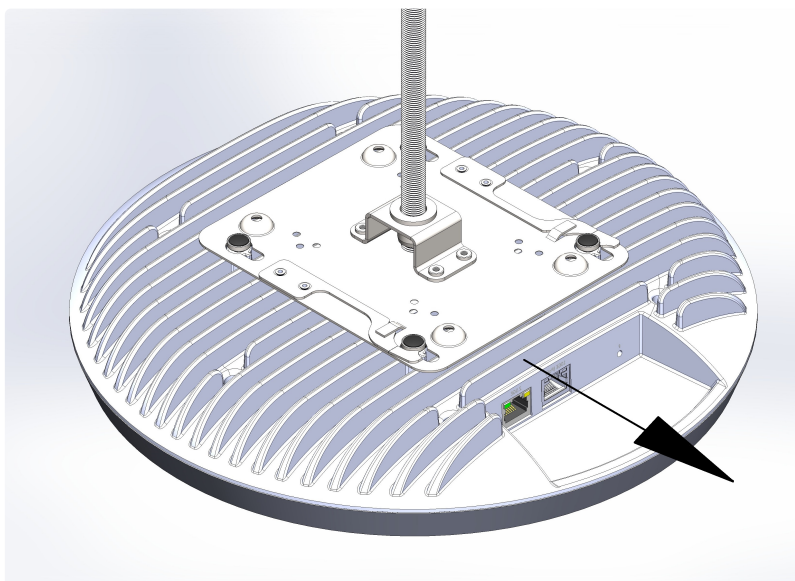


Figure 21 — Securing the device on the mounting plate

4.4 Device installation on VESA100 bracket

The design of this device provides for mounting using VESA100 brackets.

1. Unscrew the rubber feet located on the device heatsink (Figure 12 (a)).
2. Attach the bracket to the device.

✖ Before mounting on a VESA100 bracket, ensure that the mount is capable of supporting the device weight.

5 Device management via the web interface

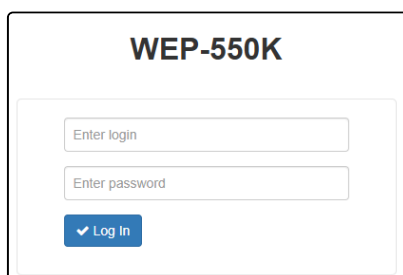
5.1 Getting started

To get started, connect to the device via the WAN interface using a web browser:

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

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

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

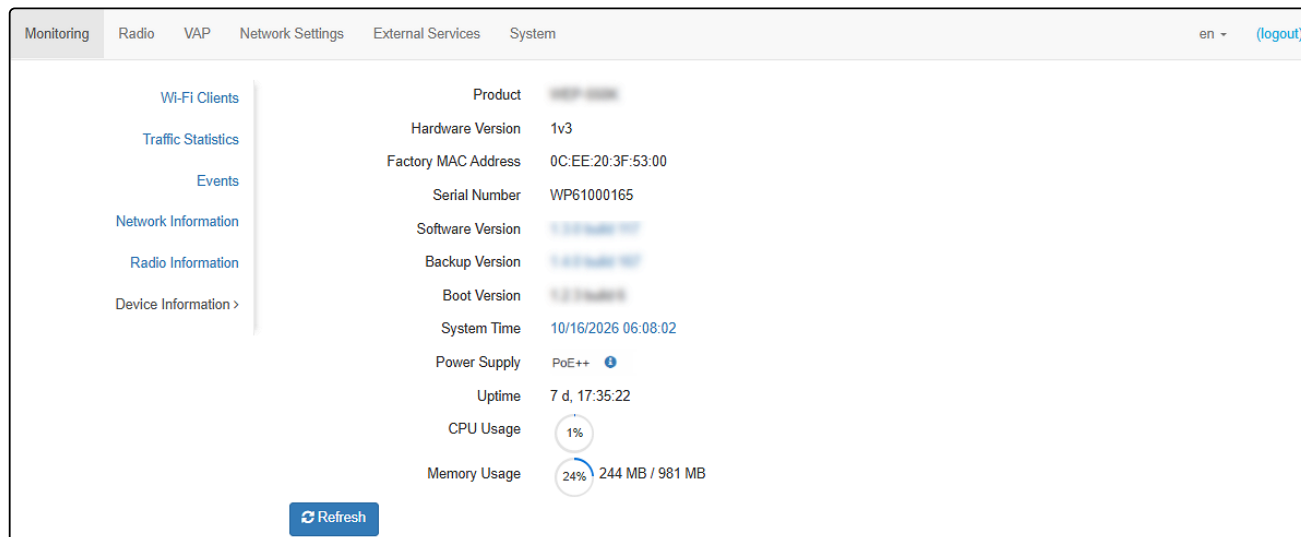


The image shows a login page for the WEP-550K device. It has a title 'WEP-550K' at the top. Below it, there are two input fields: 'Enter login' and 'Enter password'. At the bottom, there is a blue button labeled 'Log In' with a checkmark icon.

3. Enter the username in the "Enter login" field and the password in the "Enter password" field.

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

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

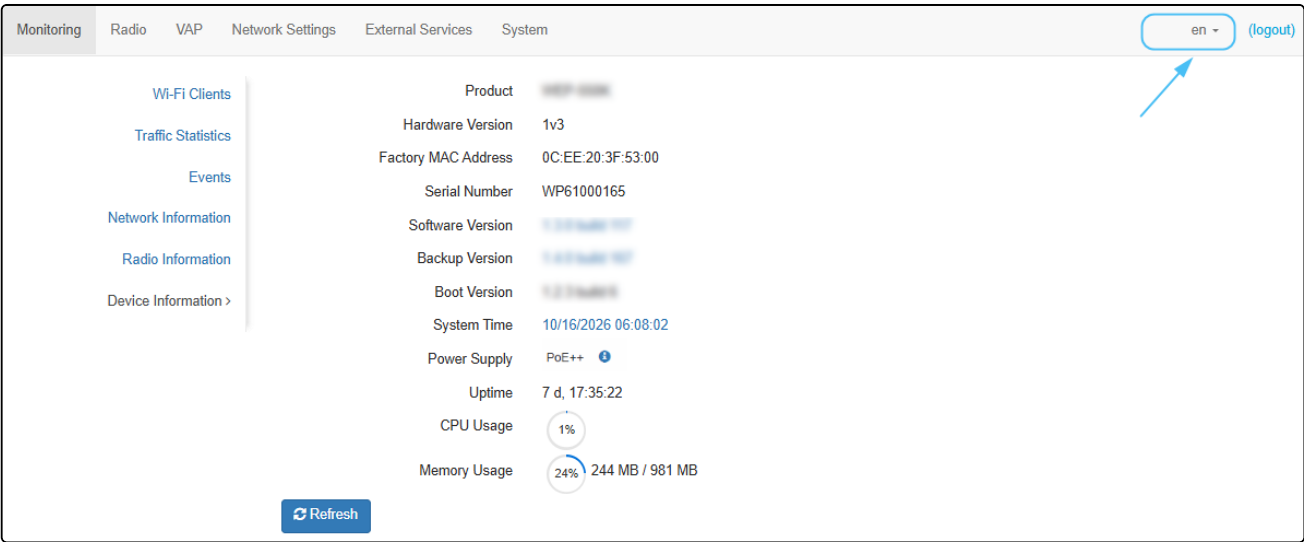


The image shows the 'Monitoring' page of the WEP-550K device. The page has a top navigation bar with tabs: Monitoring, Radio, VAP, Network Settings, External Services, and System. The 'Monitoring' tab is active. On the left, there is a sidebar with links: Wi-Fi Clients, Traffic Statistics, Events, Network Information, Radio Information, and Device Information >. The main content area displays system information:

Product	WEP-550K
Hardware Version	1v3
Factory MAC Address	0C:EE:20:3F:53:00
Serial Number	WP61000165
Software Version	1.0.0 (Build 1001)
Backup Version	1.0.0 (Build 1001)
Boot Version	1.0.0 (Build 1001)
System Time	10/16/2026 06:08:02
Power Supply	PoE++ ⓘ
Uptime	7 d, 17:35:22
CPU Usage	1%
Memory Usage	24% 244 MB / 981 MB

At the bottom left, there is a blue button labeled 'Refresh'.

5. If necessary, you can switch the information display language.



5.2 Applying configuration and discarding changes

1. Applying configuration

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

The WEP-550K web interface provides visual indication of the current status of the settings application process (Table 8).

Table 8 – Visual indication of the current status of the settings application process

Image	State description
	After clicking the "Apply" button, the process of applying the settings and writing them to the device memory starts. This is indicated by the icon in the tab name and on the "Apply" button.
	The icon in the tab name indicates successful saving and application of the settings.

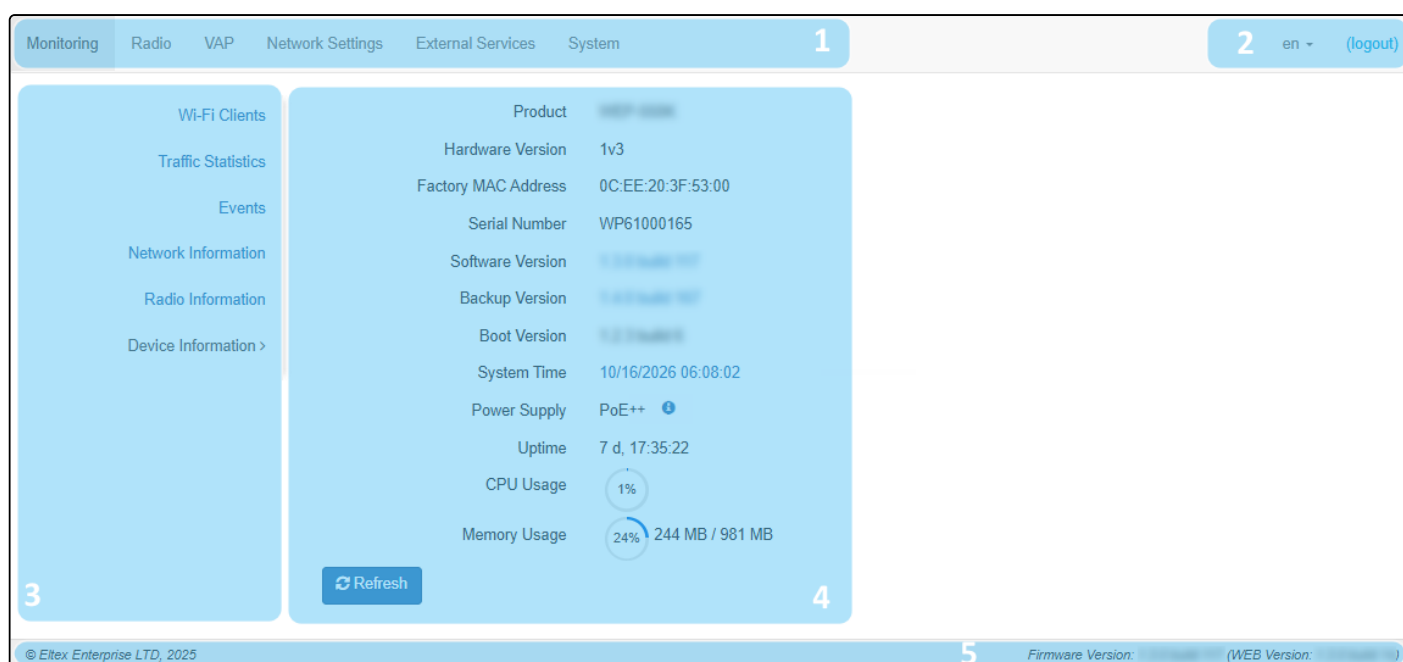
2. Discarding changes

The changes can be discarded only before clicking the "Apply" button. If you click the "Apply" button, the parameters changed on the page will be updated to the current values stored in the device memory. After clicking the "Apply" button, return to the previous settings will not be possible.

The button for discarding changes appears as follows: .

5.3 Web interface basic elements

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



User interface window is divided into five areas:

1. Menu tabs to group submenus by categories: **Monitoring, Radio, VAP, Network Settings, External Services, System.**
2. Interface language selection and the "Logout" button, designed to end a session in the web interface under a given user.
3. Submenu tabs to control the settings field.
4. Device configuration field for viewing data and configuration.
5. Information field displaying the firmware version installed on the device.

5.4 "Monitoring" menu

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

5.4.1 "Wi-Fi Clients" submenu

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

Information on connected clients is not displayed in real time. In order to update the information on the page, click the "Refresh" button.

Monitoring

Radio

VAP

Network Settings

External Services

System

en (logout)

Wi-Fi Clients >

Traffic Statistics

Events

Network Information

Radio Information

Device Information

Refresh

#	Hostname	IP Address	MAC	Interface	Link Capacity	Link Quality	RSSI, dBm	SNR, dB	TxRate	RxRate	Tx BW, MHz	Rx BW, MHz	Uptime
1	192.168.1.100	192.168.1.100	08:00:27:12:34:56	wlan2-vap0	100%	100%	-60	39	EHT NSS2-MCS3 ?xLTF GI 0.8us 1152	EHT NSS2-MCS8 ?xLTF GI 0.8us 3458	320	320	00:00:29
Total TX / RX, bytes				61 152 / 56 544				Fails, packets		0			
Total TX / RX, packets				235 / 543									

- **#** – number of the connected device in the list;
- **Hostname** – network name of the device;
- **IP address** – IP address of the connected device;
- **MAC** – MAC address of the connected device;
- **Interface** – WEP-550K interaction interface with the connected device;
- **Link Capacity** – parameter that displays the efficiency of modulation on the transmission used by an access point. It is calculated based on the number of packets transmitted to the client on each modulation, and the reduction factors. The maximum value is 100% (means that all packets are transmitted to the client at maximum modulation for the maximum nss type supported by the client). The minimum value is 2% (in the case when the packets are transmitted on the modulation nss1mcs0 for a client with MIMO 3×3 support). The parameter value is calculated for the last 10 seconds;
- **Link Quality** – parameter that displays the status of the link to the client, calculated based on the number of retransmit packets sent to the client. The maximum value is 100% (all transmitted packets were sent on the first attempt), the minimum value is 0% (no packets were successfully sent to the client). The parameter value is calculated for the last 10 s;
- **RSSI, dBm** – received signal level, dBm;
- **SNR, dB** – signal/noise ratio, dB;
- **TxRate** – channel data rate of transmission, Mbps;
- **RxRate** – channel data rate of receiving, Mbps;
- **Tx BW, MHz** – transmission bandwidth, MHz;
- **Rx BW, MHz** – reception bandwidth, MHz;
- **Uptime** – Wi-Fi client connection time.

To display more detailed information on a particular client, select it from the list.

A detailed description includes the following parameters:

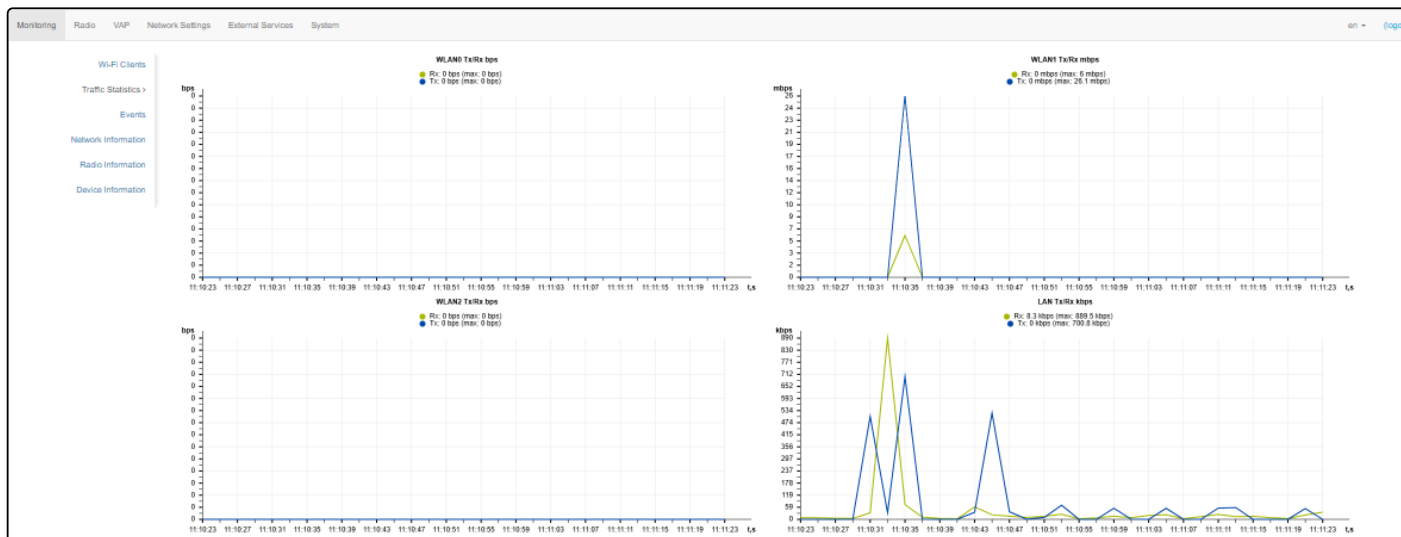
- **Total TX/RX, bytes** – number of bytes sent/received on the connected device;
- **Total TX/RX, packets** – number of packets sent/received on the connected device;
- **Fails, packets** – number of packets sent with errors on the connected device.

5.4.2 "Traffic Statistics" submenu

The **"Traffic Statistics"** submenu displays the graphs of the speed of transmitted/received traffic for the last 2 minutes, as well as statistics on the amount of transmitted/received traffic since the access point was turned on.

The LAN Tx/Rx diagram shows the speed of the transmitted/received traffic via Ethernet interface (ETH0) of the access point for the last 2 minutes. The graph is automatically updated every 6 seconds.

The WLAN0, WLAN1 and WLAN2 Tx/Rx graphs show the speed of the transmitted/received traffic via Radio 2.4 GHz, Radio 5 GHz and Radio 6 GHz interfaces for the last 2 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 packets dropped when sending;
- *Errors* – number of errors.

Transmit ▾				
Interface	Total Packets	Total Bytes	Total Drop	Errors
LAN	13856	6744400	0	0
WLAN0	0	0	0	0
WLAN1	7791	6841216	156	156
erspan0	0	0	0	0
eth1	0	0	0	0
ip6gre0	0	0	0	0
ip6tnl0	0	0	0	0
wlan1-apcli0	0	0	0	0
wlan2	0	0	0	0
wlan2-apcli0	0	0	0	0

"Receive" table description:

- *Interface* — name of the interface;
- *Total Packets* — number of successfully received packets;
- *Total Bytes* — number of successfully received bytes;
- *Total Drop* — number of packets dropped when receiving;
- *Errors* — number of errors.

Receive ▾				
Interface	Total Packets	Total Bytes	Total Drop	Errors
LAN	31894	12868940	78	0
WLAN0	0	0	0	0
WLAN1	7228	1578656	1448	1448
erspan0	0	0	0	0
eth1	0	0	0	0
ip0gre0	0	0	0	0
ip0tni0	0	0	0	0
wlan1-apcli0	0	0	0	0
wlan2	0	0	0	0
wlan2-apcli0	0	0	0	0

5.4.3 "Events" submenu

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

Monitoring

Radio

VAP

Network Settings

External Services

System

en

(logout)

Wi-Fi Clients

Traffic Statistics

Events >

Network Information

Radio Information

Device Information

Refresh

Clear

Date and Time	Type	Service	Message
Oct 16 00:33:27	daemon.info	networkd[4204]	DHCP-client: Interface br0 renew lease on 10.30.110.68.
Oct 15 21:33:27	daemon.info	networkd[4204]	DHCP-client: Interface br0 renew lease on 10.30.110.68.
Oct 15 18:33:27	daemon.info	networkd[4204]	DHCP-client: Interface br0 renew lease on 10.30.110.68.

- *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 9 – Event importance category descriptions

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

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

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

5.4.4 "Network Information" submenu

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

Monitoring

Radio

VAP

Network Settings

External Services

System

en

(logout)

Wi-Fi Clients

Traffic Statistics

Events

Network Information >

Radio Information

Device Information

WAN Status

Interface

br0

Protocol

DHCP

IP Address

192.168.1.100

Ethernet

ETH0

Link Status

Up

Speed

1000

Duplex

Full

RX Bytes

633.2 MB (663 981 727 bytes)

TX Bytes

11.6 MB (12 134 224 bytes)

ETH1

Link Status

Down

ARP

#	IP Address	MAC
0	192.168.1.1	88:87:8a:2b:4c:1a
1	192.168.1.100	28:86:2a:86:4b:f2
2	192.168.1.1	88:87:8a:2b:4c:1a
3	192.168.1.1	88:87:8a:2b:4c:1a

Routes

#	Interface	Destination	Gateway	Netmask	Flags
0	br0	0.0.0.0	192.168.1.1	0.0.0.0	UG
1	br0	192.168.1.0	0.0.0.0	255.255.255.0	U

WAN Status:

- *Interface* – name of the bridge interface;
- *Protocol* – protocol used for access to WAN;
- *IP Address* – device IP address in external network;

Ethernet:

- *Link Status* – Ethernet port status;
- *Speed* – Ethernet port connection speed;
- *Duplex* – data transfer mode:
 - *Full* – full duplex;
 - *Half* – half-duplex.
- *RX Bytes* – number of bytes received on ETH;
- *TX Bytes* – number of bytes sent from ETH.

ARP:

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

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

Routes:

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

The following flag values exist:

- **U** — means that the route is created and passable.
- **H** — indicates the route to the specific host.
- **G** — means that the route lies through 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.

5.4.5 "Radio Information" submenu

In the **"Radio Information"** submenu, the current status of the WEP-550K radio interfaces is displayed.

Monitoring	Radio	VAP	Network Settings	External Services	System	en ▾	(logout)
Wi-Fi Clients	Radio 2.4 GHz						
Traffic Statistics	Status						Off
Events	MAC						XX:XX:XX:XX:XX:XX
Network Information	Mode						IEEE 802.11b/g/n/ax/be
Radio Information >	Radio 5 GHz						
Device Information	Status						On
	MAC						XX:XX:XX:XX:XX:XX
	Mode						IEEE 802.11a/n/ac/ax/be
	Channel						40 (5200 MHz)
	Channel Bandwidth, MHz						20
	Radio 6 GHz						
	Status						On
	MAC						XX:XX:XX:XX:XX:XX
	Mode						IEEE 802.11ax/be
	Channel						37 (6135 MHz)
	Channel Bandwidth, MHz						20

The access point radio interfaces can be in two states: "On" and "Off". The status of each radio interface is shown in the identically named "Status" parameter.

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

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

"Off":

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

"On":

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

5.4.6 "Device Information" submenu

In the "**Device Information**" submenu, the main WEP-550K specifications are displayed.

Monitoring

Radio

VAP

Network Settings

External Services

System

en (logout)

Wi-Fi Clients

Traffic Statistics

Events

Network Information

Radio Information

Device Information >

Product

Hardware Version

Factory MAC Address

Serial Number

Software Version

Backup Version

Boot Version

System Time

Power Supply

Uptime

CPU Usage

Memory Usage

100P-00000

1v3

0C:EE:20:3F:53:00

WP61000165

1.0.0.0-0000-0000

1.0.0.0-0000-0000

1.0.0.0-0000-0000

10/16/2026 06:08:02

PoE++ ⓘ

7 d, 17:35:22

1%

24% 244 MB / 981 MB

Refresh

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

5.5 "Radio" menu

In the "**Radio**" menu, the radio interfaces of the device can be configured.

5.5.1 "Radio 2.4 GHz" submenu

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

✓ To connect devices in the IEEE 802.11be (Wi-Fi 7) standard, it is recommended to configure WPA2/ WPA3, WPA3, or OWE security mode.

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

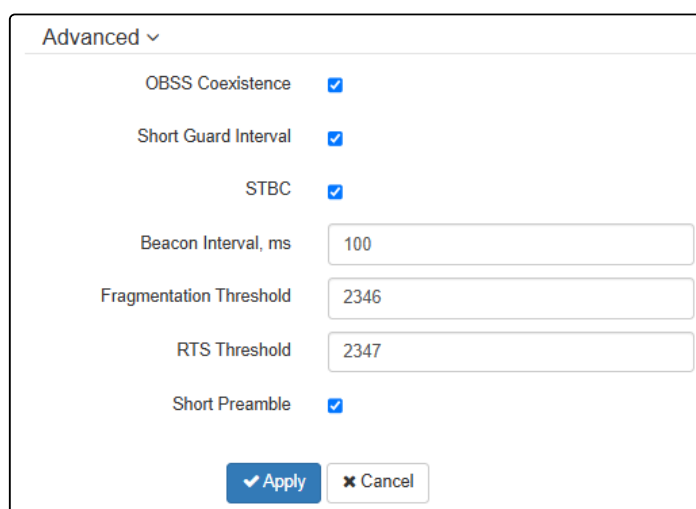
- ✓ If the "Use Limit Channels" list contains a channel that is not available for selection, it will be marked in grey. For the new configuration to be applied to the access point, only available (highlighted in blue) channels must be specified in the "Use Limit Channels" list.

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

- The "Primary Channel" parameter becomes available for editing and takes the default value "Lower",
- The channel 11 in the "Use Limit Channels" list changes its color from blue to grey.

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

In the "Advanced" section, advanced parameters of the device radio interface are configured.

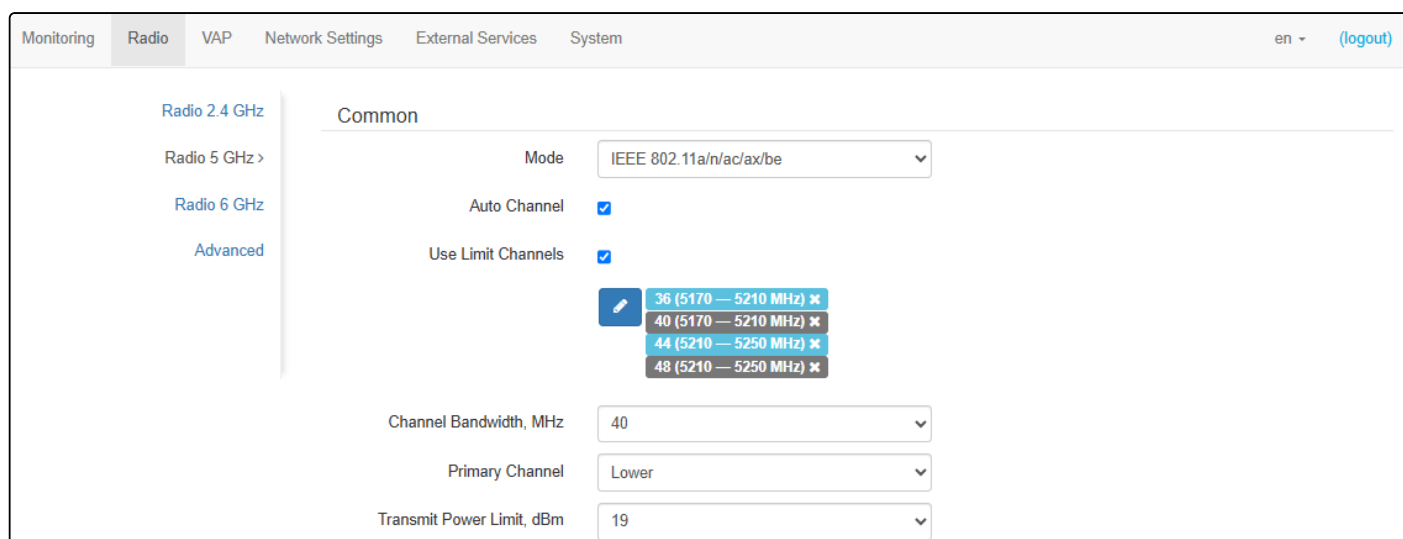


- *OBSS Coexistence* — automatic channel bandwidth reduction when the radio environment is congested. When the flag is set, the mode is enabled;
- *Short Guard Interval* — support for Short Guard Interval. The access point transmits data using a 400 ns guard interval (instead of 800 ns) when communicating with clients that also support Short Guard Interval;
- *STBC* — Space-Time Block Coding method aimed at improving data transmission reliability. When the flag is set, the device transmits one data stream through several antennas. If the flag is not set, the device does not transmit the same data stream through several antennas;
- *Beacon Interval, ms* — the period of Beacon frame transmission. The frames are transmitted so that the access point can be detected in the radio environment. The parameter accepts values 20–2000 ms, default — 100 ms;
- *Fragmentation Threshold* — frame fragmentation threshold in bytes. Accepts values 256–2346, default — 2346;
- *RTS Threshold* — specifies the number of bytes after which a Request to Send is sent. Decreasing this value may improve the access point performance when there are many connected clients, however it reduces the overall throughput of the wireless network. Accepts values 0–2347, default — 2347;
- *Short Preamble* — use of the short packet preamble.

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

5.5.2 "Radio 5 GHz" submenu

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



The screenshot shows the 'Radio 5 GHz' configuration page. The 'Common' tab is active. The 'Mode' is set to 'IEEE 802.11a/n/ac/ax/be'. 'Auto Channel' and 'Use Limit Channels' are both checked. Below these, there is a list of channels: 36 (5170 — 5210 MHz), 40 (5170 — 5210 MHz), 44 (5210 — 5250 MHz), and 48 (5210 — 5250 MHz). Each channel has a delete icon. 'Channel Bandwidth' is set to 40 MHz, 'Primary Channel' is set to Lower, and 'Transmit Power Limit' is set to 19 dBm.

✓ To connect devices in the IEEE 802.11be (Wi-Fi 7) standard, it is recommended to configure WPA2/ WPA3, WPA3 or OWE security mode.

- *Mode* — interface operation mode according to the following standards:
 - IEEE 802.11 a/n/ac;
 - IEEE 802.11a/n/ac/ax;
 - IEEE 802.11a/n/ac/ax/be.
- *Auto Channel* — when checked, the access point will automatically select the least congested radio channel for the Wi-Fi interface. When unchecked, access to set the static operating channel becomes available;
- *Channel* — select channel for data transmission;
- *Use Limit Channels* — when checked, the access point will use a user-defined list of channels to work in automatic channel selection mode. If the "Use Limit channels" flag is not checked or there are no channels in the list, the access point will select the operation channel from all available channels in the given band. 5 GHz band channels: 36–64, 132–144, 149–165;
- *Channel Bandwidth, MHz* — channel bandwidth on which the access point operates; takes values 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. The primary channel is used by clients who only support 20 MHz channel bandwidth:
 - *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.
- *Transmission Power Limit, dBm* — adjustment of the Wi-Fi transmitter signal power in dBm. Takes values from 0 to 19 dBm.

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

Example. No settings have been made on the access point yet; by default, Radio 5 GHz has "Channel Bandwidth" set to 20 MHz, and the "Use Limit channels" list specifies the channels: 36, 40, 44, 48. Suppose it is required to set "Channel Bandwidth" to 40 MHz. When this parameter is changed from 20 MHz to 40 MHz, the following happens:

- The "Primary Channel" becomes available for editing and takes the default value "Upper",
- The 36 and 44 channels in the "Use Limit Channels" list changes its color from blue to grey.

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

In the "Advanced" section, advanced parameters of the device radio interface are configured.

Advanced ▾

OBSS Coexistence ☒

DFS Support Enabled ▾

Short Guard Interval ☒

STBC ☒

Beacon Interval, ms

Fragmentation Threshold

RTS Threshold

Short Preamble ☒

- *OBSS Coexistence* — automatic channel bandwidth reduction when the radio environment is congested. When the flag is set, the mode is enabled;
- *DFS Support* — mechanism that requires wireless devices to scan the radio spectrum and avoid using channels that overlap with those used by radar systems in the 5 GHz band:
 - *Disabled* — mechanism is disabled. DFS channels are not available for selection;
 - *Enabled* — mechanism is enabled;
 - *Forced* — mechanism is disabled. DFS channels are available for selection.
- *Short Guard Interval* — support for Short Guard Interval. The access point transmits data using a 400 ns guard interval (instead of 800 ns) when communicating with clients that also support Short Guard Interval;
- *STBC* — Space-Time Block Coding method aimed at improving data transmission reliability. When the flag is set, the device transmits one data stream through several antennas. If the flag is not set, the device does not transmit the same data stream through several antennas;
- *Beacon Interval, ms* — the period of Beacon frame transmission. The frames are transmitted so that the access point can be detected in the radio environment. The parameter accepts values 20–2000 ms, default — 100 ms;
- *Fragmentation Threshold* — frame fragmentation threshold in bytes. Accepts values 256–2346, default — 2346;
- *RTS Threshold* — specifies the number of bytes after which a Request to Send is sent. Decreasing this value may improve the access point performance when there are many connected clients, however it reduces the overall throughput of the wireless network. Accepts values 0–2347, default — 2347;
- *Short Preamble* — use of the short packet preamble.

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

5.5.3 "Radio 6 GHz" submenu

In the "**Radio 6 GHz**" submenu, the main parameters of the radio interface of the device operating in the 6 GHz band can be configured.

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

Radio 2.4 GHz
Radio 5 GHz
Radio 6 GHz >
Advanced

Common

Mode IEEE 802.11ax/be

Auto Channel ☒

Use Limit Channels ☒

5 (5945 — 5985 MHz) ✕
21 (6025 — 6065 MHz) ✕
37 (6105 — 6145 MHz) ✕
53 (6185 — 6225 MHz) ✕
69 (6265 — 6305 MHz) ✕
85 (6345 — 6385 MHz) ✕

Channel Bandwidth, MHz 40

Primary Channel Lower

Transmit Power Limit, dBm 19

✓ To connect devices in the IEEE 802.11be (Wi-Fi 7) standard, it is recommended to configure the security mode WPA2/WPA3, WPA3 or OWE.

✓ For 6 GHz, only the OWE, WPA3, WPA3-Enterprise security modes are available.

- *Mode* — interface operation mode according to the following standards:
 - IEEE 802.11ax;
 - IEEE 802.11ax/be.
- *Auto Channel* — when checked, the device will automatically select the least congested radio channel for the Wi-Fi interface. Unchecking the flag opens the access to install the static operation channel;
- *Channel* — select channel for data transmission;
- *Use Limit Channels* — when checked, the access point will use a user-defined list of channels to work in automatic channel selection mode. If the "Use Limit Channels" flag is not checked or there are no channels in the list, the access point will select the operation channel from all available channels of the given frequency band. 6 GHz band channels: 1–93;
- *Channel Bandwidth, MHz* — channel bandwidth, on which the access point operates. The parameter may take values 20, 40, 80, 160, and 320 MHz;
- *Primary Channel* — parameter can only be changed if the bandwidth of a statically specified channel is equal to 40 MHz or 320 MHz.
 - The 40 MHz channel can be considered as consisting of two 20 MHz channels, which border in the frequency range. These two 20 MHz channels are called primary and secondary channels. The primary channel is used by clients who only support 20 MHz channel bandwidth:
 - *Upper* — 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.
 - The 320 MHz channel can be considered as consisting of two 160 MHz bands, which border in the frequency range. The channel used by clients who only support 20 MHz bandwidth may be located in one of these bands:
 - *Upper* — the 20 MHz data transmission channel will be located in the upper 160 MHz band;
 - *Lower* — the 20 MHz data transmission channel will be located in the lower 160 MHz band.

- *Transmission Power Limit, dBm* — adjustment of the signal strength of the Wi-Fi transmitter in dBm. Accepts values from 0 to 19 dBm.

✓ If a channel unavailable for selection is specified in the "Use Limit Channels" list, it will be marked in grey. For the new configuration to be applied on the access point, only available (highlighted in blue) channels must be specified in the "Use Limit Channels" list.

Example. No settings have been made on the access point yet, Radio 5 GHz is set to 20 MHz "Channel Bandwidth" by default, and channels are specified in the "Use Limit Channels" list: 1, 5, 9, 13. Suppose it is required to set the "Channel Bandwidth" parameter to 40 MHz. When you change this parameter from 20 MHz to 40 MHz, the following happens:

- The "Primary Channel" parameter becomes available for editing and the default value is "Upper",
- The 1 and 9 channels in the "Use Limit Channels" list change their color from blue to grey.

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

In the "Advanced" section, advanced radio interface parameters of the device are configured.

Advanced ▾

OBSS Coexistence	☐
Short Guard Interval	☒
STBC	☒
Beacon Interval, ms	100
Fragmentation Threshold	2346
RTS Threshold	2347
Short Preamble	☒

- *OBSS Coexistence* — automatic channel bandwidth reduction when the radio environment is loaded. When the flag is set, the mode is enabled;
- *Short Guard Interval* — support for Short Guard Interval. The access point transmits data using a 400 ns guard interval (instead of 800 ns) when communicating with clients which also support Short Guard Interval;
- *STBC* — Space-Time Block Coding method aimed at improving 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 transmitted for the access point to be detected in the radio environment; takes values 20–2000 ms, default: 100 ms;
- *Fragmentation Threshold* — frame fragmentation threshold in bytes. Takes values 256–2346, default: 2346;
- *RTS Threshold* — specifies the number of bytes over which the Request to Send will be sent. Decreasing this value may improve the performance of the access point when there are a lot of connected clients. However, this reduces general throughput of wireless network. The parameter takes values 0–2347, by default: 2347;
- *Short Preamble* — use of the packet short preamble.

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

5.5.4 "Advanced" submenu

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

The screenshot shows the 'Advanced' submenu for the Radio settings. The sidebar on the left lists 'Radio 2.4 GHz', 'Radio 5 GHz', 'Radio 6 GHz', and 'Advanced >'. The main content area is titled 'Advanced' and contains a 'Country' dropdown menu currently set to 'Russia', an 'Unlock' checkbox, and two buttons: 'Apply' and 'Cancel'.

- *Country* — the name of the country in which the access point operates. Select the "Unlock" checkbox to change a country. Depending on the selected value, the channel bandwidth and transmit power limit restrictions in effect in the selected country 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. If the client device is licensed for use in a different region, probably, a connection with the access point will not be established.

✗ Configuring local (regional) restrictions, 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 "Apply". Click "Cancel" to discard the changes.

5.6 "VAP" menu

The **"VAP"** menu is used to configure Wi-Fi virtual access points (VAP) and Multi-link Operation (MLO) groups.

5.6.1 "Summary" submenu

The **"Summary"** submenu displays the settings of all VAPs on the Radio 2.4 GHz, Radio 5 GHz, and Radio 6 GHz radio interfaces, as well as the MLO group settings. You can view the settings of each virtual access point in the VAP0–VAP15 sections and of MLO groups in the 1–16 sections.

VAP	Enabled	Security Mode	VLAN ID	SSID	Broadcast SSID	Band Steer	Station Isolation
VAP0	☒	Off		Virtual Access Point 1 (2.4 GHz)	☒	☐	☐
VAP1	☐	Off		Virtual Access Point 1 (2.4 GHz)	☐	☐	☐
VAP2	☐	Off		Virtual Access Point 1 (2.4 GHz)	☐	☐	☐
VAP3	☐	Off		Virtual Access Point 1 (2.4 GHz)	☐	☐	☐

[Show all](#)

- *VAP0–VAP15* – ordinal number of the virtual access point;
- *1-16* – ordinal number of the MLO group;
- *Enabled* – when this check box is selected, the virtual access point is enabled; otherwise, it is disabled;
- *Security mode* – type of data encryption used on the virtual access point;
- *VLAN ID* – VLAN number from which the tag is removed when transmitting traffic to Wi-Fi clients connected to this VAP. When traffic passes in the reverse direction, the VLAN ID tag will be added to untagged traffic from clients;
- *SSID* – virtual wireless network name;
- *Broadcast SSID* – when this check box is selected, SSID broadcasting is enabled; otherwise, it is disabled;
- *Band Steer mode* – when this check box is selected, client connections to the 5 GHz network are actively prioritized. To use this function, you need to create a VAP with an identical SSID on at least two radio interfaces and enable the "Band Steer mode" parameter on them;
- *Station Isolation* – when this check box is selected, traffic isolation between clients within a single VAP is enabled.

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

5.6.2 "VAP" submenu

The screenshot displays the 'VAP' configuration page. On the left, a sidebar contains navigation links: Monitoring, Radio, VAP (selected), Network Settings, External Services, and System. Below these are radio frequency options: 2.4 GHz, 5 GHz, 6 GHz, and MLO. The main content area shows a list of VAPs (VAP0 through VAP13) and a 'Common Settings' section for VAP0. The settings are as follows:

- Enabled:** ☒
- VLAN ID:** ☒
- SSID:** Virtual Access Point 0 (2.4GHz)
- Broadcast SSID:** ☒
- Band Steer:** ☒
- Station Isolation:** ☒
- 802.11k/v:** ☒
- Maximum Stations:** 0
- Security Mode:** Off (dropdown menu)
- 802.11r Support:** ☐

General settings:

- **Enabled** – when this check box is selected, the virtual access point is enabled; otherwise, it is disabled;
- **VLAN ID** – VLAN number from which the tag is removed when transmitting traffic to Wi-Fi clients connected to this VAP. When traffic passes in the reverse direction, the VLAN ID tag will be added to untagged traffic from clients;
- **SSID** – virtual wireless network name;
- **Broadcast SSID** – when this check box is selected, SSID broadcasting is enabled; otherwise, it is disabled;
- **Band Steer** – when this check box is selected, client connections to the 5 GHz network are actively prioritized. To use this function, you need to create a VAP with an identical SSID on at least two radio interfaces and enable the "Band Steer mode" parameter on them;
- **Station Isolation** – when this check box is selected, traffic isolation between clients within a single VAP is enabled;
- **802.11k/v** – enable support for the 802.11k/v standards on the virtual access point;
- **Maximum Stations** – maximum number of clients that can connect to the virtual network;
- **Security mode** – wireless network access security mode:

✓ To connect devices in the IEEE 802.11be (Wi-Fi 7) standard, it is recommended to configure the WPA2/ WPA3, WPA3 or OWE security mode.

- **Off** – do not use encryption for data transmission. The access point is available for any client to connect;
- **OWE (Opportunistic Wireless Encryption)** – encryption method that ensures the security of data transmitted over an unsecured network.
No additional actions or password entry are required from users to connect to the network.
WPA, WPA2, WPA/WPA2, WPA2/WPA3, WPA3 – encryption methods; when one of them is selected, the following setting becomes available:
 - **WPA Key** – key/password required to connect to the virtual access point. The key length is from 8 to 63 characters.
- **WPA-Enterprise, WPA2-Enterprise, WPA/WPA2-Enterprise, WPA2/WPA3-Enterprise, WPA3-Enterprise** – wireless channel encryption mode in which the client is authorized on a centralized RADIUS server. To configure this security mode, the RADIUS server parameters must be specified.

A key for the RADIUS server must also be specified. When a specific security mode is selected, the following settings become available.

Security Mode: WPA2/WPA3-Enterprise

MFP: Capable

PMKSA Caching: ☐

802.11r Support: ☒

Manual: ☒

FT-over-DS: ☐

R0-key-holder-id: root

R1-key-holder-id: XX:XX:XX:XX:XX:XX

Mobility Domain: 0

Remote MAC

#	MAC	Remote-R0-key-holder-id	Remote-R1-key-holder-id	RRB-key-R0	RRB-key-R1
+ Add					

Minimize

- **MFP** – management frame protection (available in security modes WPA2, WPA3, WPA2/WPA3, WPA2-Enterprise, WPA2/WPA3-Enterprise and WPA3-Enterprise; when other security modes are selected, MFP is set to *Not Required*; when security mode WPA3, WPA3-Enterprise is selected, MFP is set to *Required*):
 - *Not Required* – management frame protection is disabled;
 - *Capable* – protection works if the client supports MFP. Clients without MFP support can connect to this VAP;
 - *Required* – protection is enabled, clients that do not support MFP cannot connect.
- **PMKSA Caching** – a flag that controls enabling caching of Enterprise client connection information. When this function is enabled, the access point remembers the client device for 12 hours after authorization and does not require re-authentication on the RADIUS server when connecting within this time. Enabling this function reduces roaming time when the client returns to the access point in WPA Enterprise mode. The setting is available only in Enterprise security modes;
- **802.11r Support** – fast roaming function, works only with clients that support the IEEE 802.11r standard. 802.11r roaming is possible only between VAPs with security modes WPA2, WPA3, WPA2/WPA3, WPA2-Enterprise, WPA3-Enterprise, WPA2/WPA3-Enterprise.
 - **802.11r Support** – enable support for the 802.11r standard on a virtual access point;
 - **Manual** – when the check box is selected, you can manually configure roaming parameters;
 - **FT-over-DS** – enabling the "Over the DS" mode;
 - **R0-key-holder-id** – unique key for this VAP, for example, a serial number;
 - **R1-key-holder-id** – MAC address of the VAP (can be viewed in the output of the ifconfig command);
 - **Mobility Domain** – group number within which roaming can be performed. Accepts values from 0 to 65535;
 - **Remote MAC:**
 - **MAC** – MAC address of the VAP interface of the remote access point. Maximum number – 256;
 - **Remote-R0-key-holder-id** – unique key, must match "R0-key-holder-id" on the VAP of the remote access point;
 - **Remote-R1-key-holder-id** – MAC address of the VAP on the remote access point;
 - **RRB-key-R0** – random key. Must not match "RRB-key-R1", but must match the "RRB-key-R1" of the remote access point. Key length – 16 characters;
 - **RRB-key-R1** – random key. Must not match "RRB-key-R0", but must match the "RRB-key-R0" of the remote access point. Key length – 16 characters.

RADIUS:

RADIUS	
Domain	root
IP Address of RADIUS Server	192.168.1.20
Port of RADIUS Server	1812
Password of RADIUS Server	 
Use Accounting through RADIUS	☒
Use Other Settings For Accounting	☒
IP Address of RADIUS Server for Accounting	192.168.1.20
Port of RADIUS Server for Accounting	1813
Password of RADIUS Server for Accounting	 
Use Periodic Accounting	☒
Accounting Interval	30

- *Domain* — user domain;
- *IP Address of RADIUS server* — RADIUS server address;
- *Port of RADIUS server* — RADIUS server port used for authentication and authorization;
- *Password of RADIUS server* — password for the RADIUS server used for authentication and authorization;
- *Use Accounting through RADIUS* — when the check box is selected, "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 for collecting accounting on the RADIUS server;
- *Password of RADIUS Server* — password for the RADIUS server used for authentication and authorization;
- *Use Periodic Accounting* — enable periodic sending of "Accounting" messages to the RADIUS server. The message sending interval can be set in the "Accounting Interval" field.

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

5.6.3 "MLO" submenu

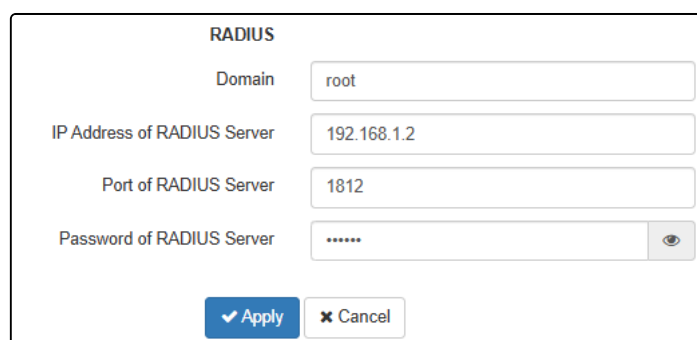
- ✓ MLO (Multi-Link Operation) is a key feature of the Wi-Fi 7 standard that allows a device (for example, a smartphone) to connect to an access point over multiple bands (2.4 GHz, 5 GHz, and 6 GHz) simultaneously.

- ✗ MLO group with index N uses VAPs with index N-1 across all radio bands; consequently, the settings for the corresponding VAPs become inaccessible when the MLO group is enabled.

Common Settings:

- *Enabled* – when the check box is selected, the virtual access point is enabled; otherwise, it is disabled;
- *SSID* – name of the virtual wireless network name;
- *Security Mode* – security mode of wireless network access:
 - *OWE (Opportunistic Wireless Encryption)* – encryption method that ensures the security of data transmitted over an insecure network.
Moreover, users are not required to take any additional steps or enter a password to connect to the network.
 - *WPA3* – encryption methods; selecting one of these methods will make the following setting available:
 - *WPA Key* – key/password required to connect to the virtual access point. The key must be between 8 and 63 characters long.
 - *WPA3-Enterprise* – wireless channel encryption mode in which the client is authorized on a centralized RADIUS server. To configure this security mode, the RADIUS server parameters must be specified (see below).
- *MFP* – management frame protection (available when using WPA2, WPA3, WPA2/WPA3, WPA2-Enterprise, WPA2/WPA3-Enterprise, or WPA3-Enterprise security modes; if other security modes are selected, MFP is set to *Not Required*, while for WPA3 or WPA3-Enterprise security modes, MFP is set to *Required*):
 - *Required* – protection is enabled, clients that do not support MFP cannot connect (the option value is set by default, and no other options are provided in this mode).

RADIUS:

A screenshot of a 'RADIUS' configuration dialog box. The dialog has a title bar 'RADIUS'. Inside, there are four input fields: 'Domain' with the value 'root', 'IP Address of RADIUS Server' with the value '192.168.1.2', 'Port of RADIUS Server' with the value '1812', and 'Password of RADIUS Server' with masked characters '.....' and a toggle icon. At the bottom, there are two buttons: '✓ Apply' and '✗ Cancel'.

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

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

5.7 "Network Settings" menu

5.7.1 "System Configuration" submenu

The screenshot displays the 'System Configuration' submenu within the 'Network Settings' tab. The interface includes a sidebar with 'System Configuration >' and 'Access' links. The main area contains the following configuration fields:

- Hostname:** A text input field with a placeholder 'XXXX-XXXX'.
- AP Location:** A text input field with the value 'root'.
- Protocol:** A dropdown menu currently set to 'Static'.
- Static IP:** A text input field with the value '192.168.1.10'.
- Netmask:** A text input field with the value '255.255.255.0'.
- Gateway:** A text input field with the placeholder 'XXXXXX:XXX:XXX'.
- Primary DNS Server:** A text input field with the placeholder 'XXXXXX:XXX:XXX'.
- Secondary DNS Server:** A text input field with the placeholder 'XXXXXX:XXX:XXX'.

At the bottom of the configuration area, there are two buttons: a blue 'Apply' button with a checkmark icon and a white 'Cancel' button with an 'X' icon.

- *Hostname* – network name of the device, specified as a string of 1–63 characters: Latin uppercase and lowercase letters, digits, hyphen "-" (the hyphen cannot be the last character in the name);
- *AP Location* – domain of the device tree node of the EMS management system in which the access point is located;
- *Protocol* – select protocol for connection of the device via Ethernet interface to service provider network:
 - *DHCP* – operation mode, when IP address, subnet mask, DNS server address, default gateway and other parameters required for operation are obtained from DHCP server automatically;
 - *Static* – operation mode, when IP address and all the necessary parameters for WAN interface are assigned statically. If "Static" is selected, the following parameters will be available to set:
 - *Static IP* – IP address of the device WAN interface in the provider network;
 - *Netmask* – external subnet mask;
 - *Gateway* – address, to which the packet is sent, if the route in routing table is not found for it.
- *Primary DNS server, Secondary DNS server* – IP addresses of DNS servers. If addresses of DNS servers are not automatically assigned via DHCP, set them manually.

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

5.7.2 "Access" submenu

In the "**Access**" submenu, access to the device via the web interface, Telnet, SSH, NETCONF can be configured.

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

✓ The ports for the HTTP and HTTPS protocols should not have the same value.

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

The screenshot displays the 'Access' configuration page within a web interface. The top navigation bar includes 'Monitoring', 'Radio', 'VAP', 'Network Settings' (selected), 'External Services', and 'System'. On the right, there is a language dropdown set to 'en' and a '(logout)' link. The left sidebar shows 'System Configuration' with 'Access >' selected. The main content area contains the following settings:

- WEB**: ☒ (checked)
- HTTP Port**:
- WEB-HTTPS**: ☒ (checked)
- HTTPS Port**:
- Telnet**: ☐ (unchecked)
- SSH**: ☒ (checked)
- NETCONF**: ☒ (checked)

At the bottom of the configuration area, there are two buttons: a blue '✓ Apply' button and a grey '✕ Cancel' button.

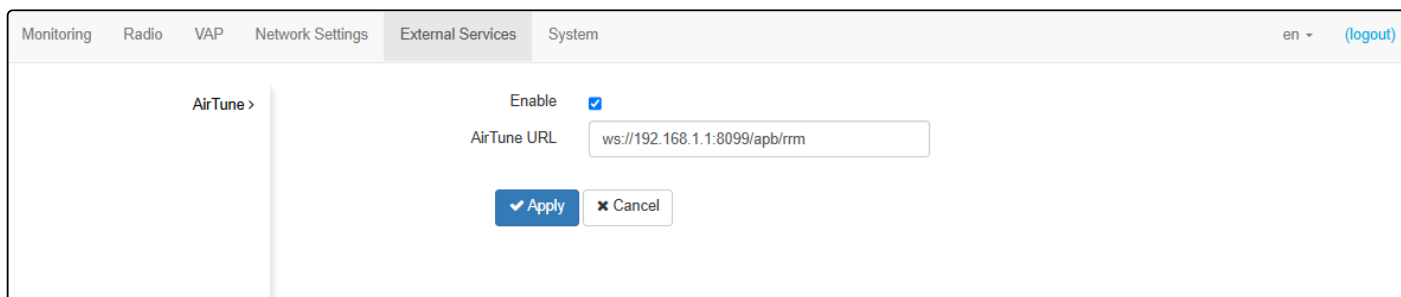
To apply a new configuration and save settings to non-volatile memory, click "Apply". Click "Cancel" to discard the changes.

5.8 "External Services" menu

5.8.1 "AirTune" submenu

The "**AirTune**" submenu is intended to enable and configure the AirTune service on the access point.

The AirTune service is used to optimize radio resources (Radio Resource Management) and to automatically configure seamless 802.11 k/r roaming.



The screenshot shows the web interface for configuring the AirTune service. At the top, there is a navigation bar with tabs: Monitoring, Radio, VAP, Network Settings, External Services (selected), and System. On the right of the navigation bar, there is a language dropdown set to 'en' and a '(logout)' link. Below the navigation bar, on the left, is a sidebar with the 'AirTune >' menu item. The main content area on the right contains the configuration options: an 'Enable' checkbox which is checked, and an 'AirTune URL' text input field containing the value 'ws://192.168.1.1:8099/apb/rrm'. At the bottom of the configuration area are two buttons: a blue '✓ Apply' button and a grey '✗ Cancel' button.

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

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

5.9 "System" menu

In the "**System**" menu, you can configure the system, time, and access to the device over various protocols, change the password, and update the device firmware.

5.9.1 "Device Firmware Upgrade" submenu

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

The screenshot shows the 'System' menu with the 'Device Firmware Upgrade' submenu selected. The submenu includes links for Configuration, Reboot, Password, Log, Date and Time, and Troubleshooting. The main content area displays the 'Active Version' and 'Backup Version' of the firmware, both showing '1.0.0 (stable)'. A 'Set Active' button is next to the 'Backup Version'. Below this, a message states: 'The latest firmware version is available at: <http://eltex-co.ru/support/downloads/>'. The 'Firmware Image' section has a 'Choose File' button and a 'No file chosen' label. A 'Start Upgrading' button is at the bottom.

- *Active Version* — installed firmware version, which is operating at the moment;
- *Backup version* — firmware version installed on the device that you can switch to without uploading a firmware file.
 - *Set active* — button that makes the backup firmware version active; a device reboot is required. The active firmware version then becomes the backup one.

Firmware upgrade

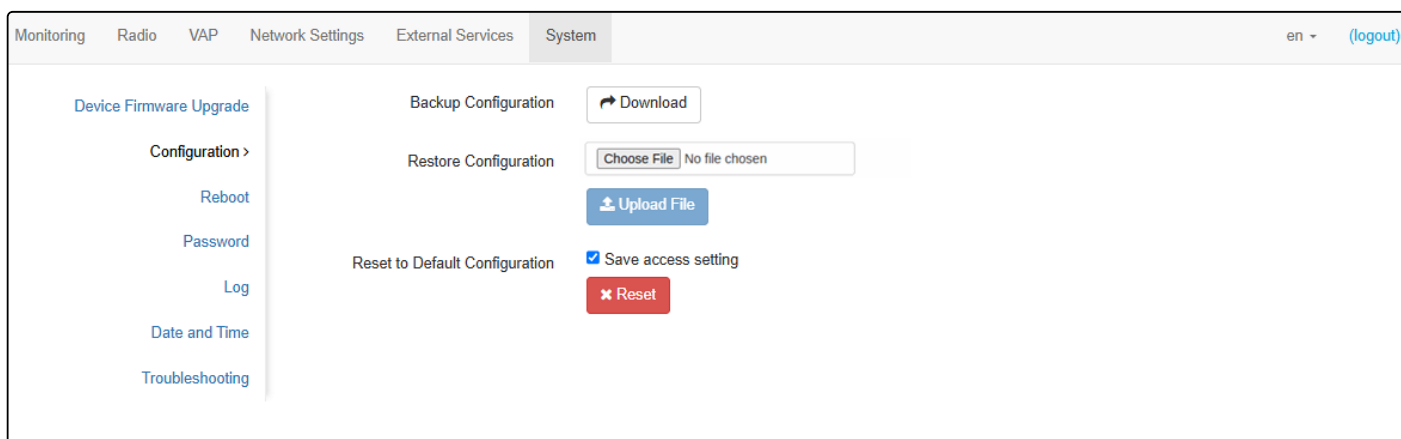
Download the firmware file from the <https://eltex.ru/download> website, selecting WEP-550K in the list of devices, and save it on your computer. After that, click "Choose File" in the *Firmware Image* field and specify the path to the firmware file in .tar.gz format.

To start the update process, click the "Start Upgrading" button. The update process will take several minutes (its current status will be shown on the page), after which the device will automatically reboot.

⚠ Do not disconnect the device from the power supply and do not reboot it during the firmware update process.

5.9.2 "Configuration" submenu

The **"Configuration"** submenu is used to save and restore the current configuration.



Download configuration

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

Restore Configuration

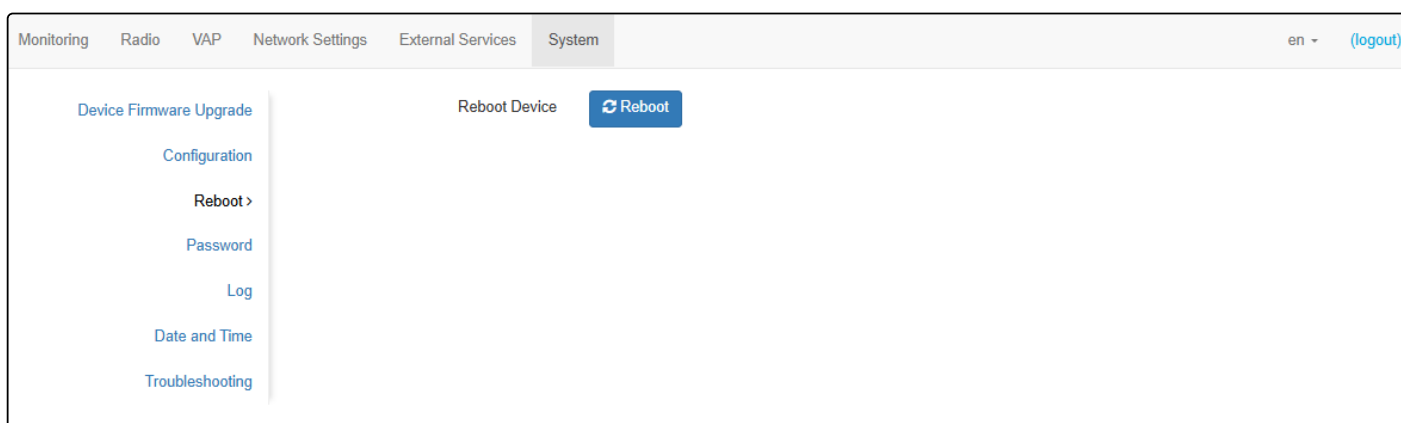
To load a configuration file saved on a local computer, the *"Restore Configuration"* item is used. To update the device configuration, click the "Choose file" button, specify the file (in .tar.gz format), and click the "Upload File" button. The uploaded configuration is applied automatically without rebooting the device.

Reset to Default Configuration

To reset all device settings to the standard factory defaults, click the "Reset" button. If the "Save access setting" check box is enabled, those configuration parameters that control access to the device (IP address configuration, Telnet/SSH/NETCONF/Web access settings) will be retained.

5.9.3 "Reboot" submenu

To reboot the device, click the "Reboot" button. The device restart process takes approximately 1.5 minutes.



5.9.4 "Password" submenu

When logging in via the web interface, the administrator (default password: **password**) has full access to the device: reading and writing of any settings, full monitoring of the device status.

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

5.9.5 "Log" submenu

The **"Log"** submenu is intended for configuring the output of various system debug messages to identify the causes of device operation problems.

- *Mode* – Syslog agent operating mode:
 - *Local File* – log information is saved to a local file and is available in the device web interface on the ["Monitoring/Events"](#);
 - *Server and File* – log information is sent to a remote Syslog server and saved to a local file.
- *Syslog Server Address* – IP address or domain name of the Syslog server;
- *Syslog Server Port* – port for incoming messages of the Syslog server (default – 514, acceptable values 1–65535);
- *File Size, KB* – maximum log file size (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.

5.9.6 "Date and Time" submenu

In the **"Date and Time"** submenu, the time can be configured manually or using the time synchronization protocol (NTP).

5.9.6.1 Manual

The screenshot shows the 'System' submenu with the 'Date and Time' configuration page. The left sidebar contains links: Device Firmware Upgrade, Configuration, Reboot, Password, Log, Date and Time > (active), and Troubleshooting. The main content area has a 'Mode' section with 'Manual' selected and 'NTP Server' unselected. Below this, the 'Date and Time device' is set to '10/16/2026 11:58:40' with an 'Edit' button. The 'Time Zone' is set to 'Moscow, Russia' in a dropdown menu. The 'Enable daylight saving time' checkbox is checked. Below this, the 'DST Start' and 'DST End' fields are each composed of three input boxes for day, month, and year, followed by 'in' and 'at' labels and two input boxes for hour and minute. All these fields currently show '(not selected)'. The 'DST Offset (minutes)' is set to '60'. At the bottom, there are 'Apply' and 'Cancel' buttons.

- *Date and Time device* — the date and time on the device at the moment. If correction is required, click the "Edit" button.
 - *Date, Time* — set the current date and time or click the "Set current date and time" button to set the device time from your PC.
- *Time Zone* — allows you to set the time zone according to the nearest city in your region from the given list;
- *Enable daylight saving time* — when the check box is selected, the transition between summer/winter time will be performed automatically in the specified time period:
 - *DST Start* — day and time when the transition to daylight saving time will be performed;
 - *DST End* — day and time when the transition to standard time will be performed;
 - *DST Offset (minutes)* — time period in minutes by which the time is shifted. Can take a value from 0 to 720 minutes.

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

5.9.6.2 NTP server

The screenshot shows the 'System' settings page with the 'NTP Server' tab selected. On the left is a sidebar menu with options: Device Firmware Upgrade, Configuration, Reboot, Password, Log, Date and Time >, and Troubleshooting. The main content area has a 'Mode' section with 'Manual' and 'NTP Server' (selected) radio buttons. Below this is the 'Date and Time device' showing '10/16/2026 11:58:56'. The 'NTP Server' is set to 'pool.ntp.org' in a dropdown. The 'Time Zone' is set to 'Moscow, Russia' in a dropdown. There is a checked checkbox for 'Enable daylight saving time'. Below this are fields for 'DST Start' and 'DST End', each with three dropdowns for day, month, and year, followed by 'in', 'at', and time fields (hours, minutes, seconds). The 'DST Offset (minutes)' is set to '60'. At the bottom are 'Apply' and 'Cancel' buttons.

- *Date and Time device* – the date and time on the device at the moment;
- *NTP Server* – IP address/domain name of the time synchronization server. You can set the address or select it from the existing list;
- *Time Zone* – allows you to set the time zone according to the nearest city in your region from the given list;
- *Enable daylight saving time* – when the check box is selected, the transition between summer/winter time will be performed automatically in the specified time period:
 - *DST Start* – day and time when the transition to daylight saving time will be performed;
 - *DST End* – day and time when the transition to standard time will be performed;
 - *DST Offset (minutes)* – the time period in minutes by which the time is shifted. Can take a value from 0 to 720 minutes.

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

5.9.7 "Troubleshooting" submenu

The screenshot shows the 'System' settings page with the 'Troubleshooting' submenu selected. The sidebar menu is the same as in the previous screenshot. The main content area shows 'Troubleshooting File' and a 'Download' button with a download icon.

Troubleshooting File

To download the archive *troubleshooting.tar.gz* from the device to a local computer, click the "Download" button.

6 Managing the device using the command line

- ✓ To display the available settings of a specific configuration section, enter the **show-config** command.
To view hints about what values a device configuration parameter can take, press the key combination (in English layout) **[Shift + ?]**.
To obtain a list of parameters available for editing in this configuration section, press the **Tab** key.
To save settings, enter the **save** command.
To go to the previous configuration section, enter the **exit** command.
To go to the root section, enter the **end** command.

6.1 Connection to the device

By default, the WEP-550K device is configured to obtain an IP address via DHCP. If this does not occur, you can connect to the device via the factory IP address.

- ✓ Factory IP address of the WEP-550K device: **192.168.1.10**, subnet mask: **255.255.255.0**.

Connection to the device is performed via SSH/Telnet:

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

6.2 Configuring network parameters

Configuring static network parameters of the access point

```
WEP-550K(root):/# configure
WEP-550K(config):/# interface
WEP-550K(config):/interface# br0
WEP-550K(config):/interface/br0# common
WEP-550K(config):/interface/br0/common# static-ip X.X.X.X (where X.X.X.X is the IP address of WEP-550K)
WEP-550K(config):/interface/br0/common# netmask X.X.X.X (where X.X.X.X is the subnet mask)
WEP-550K(config):/interface/br0/common# dns-server-1 X.X.X.X (where X.X.X.X is the IP address of DNS server No. 1)
WEP-550K(config):/interface/br0/common# dns-server-2 X.X.X.X (where X.X.X.X is the IP address of DNS server No. 2)
WEP-550K(config):/interface/br0/common# protocol static-ip (change operation mode from DHCP to Static-IP)
WEP-550K(config):/interface/br0/common# save (save settings)
```

Adding a static route:

```
WEP-550K(config):/interface/br0/common# exit
WEP-550K(config):/interface/br0# exit
WEP-550K(config):/interface# exit
WEP-550K(config):/# route
WEP-550K(config):/route# add default (where default is the route name)
WEP-550K(config):/route# default
WEP-550K(config):/route/default# destination X.X.X.X (where X.X.X.X is IP address of the destination network or node, for default route — 0.0.0.0)
WEP-550K(config):/route/default# netmask X.X.X.X (where X.X.X.X is destination network mask, for the default route — 0.0.0.0)
WEP-550K(config):/route/default# gateway X.X.X.X (where X.X.X.X is gateway IP address)
WEP-550K(config):/route/default# save (save settings)
```

Configuring network parameter reception via DHCP

```
WEP-550K(root):/# configure
WEP-550K(config):/# interface
WEP-550K(config):/interface# br0
WEP-550K(config):/interface/br0# common
WEP-550K(config):/interface/br0/common# protocol dhcp
WEP-550K(config):/interface/br0/common# save (save settings)
```

6.2.1 Configuring remote management

Configuring SSH

```
WEP-550K(root):/# configure  
WEP-550K(config):/# ssh  
WEP-550K(config):/ssh# enable true (remote access management via SSH. To disable, enter false. By default:  
true)  
WEP-550K(config):/ssh# port X (where X is the SSH server port. By default: 22)  
WEP-550K(config):/ssh# session-limit X (where X is the maximum number of SSH sessions. By default: 7)  
WEP-550K(config):/ssh# save (save settings)
```

Configuring Telnet

```
WEP-550K(root):/# configure  
WEP-550K(config):/# telnet  
WEP-550K(config):/telnet# enable true (remote access management via Telnet. To disable, enter false. By  
default: false)  
WEP-550K(config):/telnet# port X (where X is the port. By default: 23)  
WEP-550K(config):/telnet# session-limit X (where X is the maximum number of Telnet sessions. By default: 7)  
WEP-550K(config):/telnet# save (save settings)
```

6.3 Configuring Wi-Fi virtual access points (VAP)

When configuring a VAP, keep in mind that interface names in the 2.4 GHz band start with wlan0, in the 5 GHz band – wlan1, and in the 6 GHz band – wlan2.

✔ To connect devices supporting the IEEE 802.11be (Wi-Fi 7) standard, it is recommended to configure WPA2/WPA3, WPA3 or OWE security mode.

✔ For 6 GHz, only OWE, WPA3, WPA3-Enterprise security modes are available.

Table 10 – Commands for configuring security mode on VAP

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

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

6.3.1 Configuring VAP without Encryption

Creating a VAP without encryption with periodic sending of accounting to the RADIUS server

```

WEP-550K(root):/# configure
WEP-550K(config):/# interface
WEP-550K(config):/interface# wlan1-vap0
WEP-550K(config):/interface/wlan1-vap0# vap
WEP-550K(config):/interface/wlan1-vap0/vap# ssid 'SSID_WEP-550K_open' (change SSID name)
WEP-550K(config):/interface/wlan1-vap0/vap# ap-security
WEP-550K(config):/interface/wlan1-vap0/vap/ap-security# mode off (encryption mode off — without password)
WEP-550K(config):/interface/wlan1-vap0/vap/ap-security# exit
WEP-550K(config):/interface/wlan1-vap0/vap# radius
WEP-550K(config):/interface/wlan1-vap0/vap/radius# acct-enable true (enable sending of "Accounting"
messages to the RADIUS server. By default: false)
WEP-550K(config):/interface/wlan1-vap0/vap/radius# acct-address X.X.X.X (where X.X.X.X is the IP address of
the RADIUS server used for accounting)
WEP-550K(config):/interface/wlan1-vap0/vap/radius# acct-password secret (where secret is the password for
the RADIUS server used for accounting)
WEP-550K(config):/interface/wlan1-vap0/vap/radius# acct-periodic true (enable periodic sending of
"Accounting" messages to the RADIUS server. By default: false)
WEP-550K(config):/interface/wlan1-vap0/vap/radius# acct-interval 600 (interval of sending "Accounting"
messages to the RADIUS server)
WEP-550K(config):/interface/wlan1-vap0/vap/radius# exit
WEP-550K(config):/interface/wlan1-vap0/vap# exit
WEP-550K(config):/interface/wlan1-vap0# common
WEP-550K(config):/interface/wlan1-vap0/common# enabled true (enable the virtual access point)
WEP-550K(config):/interface/wlan1-vap0/common# save (save settings)

```

6.3.2 Configuring VAP with OWE Encryption

- ✓ Only Wi-Fi 6 and higher clients will be able to connect to a VAP with OWE security mode.

Creating a VAP with OWE Encryption

```

WEP-550K(root):/# configure
WEP-550K(config):/# interface
WEP-550K(config):/interface# wlan1-vap0
WEP-550K(config):/interface/wlan1-vap0# vap
WEP-550K(config):/interface/wlan1-vap0/vap# ssid 'SSID_WEP-550K_owe' (change SSID name)
WEP-550K(config):/interface/wlan1-vap0/vap# ap-security
WEP-550K(config):/interface/wlan1-vap0/vap/ap-security# mode OWE (encryption mode OWE — encrypted
connection without entering a password. In this mode, Wi-Fi 6 and higher clients will be able to connect)
WEP-550K(config):/interface/wlan1-vap0/vap/ap-security# exit
WEP-550K(config):/interface/wlan1-vap0/vap# radius
WEP-550K(config):/interface/wlan1-vap0/vap/radius# acct-enable true (enable sending of "Accounting"
messages to the RADIUS server. By default: false)
WEP-550K(config):/interface/wlan1-vap0/vap/radius# acct-address X.X.X.X (where X.X.X.X is the IP address of
the RADIUS server used for accounting)
WEP-550K(config):/interface/wlan1-vap0/vap/radius# acct-password secret (where secret is the password for
the RADIUS server used for accounting)
WEP-550K(config):/interface/wlan1-vap0/vap/radius# acct-periodic true (enable periodic sending of
"Accounting" messages to the RADIUS server. By default: false)
WEP-550K(config):/interface/wlan1-vap0/vap/radius# acct-interval 600 (interval of sending "Accounting"
messages to the RADIUS server)
WEP-550K(config):/interface/wlan1-vap0/vap/radius# exit
WEP-550K(config):/interface/wlan1-vap0/vap# exit
WEP-550K(config):/interface/wlan1-vap0# common
WEP-550K(config):/interface/wlan1-vap0/common# enabled true (enable the virtual access point)
WEP-550K(config):/interface/wlan1-vap0/common# save (save settings)

```

6.3.3 Configuring VAP with WPA-Personal security mode

Creating a VAP with WPA-Personal security mode with periodic sending of accounting to the RADIUS server

```

WEP-550K(root):/# configure
WEP-550K(config):/# interface
WEP-550K(config):/interface# wlan1-vap0
WEP-550K(config):/interface/wlan1-vap0# vap
WEP-550K(config):/interface/wlan1-vap0/vap# ssid 'SSID_WEP-550K_Wpa2' (change SSID name)
WEP-550K(config):/interface/wlan1-vap0/vap# ap-security
WEP-550K(config):/interface/wlan1-vap0/vap/ap-security# mode WPA_WPA2 (encryption mode — WPA/WPA2)
WEP-550K(config):/interface/wlan1-vap0/vap/ap-security# key-wpa password123 (key/password required to
connect to the virtual access point. The key length must be from 8 to 63 characters)
WEP-550K(config):/interface/wlan1-vap0/vap/ap-security# exit
WEP-550K(config):/interface/wlan1-vap0/vap# radius
WEP-550K(config):/interface/wlan1-vap0/vap/radius# acct-enable true (enable sending of "Accounting"
messages to the RADIUS server. By default: false)
WEP-550K(config):/interface/wlan1-vap0/vap/radius# acct-address X.X.X.X (where X.X.X.X is the IP address of
the RADIUS server used for accounting)
WEP-550K(config):/interface/wlan1-vap0/vap/radius# acct-password secret (where secret is the password for
the RADIUS server used for accounting)
WEP-550K(config):/interface/wlan1-vap0/vap/radius# acct-periodic true (enable periodic sending of
"Accounting" messages to the RADIUS server. By default: false)
WEP-550K(config):/interface/wlan1-vap0/vap/radius# acct-interval 600 (interval of sending "Accounting"
messages to the RADIUS server)
WEP-550K(config):/interface/wlan1-vap0/vap/radius# exit
WEP-550K(config):/interface/wlan1-vap0/vap# exit
WEP-550K(config):/interface/wlan1-vap0# common
WEP-550K(config):/interface/wlan1-vap0/common# enabled true (enable the virtual access point)
WEP-550K(config):/interface/wlan1-vap0/common# save (save settings)

```

6.3.4 Configuring VAP with Enterprise authorization

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

```

WEP-550K(root):/# configure
WEP-550K(config):/# interface
WEP-550K(config):/interface# wlan1-vap0
WEP-550K(config):/interface/wlan1-vap0# vap
WEP-550K(config):/interface/wlan1-vap0/vap# ssid 'SSID_WEP-550K_enterprise' (change SSID name)
WEP-550K(config):/interface/wlan1-vap0/vap# ap-security
WEP-550K(config):/interface/wlan1-vap0/vap/ap-security# mode WPA_WPA2_1X (encryption mode — WPA/
WPA2-Enterprise)
WEP-550K(config):/interface/wlan1-vap0/vap/ap-security# exit
WEP-550K(config):/interface/wlan1-vap0/vap# radius
WEP-550K(config):/interface/wlan1-vap0/vap/radius# domain root (where root is the user domain)
WEP-550K(config):/interface/wlan1-vap0/vap/radius# auth-address X.X.X.X (where X.X.X.X is the IP address of
the RADIUS server)
WEP-550K(config):/interface/wlan1-vap0/vap/radius# auth-port X (where X is the RADIUS server port used for
authentication and authorization. By default: 1812)
WEP-550K(config):/interface/wlan1-vap0/vap/radius# auth-password secret (where secret is the password for
the RADIUS server used for authentication and authorization)
WEP-550K(config):/interface/wlan1-vap0/vap/radius# acct-enable true (enable sending of "Accounting"
messages to the RADIUS server. By default: false)
WEP-550K(config):/interface/wlan1-vap0/vap/radius# acct-address X.X.X.X (where X.X.X.X is the IP address of
the RADIUS server used for accounting)
WEP-550K(config):/interface/wlan1-vap0/vap/radius# acct-password secret (where secret is the password for
the RADIUS server used for accounting)
WEP-550K(config):/interface/wlan1-vap0/vap/radius# acct-periodic true (enable periodic sending of
"Accounting" messages to the RADIUS server. By default: false)
WEP-550K(config):/interface/wlan1-vap0/vap/radius# acct-interval 600 (interval of sending "Accounting"
messages to the RADIUS server)
WEP-550K(config):/interface/wlan1-vap0/vap/radius# exit
WEP-550K(config):/interface/wlan1-vap0/vap# exit
WEP-550K(config):/interface/wlan1-vap0# common
WEP-550K(config):/interface/wlan1-vap0/common# enabled true (enable the virtual access point)
WEP-550K(config):/interface/wlan1-vap0/common# save (save settings)

```

6.3.5 Configuring VAP with external Captive Portal

Commands to configure the external Captive Portal

```

WEP-550K(root):/# configure
WEP-550K(config):/# interface
WEP-550K(config):/interface# wlan1-vap0
WEP-550K(config):/interface/wlan1-vap0# vap
WEP-550K(config):/interface/wlan1-vap0/vap# vlan-id X (where X is the VLAN-ID on the VAP)
WEP-550K(config):/interface/wlan1-vap0/vap# ap-security
WEP-550K(config):/interface/wlan1-vap0/vap/ap-security# mode off (encryption mode off — without password)
WEP-550K(config):/interface/wlan1-vap0/vap/ap-security# exit
WEP-550K(config):/interface/wlan1-vap0/vap# ssid 'Portal_WEP-550K' (change SSID name)
WEP-550K(config):/interface/wlan1-vap0/vap# captive-portal
WEP-550K(config):/interface/wlan1-vap0/vap/captive-portal# verification-mode external-portal (enable external Captive Portal support. By default: portal)
WEP-550K(config):/interface/wlan1-vap0/vap/captive-portal# scenarios
WEP-550K(config):/interface/wlan1-vap0/vap/captive-portal/scenarios# scenario-redirect
WEP-550K(config):/interface/wlan1-vap0/vap/captive-portal/scenarios/scenario-redirect# redirect-url "https://X.X.X.X/<NAS_ID>/?switch_url=<SWITCH_URL>&ap_mac=<AP_MAC>&client_mac=<CLIENT_MAC>&wlan=<SSID>&original-url=<ORIGINAL_URL>&nas-ip=<NAS_IP>&ap_location=<AP_LOCATION>&nas_id=<NAS_ID>" (specify the URL of the external virtual portal according to the table 11)
WEP-550K(config):/interface/wlan1-vap0/vap/captive-portal/scenarios/scenario-redirect# exit
WEP-550K(config):/interface/wlan1-vap0/vap/captive-portal/scenarios# exit
WEP-550K(config):/interface/wlan1-vap0/vap/captive-portal# enabled true (enable the captive portal functionality)
WEP-550K(config):/interface/wlan1-vap0/vap/captive-portal# exit
WEP-550K(config):/interface/wlan1-vap0/vap# radius
WEP-550K(config):/interface/wlan1-vap0/vap/radius# auth-address X.X.X.X (where X.X.X.X is the IP address of the RADIUS server used for authorization)
WEP-550K(config):/interface/wlan1-vap0/vap/radius# auth-password secret (where secret is the password for the RADIUS server used for authorization)
WEP-550K(config):/interface/wlan1-vap0/vap/radius# exit
WEP-550K(config):/interface/wlan1-vap0/vap# save (save settings)

```

Additional commands to configure the external Captive Portal

```

WEP-550K(config):/interface/wlan1-vap0/vap/captive-portal# preauth-filter-mode acl
(parameter that determines how traffic from unauthorized clients will be filtered. Possible values: acl, white-list. By default: white-list)
WEP-550K(config):/interface/wlan1-vap0/vap/captive-portal# http-auth false (disable authorization via http. By default: true)
WEP-550K(config):/interface/wlan1-vap0/vap/captive-portal# ipv4-acl ipv4_list (where ipv4_list — name list rules ipv4-acl)
WEP-550K(config):/interface/wlan1-vap0/vap/captive-portal# url-acl url_list (where url_list — name list rules url-acl)
WEP-550K(config):/interface/wlan1-vap0/vap/captive-portal# filter-dns-by-acl true (enable DNS request filtering by preauth-acl rules. By default: false)
WEP-550K(config):/interface/wlan1-vap0/vap/captive-portal# client-mac-format XX-XX-XX-XX-XX-XX (where XX-XX-XX-XX-XX-XX is the client MAC address format that will be substituted instead of <AP_MAC> in requests to the external portal. Possible values: XX-XX-XX-XX-XX-XX, XX:XX:XX:XX:XX:XX, XXXXXXXXXXXX, xx-xx-xx-xx-xx-xx, xx:xx:xx:xx:xx:xx, xxxxxxxxxxxx. By default: xxxxxxxxxxxx)
WEP-550K(config):/interface/wlan1-vap0/vap/captive-portal# nas-id-format XX-XX-XX-XX-XX-XX (where XX-XX-XX-XX-XX-XX is the access point MAC address format that will be substituted instead of <NAS_ID> in requests to the external portal. Possible values: XX-XX-XX-XX-XX-XX, XX:XX:XX:XX:XX:XX, XXXXXXXXXXXX, xx-xx-xx-xx-xx-xx, xx:xx:xx:xx:xx:xx, xxxxxxxxxxxx. By default: xxxxxxxxxxxx)
WEP-550K(config):/interface/wlan1-vap0/vap/captive-portal# disconnect-on-reject true (parameter responsible for disconnecting the client after receiving Access-Reject. To disable, enter false)
WEP-550K(config):/interface/wlan1-vap0/vap/captive-portal# exit
WEP-550K(config):/interface/wlan1-vap0/vap# radius
WEP-550K(config):/interface/wlan1-vap0/vap/radius# use-macaddr-as-password true (transmit the client MAC address as the password in RADIUS requests. By default: false)
WEP-550K(config):/interface/wlan1-vap0/vap/radius# macaddr-format XX-XX-XX-XX-XX-XX (where XX-XX-XX-XX-XX-XX is the client MAC address format to be used in RADIUS requests. This feature works only when use-macaddr-as-password = true. Possible values: XX-XX-XX-XX-XX-XX, XX:XX:XX:XX:XX:XX, XXXXXXXXXXXX, xx-xx-xx-xx-xx-xx, xx:xx:xx:xx:xx:xx, xxxxxxxxxxxx. By default: xxxxxxxxxxxx)
WEP-550K(config):/interface/wlan1-vap0/vap/radius# exit
WEP-550K(config):/interface/wlan1-vap0/vap# save (save settings)

```

✓ To get information about the interaction algorithm with the external portal, see the [scheme](#).

Table 11 — Configuring the URL template for external captive portal authorization

Parameter	Description
<NAS_ID>	NAS ID set on VAP or in system. If neither of these parameters is set, then the MAC address of the access point in the "nas-id-format" format will be used as the NAS ID in RADIUS and HTTP(S) packets
<NAS_IP>	IP address of the access point
<SWITCH_URL>	Domain name displayed to the client upon redirection
<AP_MAC>	MAC address of the access point
<CLIENT_MAC>	MAC address of the client
<SSID>	SSID
<ORIGINAL_URL>	URL initially requested by the client
<AP_LOCATION>	AP location of the access point

6.3.6 Configuring an additional RADIUS server on VAP

✓ This function is available only for captive portal and Enterprise authorization modes.

Commands for configuring an additional RADIUS server on a VAP

```
WEP-550K(root):/# configure
WEP-550K(config):/# interface
WEP-550K(config):/interface# wlan1-vap0
WEP-550K(config):/interface/wlan1-vap0# vap
WEP-550K(config):/interface/wlan1-vap0/vap# radius (configure the main RADIUS server)
WEP-550K(config):/interface/wlan1-vap0/vap/radius# backup (configure an additional RADIUS server)
WEP-550K(config):/interface/wlan1-vap0/vap/radius/backup# add <IP address of the additional RADIUS server in the configuration> (create an additional RADIUS server configuration section. Maximum number: 4)
WEP-550K(config):/interface/wlan1-vap0/vap/radius/backup# X.X.X.X (where X.X.X.X is the IP address of the additional RADIUS server in the configuration)
WEP-550K(config):/interface/wlan1-vap0/vap/radius/backup/X.X.X.X# auth-address X.X.X.X (where X.X.X.X is the IP address of the RADIUS server)
WEP-550K(config):/interface/wlan1-vap0/vap/radius/backup/X.X.X.X# auth-port X (where X is the RADIUS server port used for authentication and authorization. Default: 1812)
WEP-550K(config):/interface/wlan1-vap0/vap/radius/backup/X.X.X.X# auth-password secret (where secret is the password for the RADIUS server used for authentication and authorization)
WEP-550K(config):/interface/wlan1-vap0/vap/radius/backup/X.X.X.X# acct-address X.X.X.X (where X.X.X.X is the IP address of the RADIUS server used for accounting)
WEP-550K(config):/interface/wlan1-vap0/vap/radius/backup/X.X.X.X# acct-port X (where X is the RADIUS server port used for accounting. Default: 1813)
WEP-550K(config):/interface/wlan1-vap0/vap/radius/backup/X.X.X.X# acct-password secret (where secret is the password for the RADIUS server used for accounting)
WEP-550K(config):/interface/wlan1-vap0/vap/radius/backup/X.X.X.X# order 1 (where order is the RADIUS server priority. If the priority was not explicitly specified, it is considered to be 0. In this case, the server selection order will correspond to the order in which the RADIUS server was added to the configuration)
WEP-550K(config):/interface/wlan1-vap0/vap/radius/backup/X.X.X.X# save (save settings)
```

6.3.7 Advanced VAP settings

Assigning a VLAN ID on a VAP

```
WEP-550K(config):/interface/wlan1-vap0/vap# vlan-id X (where X is the VLAN ID number on the VAP)
```

Enabling Band Steer mode

```
WEP-550K(config):/interface/wlan1-vap0/vap# band-steer-mode true (enable the Band Steer mode. To disable, enter false)
```

Enabling MFP mode (802.11W)

WEP-550K(config):/interface/wlan1-vap0/vap/ap-security# **mfp required** (enable protection of management frames. **required** — MFP support is required from the client, clients without MFP will not be able to connect. **capable** — compatible with MFP, clients without MFP support can connect. To disable, enter **off**)

Enabling TLS during authorization

WEP-550K(config):/interface/wlan1-vap0/vap/radius# **tls-enable true** (use TLS during authorization. To disable, enter **false**)

Enabling hidden SSID

WEP-550K(config):/interface/wlan1-vap0/vap# **hidden true** (enable hidden SSID. To disable, enter **false**)

Enabling client isolation on a VAP

WEP-550K(config):/interface/wlan1-vap0/vap# **station-isolation true** (enable traffic isolation between clients within a single VAP. To disable, enter **false**)

Limiting the number of clients on a VAP

WEP-550K(config):/interface/wlan1-vap0/vap# **sta-limit X** (where X is the maximum allowed number of clients that can connect to the virtual network)

Enabling Minimal Signal

WEP-550K(config):/interface/wlan1-vap0/vap# **check-signal-enable true** (enable the use of the Minimal Signal feature. To disable, enter **false**)

WEP-550K(config):/interface/wlan1-vap0/vap# **min-signal X** (where X is the RSSI threshold value at which the access point will start disconnecting clients from the VAP. The parameter can take values from -100 to -1)

WEP-550K(config):/interface/wlan1-vap0/vap# **check-signal-timeout X** (where X is the time period in seconds after which a decision is made to disconnect the client device from the virtual network)

WEP-550K(config):/interface/wlan1-vap0/vap# **save** (save settings)

Enabling subscriber traffic transmission outside a GRE tunnel

WEP-550K(config):/interface/wlan1-vap0/vap# **local-switching true** (enable subscriber traffic transmission outside a GRE tunnel. To disable, enter **false**. Disabled by default)

Configuring MAC-based access control via a RADIUS server

```

WEP-550K(config):/interface/wlan1-vap0/vap# acl
WEP-550K(config):/interface/wlan1-vap0/vap/acl# mode radius (select the radius mode — checking MAC
addresses via the RADIUS server)
WEP-550K(config):/interface/wlan1-vap0/vap/acl# policy allow (select the policy. Possible values: allow —
allow connection only for those clients that were approved by the RADIUS server; deny — deny connection for
clients that were approved by the RADIUS server. Default value: deny)
WEP-550K(config):/interface/wlan1-vap0/vap/acl# enable true (enable MAC-based access control via the
RADIUS server. To disable, enter false)
WEP-550K(config):/interface/wlan1-vap0/vap/acl# exit
WEP-550K(config):/interface/wlan1-vap0/vap# radius
WEP-550K(config):/interface/wlan1-vap0/vap/radius# domain root (where root is the user domain)
WEP-550K(config):/interface/wlan1-vap0/vap/radius# auth-address X.X.X.X (where X.X.X.X is the IP address of
the RADIUS server)
WEP-550K(config):/interface/wlan1-vap0/vap/radius# auth-port X (where X is the RADIUS server port used for
authentication and authorization. Default value: 1812)
WEP-550K(config):/interface/wlan1-vap0/vap/radius# auth-password secret (where secret is the password for
the RADIUS server used for authentication and authorization)
WEP-550K(config):/interface/wlan1-vap0/vap/radius# acct-enable true (enable sending of "Accounting"
messages to the RADIUS server. Default value: false)
WEP-550K(config):/interface/wlan1-vap0/vap/radius# acct-address X.X.X.X (where X.X.X.X is the IP address of
the RADIUS server used for accounting)
WEP-550K(config):/interface/wlan1-vap0/vap/radius# acct-password secret (where secret is the password for
the RADIUS server used for accounting)
WEP-550K(config):/interface/wlan1-vap0/vap/radius# acct-periodic true (enable periodic sending of
"Accounting" messages to the RADIUS server. Default value: false)
WEP-550K(config):/interface/wlan1-vap0/vap/radius# acct-interval 600 (interval of sending "Accounting"
messages to the RADIUS server)
WEP-550K(config):/interface/wlan1-vap0/vap/radius# exit
WEP-550K(config):/interface/wlan1-vap0/vap# save (save settings)

```

Configuring 802.11r

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

802.11r roaming is possible only between VAPs with WPA2/WPA3-Personal and WPA2/WPA3-Enterprise security modes.

For instructions on configuring a VAP with WPA2-Personal security mode and others, see the section [Configuring VAP with WPA-Personal security mode](#).

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

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

Configuring 802.11r on AP1

```
WEP-550K(config):/interface/wlan1-vap0/vap/ft-config# enabled false
WEP-550K(config):/interface/wlan1-vap0/vap/ft-config# r1-key-holder-id E8:28:C1:FC:D6:80 (VAP MAC
address. Can be viewed in the output of the ifconfig command)
WEP-550K(config):/interface/wlan1-vap0/vap/ft-config# r0-key-holder-id 12345 (unique key for this VAP)
WEP-550K(config):/interface/wlan1-vap0/vap/ft-config# mobility-domain 100 (domain must match on
remote VAPs)
WEP-550K(config):/interface/wlan1-vap0/vap/ft-config# mac
WEP-550K(config):/interface/wlan1-vap0/vap/ft-config/mac# add E4:5A:D4:E2:C4:B0 (MAC address of the VAP
interface of the remote access point — AP2)
WEP-550K(config):/interface/wlan1-vap0/vap/ft-config/mac# E4:5A:D4:E2:C4:B0
WEP-550K(config):/interface/wlan1-vap0/vap/ft-config/mac/E4:5A:D4:E2:C4:B0# r0-kh-id 23456 (unique key of
the remote VAP of access point AP2 — r0-key-holder-id)
WEP-550K(config):/interface/wlan1-vap0/vap/ft-config/mac/E4:5A:D4:E2:C4:B0# r1-kh-id E4:5A:D4:E2:C4:B0
(MAC address of the remote VAP on AP2)
WEP-550K(config):/interface/wlan1-vap0/vap/ft-config/mac/E4:5A:D4:E2:C4:B0# r0-kh-key 0102030405060708
(random key. Must not match the r1-kh-key of AP1, but must match the r1-kh-key of the remote AP2)
WEP-550K(config):/interface/wlan1-vap0/vap/ft-config/mac/E4:5A:D4:E2:C4:B0# r1-kh-key 0001020304050607
(random key. Must not match the r0-kh-key of AP1, but must match the r0-kh-key of the remote AP2)
WEP-550K(config):/interface/wlan1-vap0/vap/ft-config/mac/E4:5A:D4:E2:C4:B0# exit
WEP-550K(config):/interface/wlan1-vap0/vap/ft-config/mac# exit
WEP-550K(config):/interface/wlan1-vap0/vap/ft-config# enabled true (enable access point operation over the
802.11r protocol)
WEP-550K(config):/interface/wlan1-vap0/vap/ft-config# save (save settings)
```

Configuring 802.11r on AP2

```

WEP-550K(config):/interface/wlan1-vap0/vap/ft-config# enabled false
WEP-550K(config):/interface/wlan1-vap0/vap/ft-config# r1-key-holder-id E4:5A:D4:E2:C4:B0 (VAP MAC
address. Can be viewed in the output of the ifconfig command)
WEP-550K(config):/interface/wlan1-vap0/vap/ft-config# r0-key-holder-id 23456 (unique key for this VAP)
WEP-550K(config):/interface/wlan1-vap0/vap/ft-config# mobility-domain 100 (domain must match on
remote VAPs)
WEP-550K(config):/interface/wlan1-vap0/vap/ft-config# mac
WEP-550K(config):/interface/wlan1-vap0/vap/ft-config/mac# add E8:28:C1:FC:D6:80 (MAC address of the VAP
interface of the remote access point — AP1)
WEP-550K(config):/interface/wlan1-vap0/vap/ft-config/mac# E8:28:C1:FC:D6:80
WEP-550K(config):/interface/wlan1-vap0/vap/ft-config/mac/E8:28:C1:FC:D6:80# r0-kh-id 12345 (unique key of
the remote VAP of access point AP1 — r0-key-holder-id)
WEP-550K(config):/interface/wlan1-vap0/vap/ft-config/mac/E8:28:C1:FC:D6:80# r1-kh-id E8:28:C1:FC:D6:80
(MAC address of remote VAP on AP1)
WEP-550K(config):/interface/wlan1-vap0/vap/ft-config/mac/E8:28:C1:FC:D6:80# r0-kh-key 0001020304050607
(random key. Must not match the r1-kh-key of AP2, but must match the r1-kh-key of the remote AP1)
WEP-550K(config):/interface/wlan1-vap0/vap/ft-config/mac/E8:28:C1:FC:D6:80# r1-kh-key 0102030405060708
(random key. Must not match the r0-kh-key of AP2, but must match the r0-kh-key of the remote AP1)
WEP-550K(config):/interface/wlan1-vap0/vap/ft-config/mac/E8:28:C1:FC:D6:80# exit
WEP-550K(config):/interface/wlan1-vap0/vap/ft-config/mac# exit
WEP-550K(config):/interface/wlan1-vap0/vap/ft-config# enabled true (enable access point operation over the
802.11r protocol)
WEP-550K(config):/interface/wlan1-vap0/vap/ft-config# save (save settings)

```

Configuring 802.11k

Roaming over the 802.11k protocol can be organized between any networks (open/encrypted). If the access point is configured for 802.11k operation, then when a client connects, the access point sends it a list of "friendly" access points to which the client can switch during roaming. The list contains information about the MAC addresses of the access points and the channels on which they operate.

Using 802.11k reduces the time spent searching for another network while roaming, since the client does not need to scan the channels on which there are no target access points available for switching.

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

Below is an example of configuring 802.11k on an access point — compiling a list of "friendly" access points.

Configuring 802.11k

```
WEP-550K(config):/interface/wlan1-vap0/vap/w80211kv-config# enabled false
WEP-550K(config):/interface/wlan1-vap0/vap/w80211kv-config# mac
WEP-550K(config):/interface/wlan1-vap0/vap/w80211kv-config/mac# add E8:28:C1:FC:D6:90 (where
E8:28:C1:FC:D6:90 is the MAC address of the "friendly" access point)
WEP-550K(config):/interface/wlan1-vap0/vap/w80211kv-config/mac# E8:28:C1:FC:D6:90
WEP-550K(config):/interface/wlan1-vap0/vap/w80211kv-config/mac/E8:28:C1:FC:D6:90# channel 132 (where
132 is the channel on which the access point with MAC address E8:28:C1:FC:D6:90 operates)
WEP-550K(config):/interface/wlan1-vap0/vap/w80211kv-config/mac/E8:28:C1:FC:D6:90# exit
WEP-550K(config):/interface/wlan1-vap0/vap/w80211kv-config/mac# add E8:28:C1:FC:D6:70 (where
E8:28:C1:FC:D6:70 is the MAC address of the "friendly" access point)
WEP-550K(config):/interface/wlan1-vap0/vap/w80211kv-config/mac# E8:28:C1:FC:D6:70
WEP-550K(config):/interface/wlan1-vap0/vap/w80211kv-config/mac/E8:28:C1:FC:D6:70# channel 36 (where 36
is the channel on which the access point with MAC address E8:28:C1:FC:D6:70 operates)
WEP-550K(config):/interface/wlan1-vap0/vap/w80211kv-config/mac/E8:28:C1:FC:D6:70# exit
WEP-550K(config):/interface/wlan1-vap0/vap/w80211kv-config/mac# exit
WEP-550K(config):/interface/wlan1-vap0/vap/w80211kv-config# enabled true (enable access point operation
over the 802.11k protocol)
WEP-550K(config):/interface/wlan1-vap0/vap/w80211kv-config# save (save settings)
```

Configuring 802.11v

Roaming over the 802.11v protocol can be organized between any networks (open/encrypted). If the access point is configured for 802.11v operation, then during its operation the device sends a special packet (BSS Transition) toward the client upon command from the administrator/controller (AirTune) with a recommendation for the client to roam. Whether the client device follows the access point's advice or not cannot be guaranteed, since ultimately the decision to switch to another access point is made by the client side. In combination with the 802.11k standard, the handover recommendation message also conveys to the client a list of access points recommended for roaming, indicating the channel on which each access point operates and the standard it uses (IEEE 802.11n/ac/ax). After that, the client analyzes the radio environment and makes a decision depending on the signal level, channel loading, and configuration of the remote access point.

This type of roaming is available only for client devices that support 802.11v.

Configuring 802.11v

```
WEP-550K(config):/interface/wlan1-vap0/vap/w80211kv-config# enabled true (enable access point operation over the 802.11k/v protocol)
```

```
WEP-550K(config):/interface/wlan1-vap0/vap/w80211kv-config# save (save settings)
```

6.4 Configuring MLO

- ✓ MLO group uses one VAP from each band (2.4, 5 and 6 GHz), the number of the used VAP being N-1, where N is the group number. For example MLO group 4 uses the following VAPs: wlan0-vap3, wlan1-vap3 and wlan2-vap3.

When an MLO group is enabled, settings of the corresponding VAP will be ignored.

6.4.1 Configuring MLO Group with OWE

Creating an MLO group with OWE encryption mode

```
WEP-550K(root):/# configure
WEP-550K(config):/# mlo
WEP-550K(config):/mlo# mlo-group
WEP-550K(config):/mlo/mlo-group# 1
WEP-550K(config):/mlo/mlo-group/1# ssid SSID_WEP-550K_MLO_owe (change SSID name)
WEP-550K(config):/mlo/mlo-group/1# ap-security
WEP-550K(config):/mlo/mlo-group/1/ap-security# mode OWE (encryption mode — OWE)
WEP-550K(config):/mlo/mlo-group/1/ap-security# exit
WEP-550K(config):/mlo/mlo-group/1# enabled true (enable MLO group)
WEP-550K(config):/mlo/mlo-group/1# save (save settings)
```

6.4.2 Configuring MLO Group with WPA-Personal security mode

Creating an MLO group with WPA3-Personal security mode

```

WEP-550K(root):/# configure
WEP-550K(config):/# mlo
WEP-550K(config):/mlo# mlo-group
WEP-550K(config):/mlo/mlo-group# 1
WEP-550K(config):/mlo/mlo-group/1# ssid SSID_WEP-550K_MLO_Wpa3 (change SSID name)
WEP-550K(config):/mlo/mlo-group/1# ap-security
WEP-550K(config):/mlo/mlo-group/1/ap-security# mode WPA3 (encryption mode — WPA3)
WEP-550K(config):/mlo/mlo-group/1/ap-security# key-wpa password123 (key/password, required to connect
to the virtual access point. The key length must be from 8 to 63 characters)
WEP-550K(config):/mlo/mlo-group/1/ap-security# exit
WEP-550K(config):/mlo/mlo-group/1# enabled true (enable MLO group)
WEP-550K(config):/mlo/mlo-group/1# save (save settings)

```

6.4.3 Configuring MLO Group with Enterprise authorization

Creating an MLO group with WPA3-Enterprise security mode

```

WEP-550K(root):/# configure
WEP-550K(config):/# mlo
WEP-550K(config):/mlo# mlo-group
WEP-550K(config):/mlo/mlo-group# 1
WEP-550K(config):/mlo/mlo-group/1# ssid SSID_WEP-550K_MLO_Wpa3E (change SSID name)
WEP-550K(config):/mlo/mlo-group/1# ap-security
WEP-550K(config):/mlo/mlo-group/1/ap-security# mode WPA3_1X (encryption mode — WPA3-Enterprise)
WEP-550K(config):/mlo/mlo-group/1/ap-security# exit
WEP-550K(config):/mlo/mlo-group/1# radius
WEP-550K(config):/mlo/mlo-group/1/radius# auth-address X.X.X.X (where X.X.X.X is the IP address of the
RADIUS server)
WEP-550K(config):/mlo/mlo-group/1/radius# auth-port X (where X is the port of the RADIUS server, which is
used for authentication and authorization. By default: 1812)
WEP-550K(config):/mlo/mlo-group/1/radius# auth-password secret (where secret is the password for the
RADIUS server used for authentication and authorization)
WEP-550K(config):/mlo/mlo-group/1/radius# exit
WEP-550K(config):/mlo/mlo-group/1# enabled true (enable MLO group)
WEP-550K(config):/mlo/mlo-group/1# save

```

6.5 Configuring AirTune

Configuring AirTune

```
WEP-550K(config):/# airtune
WEP-550K(config):/airtune# airtune_service_url ws://192.168.1.20:8099/apb/rrm (where 192.168.1.20 is the
IP address of the server where the AirTune service is set)
WEP-550K(config):/airtune# enabled true (enable interaction with the AirTune service. To disable, enter false)
WEP-550K(config):/airtune# save (save settings)
```

To enable automatic 802.11r configuration via the AirTune service on the access point, enable the 802.11r function. To do this, perform the following settings:

Configuring 802.11r via AirTune

```
WEP-550K(config):/interface/wlan1-vap0/vap/ft-config# enabled true (enable access point operation via
protocol 802.11r)
WEP-550K(config):/interface/wlan1-vap0/vap/ft-config# save (save settings)
```

To enable automatic 802.11k/v configuration via the AirTune service on the access point, enable the 802.11k/v function on the SSID. To do this, perform the following settings:

Configuring 802.11k/v via AirTune

```
WEP-550K(config):/interface/wlan1-vap0/vap/w80211kv-config# enabled true (enable support for protocol
802.11k/v on the virtual access point)
WEP-550K(config):/interface/wlan1-vap0/vap/w80211kv-config# save (save settings)
```

The configuration of the AirTune service is described in the SoftWLC controller documentation.

6.6 Radio settings

By default, Radio uses automatic operating channel selection. To set the channel manually or change the power, use the following commands:

Changing the working channel and power of the radio interface

```
WEP-550K(root):/# configure
WEP-550K(config):/# interface
WEP-550K(config):/interface# wlan0
WEP-550K(config):/interface/wlan0# wlan
WEP-550K(config):/interface/wlan0/wlan# radio
WEP-550K(config):/interface/wlan0/wlan/radio# channel X (where X is the number of the static channel on
which the access point will operate)
WEP-550K(config):/interface/wlan0/wlan/radio# auto-channel false (disable automatic channel selection. To
enable, enter true)
WEP-550K(config):/interface/wlan0/wlan/radio# use-limit-channels false (disable the use of the limited
channel list. To enable, enter true)
WEP-550K(config):/interface/wlan0/wlan/radio# bandwidth X (where X is the channel width. The parameter can
take the following values: for Radio 1: 20, 40; Radio 2: 20, 40, 80)
WEP-550K(config):/interface/wlan0/wlan/radio# tx-power X (where X is the power level in dBm. The parameter
can take the following values: for Radio 1: 0–16 dBm; for Radio 2: 0–19 dBm)
WEP-550K(config):/interface/wlan0/wlan/radio# save (save settings)
```

✓ Lists of available channels

The following channels are available for Radio 2.4 GHz:

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

The following channels are available for Radio 5 GHz:

- when the channel width is 20 MHz: 36, 40, 44, 48, 52, 56, 60, 64, 132, 136, 140, 144, 149, 153, 157, 161, 165.
- when the channel width is 40 MHz:
 - if "control-sideband" = lower: 36, 44, 52, 60, 132, 140, 149, 157.
 - if "control-sideband" = upper: 40, 48, 56, 64, 136, 144, 153, 161.
- when the channel width is 80 MHz: 36, 40, 44, 48, 52, 56, 60, 64, 132, 136, 140, 144, 149, 153, 157, 161.
- when the channel width is 160 MHz: 36, 40, 44, 48, 52, 56, 60, 64.

The following channels are available for Radio 6 GHz:

- when the channel width is 20 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.
- when the channel width is 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.
- when the channel width is 80/160 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.
- when the channel width is 320 MHz:
 - if "control-sideband" = lower: 1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61.
 - if "control-sideband" = upper: 33, 37, 41, 45, 49, 53, 57, 61, 65, 69, 73, 77, 81, 85, 89, 93.

6.6.1 Advanced Radio settings

Configuring a limited channel list

WEP-550K(config):/interface/wlan0/wlan/radio# **use-limit-channels true** (enable the use of the limited channel list in automatic channel selection operation. To disable, enter **false**. By default: true)

WEP-550K(config):/interface/wlan0/wlan/radio# **limit-channels '1 6 11'** (where 1, 6, 11 are the channels of the band in which the configurable radio interface can operate)

Changing the primary channel

WEP-550K(config):/interface/wlan0/wlan/radio# **control-sideband lower** (parameter can take the following values: **lower**, **upper**. By default: for Radio 1: lower; for Radio 2: upper)

Enabling use of short guard interval

WEP-550K(config):/interface/wlan0/wlan/radio# **sgi true** (enable the use of the shortened guard interval for data transmission — 400 ns, instead of 800 ns. To disable, enter **false**)

Enabling STBC

WEP-550K(config):/interface/wlan0/wlan/radio# **stbc true** (enable the space-time block coding (STBC) method, designed to improve data transmission reliability. To disable, enter **false**)

Enabling the use of short preamble

WEP-550K(config):/interface/wlan0/wlan/radio# **short-preamble true** (enable the use of the packet short preamble. To disable, enter **false**)

Enabling Wi-Fi Multimedia (WMM)

WEP-550K(config):/interface/wlan0/wlan/radio# **wmm true** (enable WMM (Wi-Fi Multimedia) support. To disable, enter **false**)

Configuring the DFS mechanism

Configuration is performed only on Radio 5 GHz (wlan1)

WEP-550K(config):/interface/wlan1/wlan/radio# **dfs X** (where X is the operating mode of the DFS mechanism. Possible values: **forced** — mechanism is disabled, DFS channels are available for selection; **auto** — mechanism is enabled; **disabled** — mechanism is disabled, DFS channels are not available for selection)

Enabling automatic channel width change mode

WEP-550K(config):/interface/wlan0/wlan/radio# **obss-coex true** (enable automatic channel width change mode from 40 MHz to 20 MHz when the radio environment is congested. To disable, enter **false**)

6.7 System settings

6.7.1 Device firmware update

Firmware upgrade of access points via tftp

WEP-550K(root):/# **firmware upload tftp** <IP Address of TFTP server> <Firmware file name> (example: **firmware upload tftp 192.168.1.15 WEP-550K-1.3.0_build_X.tar.gz**)
WEP-550K(root):/# **firmware upgrade**

Firmware upgrade of access points via http

WEP-550K(root):/# **firmware upload http** <URL to download the firmware file> (example: **firmware upload http http://192.168.1.100:8080/files/WEP-550K-1.3.0_build_X.tar.gz**)
WEP-550K(root):/# **firmware upgrade**

Switching to access point backup firmware

WEP-550K(root):/# **firmware switch**

6.7.2 Device configuration management

Reset device configuration to default without saving access parameters

WEP-550K(root):/# **manage-config reset-to-default**

Reset device configuration to default with preserving access parameters

WEP-550K(root):/# **manage-config reset-to-default-without-management**

Download the device configuration file to a TFTP server

WEP-550K(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 Address device>:/etc/config/config.json **config.json** (example: **scp admin@192.168.1.15:/etc/config/config.json config.json**. This command is performed on the server/PC)

Upload a configuration file to the device from a TFTP server

```
WEP-550K(root):/# manage-config upload tftp <IP Address of TFTP server> <Configuration file name>
(example: manage-config upload tftp 192.168.1.15 config.json)
WEP-550K(root):/# manage-config apply (apply configuration on the access point)
```

6.7.3 Device reboot

Command for rebooting the device

```
WEP-550K(root):/# reboot
```

6.7.4 Configuring the authentication mode

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

Changing the password for the admin account

```
WEP-550K(root):/# configure
WEP-550K(config):/# authentication
WEP-550K(config):/authentication# admin-password <new password for the admin account> (from 1 to 64
characters, including Latin letters and digits)
WEP-550K(config):/authentication# save
```

6.7.5 Setting the date and time

Commands for configuring time synchronization with an NTP server

```
WEP-550K(root):/# configure
WEP-550K(config):/# date-time
WEP-550K(config):/date-time# mode ntp (enable NTP mode)
WEP-550K(config):/date-time# ntp
WEP-550K(config):/date-time/ntp# server <IP address of the NTP server> (set the NTP server)
WEP-550K(config):/date-time/ntp# alt-servers (set additional NTP servers)
WEP-550K(config):/date-time/ntp/alt-servers# add <domain name/IP address of the NTP server in the
configuration> (create a configuration section for an additional NTP server. Maximum number: 8. To delete,
use the command del)
WEP-550K(config):/date-time/ntp/alt-servers# exit
WEP-550K(config):/date-time/ntp# exit
WEP-550K(config):/date-time# common
WEP-550K(config):/date-time/common# timezone 'Asia/Novosibirsk (Novosibirsk)' (set the time zone)
WEP-550K(config):/date-time/common# save (save settings)
```

6.7.6 Advanced system settings

Changing the device name

```
WEP-550K(root):/# configure
WEP-550K(config):/# system
WEP-550K(config):/system# hostname WEP-550K_room2 (where WEP-550K_room2 is a new device name. The
parameter can accept values from 1 to 63 characters: capital and lowercase Latin letters, digits, hyphen
character "-" (hyphen can not be the last character in name). By default: WEP-550K)
WEP-550K(config):/system# save (save settings)
```

Changing geographical domain

```
WEP-550K(root):/# configure
WEP-550K(config):/# system
WEP-550K(config):/system# ap-location ap.test.root (where ap.test.root is the domain of the device tree node
of the EMS management system in which the access point is located. By default: root)
WEP-550K(config):/system# save (save settings)
```

Changing Radius NAS-ID

```
WEP-550K(root):/# configure
WEP-550K(config):/# system
WEP-550K(config):/system# nas-id Lenina_1.Novosibirsk.root (where Lenina_1.Novosibirsk.root is the
identifier of this access point. The parameter is intended to identify the device on the RADIUS server if RADIUS
expects a value other than the MAC address. By default: MAC address of the access point)
WEP-550K(config):/system# save (save settings)
```

Configuring LLDP

```
WEP-550K(root):/# configure
WEP-550K(config):/# lldp
WEP-550K(config):/lldp# enabled true (enable the LLDP functionality. To disable, enter false. By default: true)
WEP-550K(config):/lldp# tx-interval 60 (changing the period for sending LLDP messages. By default: 30)
WEP-550K(config):/lldp# system-name WEP-550K_reserv (where WEP-550K_reserv is a new device name. By
default: WEP-550K)
WEP-550K(config):/lldp# save (save settings)
```

6.8 Configuring Captive Portal parameters

Configuring the parameter names passed by the authorization web server

```
WEP-550K(root):/# configure
WEP-550K(config):/# captive-portal
WEP-550K(config):/captive-portal# web-redirector
WEP-550K(config):/captive-portal/web-redirector# param-names
WEP-550K(config):/captive-portal/web-redirector/param-names# redirect_url original_url (setting the name of the parameter containing the original URL requested by the client. The client will be redirected to this URL if the authorization is successful)
WEP-550K(config):/captive-portal/web-redirector/param-names# error_url err_url (setting the name of the parameter containing the URL where the client will be redirected in case of an authorization error)
WEP-550K(config):/captive-portal/web-redirector/param-names# username login (setting the name of the parameter containing the login for the client)
WEP-550K(config):/captive-portal/web-redirector/param-names# password pass (setting the name of the parameter containing the password for the client)
WEP-550K(config):/captive-portal/web-redirector/param-names# save (save settings)
```

- ✓ The setting is needed if the parameter names in the http response with code 302 differ from the default names accepted by the access point.

- ✓ In the values of the **redirect_url**, **error_url**, **username**, **password** parameters, only the following characters can be used [a-zA-Z0-9\$\-_~!*'(),]{0,255}

Configuring the adaptive captive portal mode

```
WEP-550K(root):/# configure
WEP-550K(config):/# captive-portal
WEP-550K(config):/captive-portal# web-redirector
WEP-550K(config):/captive-portal/web-redirector# captive-adaptive true (enabling the adaptive captive portal mode for iOS devices. To disable, enter false. By default: false)
WEP-550K(config):/captive-portal/web-redirector# save (save settings)
```

- ✓ With the adaptive mode enabled, the connection will not be dropped when the authorization window is minimized on iOS devices.

Configuring ipv4-acl rules

```

WEP-550K(root):/# configure
WEP-550K(config):/# acl
WEP-550K(config):/acl# ipv4
WEP-550K(config):/acl/ipv4# add ipv4_list (create an ACL rule list)
WEP-550K(config):/acl/ipv4#ipv4_list
WEP-550K(config):/acl/ipv4/ipv4_list# entry
WEP-550K(config):/acl/ipv4/ipv4_list/entry# add 0 (create an ACL rule)
WEP-550K(config):/acl/ipv4/ipv4_list/entry# 0
WEP-550K(config):/acl/ipv4/ipv4_list/entry/0# action permit (specify the action for the rule. Possible values:
permit — allow, deny — deny)
WEP-550K(config):/acl/ipv4/ipv4_list/entry/0# protocol-mode any (configure the protocol mode that the rule
applies to. Possible values: any — any protocol, value — specific protocol)
WEP-550K(config):/acl/ipv4/ipv4_list/entry/0# protocol gre (select the protocol. Possible values: gre, icmp,
igmp, tcp, udp)
WEP-550K(config):/acl/ipv4/ipv4_list/entry/0# src-port-start X (where X is the starting source port)
WEP-550K(config):/acl/ipv4/ipv4_list/entry/0# src-port-end X (where X is the ending source port. Used only for
src-port-mode range)
WEP-550K(config):/acl/ipv4/ipv4_list/entry/0# src-mode host (configure the source filtering mode. Possible
values: any — any source, host — filtering by host address, network — filtering by network address)
WEP-550K(config):/acl/ipv4/ipv4_list/entry/0# src-ip X.X.X.X (where X.X.X.X is the source host IP address)
WEP-550K(config):/acl/ipv4/ipv4_list/entry/0# src-mask X.X.X.X (where X.X.X.X is the source host subnet mask)
WEP-550K(config):/acl/ipv4/ipv4_list/entry/0# src-port-mode any (configure the source port mode. Possible
values: any — any mode, eq — equal, gt — greater than, lt — less than, neq — not equal, range — port range)
WEP-550K(config):/acl/ipv4/ipv4_list/entry/0# dst-mode host (configure the destination filtering mode. Possible
values: any — any source, host — filtering by host address, network — filtering by network address)
WEP-550K(config):/acl/ipv4/ipv4_list/entry/0# dst-ip X.X.X.X (where X.X.X.X is the destination host IP address)
WEP-550K(config):/acl/ipv4/ipv4_list/entry/0# dst-mask X.X.X.X (where X.X.X.X is the destination host subnet
mask)
WEP-550K(config):/acl/ipv4/ipv4_list/entry/0# dst-port-mode any (configure the destination port mode.
Possible values: any — any mode, eq — equal, gt — greater, lt — less, neq — not equal, range — port range))
WEP-550K(config):/acl/ipv4/ipv4_list/entry/0# dst-port-start X (where X is the starting destination port)
WEP-550K(config):/acl/ipv4/ipv4_list/entry/0# dst-port-end X (where X is the ending destination port.
Used only for dst-port-mode range)
WEP-550K(config):/acl/ipv4/ipv4-acl/ipv4_list/entry/0# save (save settings)

```

Configuring url-acl rules

```

WEP-550K(root):/# configure
WEP-550K(config):/# acl
WEP-550K(config):/acl# url
WEP-550K(config):/acl/url# add url_list (create an ACL rule list)
WEP-550K(config):/acl/url# url_list
WEP-550K(config):/acl/url/url_list# action permit (specify the action for the list. Possible values: permit —
allow, deny — deny)
WEP-550K(config):/acl/url/url_list# entry
WEP-550K(config):/acl/url/url_list/entry# add 0 (create an ACL rule)
WEP-550K(config):/acl/url/url_list/entry# 0
WEP-550K(config):/acl/url/url_list/entry/0# domain <Domain name> (specify a domain name or a regular
expression)
WEP-550K(config):/acl/url/url_list/entry/0# save (save settings)

```

6.9 Configuring DAS server

The DAS server function processes dynamic RADIUS authorization requests from access points.

Commands for configuring the DAS server

```
WEP-550K(root):/# configure  
WEP-550K(config):/# das-server  
WEP-550K(config):/das-server# enabled true (enable the DAS server. To disable, enter false)  
WEP-550K(config):/das-server# auth-password secret (where secret — is the DAS server password, used to  
encrypt RADIUS requests)  
WEP-550K(config):/das-server# save (save settings)
```

6.10 Monitoring

6.10.1 Wi-Fi clients

WEP-550K(root):/# **monitoring associated-clients**

```

index                | 0
ssid                 | Virtual Access Point 0 (6GHz)
hw-addr              | 0a:a5:08:xx:xx:xx
ip-addr              | 192.168.1.15
hostname             | client
domain               | root
authenticated        | yes
associated            | yes
authorized            | yes
captive-portal-vap   | no
enterprise-vap        | no
band                  | 6
tx-fails              | 14
link-capacity         | 100%
link-quality          | 100%
uptime               | 00:12:05
interface           | wlan2-vap0
rfid                  | 2
wid                   | 0
tx-bw                 | 320M
rx-bw                 | 320M
rx-bw-all            | 320M
rssi-1                | -30
rssi-2                | -32
rssi                  | -32
snr-1                 | 55
snr-2                 | 54
snr                   | 54
mfp                   | yes
tx-rate               | EHT NSS2-MCS10 ?xLTF GI 0.8us 4322
rx-rate               | EHT NSS2-MCS12 ?xLTF GI 0.8us 5188
tx-retry-count        | 14
rx-retry-count        | 1156
tx-period-retry       | 0
using-802.11r         | no
using-802.11k         | no
using-802.11v         | no
wireless-mode         | be
mlo-enabled           | yes
mld-mac               | 0a:a5:08:15:aa:dc
mlo-link-1-band       | 6
mlo-link-1-mac        | 0a:a5:08:15:aa:61
name                  | wlan2-vap0:sta-0

```

Counter	Transmitted	Received
Total Packets:	7110	9168
TX success:	100	
Total Bytes:	5454016	1939584
Data Packets:	0	4263
Data Bytes:	0	1169546

Mgmt Packets:	7	32
Mgmt Bytes:	0	0
Dropped Packets:	0	0
Dropped Bytes:	0	0
Lost Packets:	0	

Multicast groups: none

6.10.2 Device information

WEP-550K(root):/# **monitoring information**

```

system-time           | 07:54:17 13.05.2026
uptime                | 00:01:42
hostname              | WEP-550K
software-version      | 1.3.0 build X
secondary-software-version | 1.3.0 build X
boot-version          | 1.3.0 build X
uboot-version         | 1.3.0 build X
memory-usage          | 52%
memory-free           | 466M
memory-used           | 515M
memory-total          | 981M
cpu-load              | 2.9%
cpu-average           | 2.30%
is-default-config     | true
vendor                | Eltex
device-type           | Access Point
board-type             | WEP-550K
hw-platform           | WEP-550K
factory-wan-mac        | 0C:EE:20:xx:xx:xx
factory-lan-mac        | 0C:EE:20:xx:xx:xx
factory-serial-number  | WPxxxxxxxx
hw-revision            | 1v2
session-password-initialized | false
ott-mode              | false
last-reboot-reason     | reboot by user
test-changes-mode      | false
power-supply           | PoE++

```

6.10.3 Network information

WEP-550K(root):/# **monitoring wan-status**

Common information:

interface	br0
mac	0c:ee:20:xx:xx:xx
rx-bytes	456875
rx-packets	5835
tx-bytes	24328
tx-packets	241

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

WEP-550K(root):/# **monitoring ethernet-ports**

ETH0:

```

name: ETH0
link: up
speed: 1000
duplex: enabled
media-type: copper
rx-bytes: 69952
rx-packets: 662
tx-bytes: 22397
tx-packets: 143

```

ETH1:

```

name: ETH1
link: down
speed: 10
duplex: disabled
media-type: copper
rx-bytes: 0
rx-packets: 0
tx-bytes: 0
tx-packets: 0

```

WEP-550K(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

WEP-550K(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

WEP-550K(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	e0:d9:e3:xx:xx:xx	gi 0/16	MES	B,R	120

6.10.4 Wireless interfaces

WEP-550K(root):/# **monitoring radio-interface**

```

name           | wlan0
rfid           | 0
status        | on
band           | 2.4 GHz
hwaddr        | 0C:EE:20:xx:xx:xx
tx-power      | 15 dBm
connection status | AP mode
operation mode | vap
mode          | b/g/n/ax/be
noise-1       | -92 dBm
noise-2       | -92 dBm
channel       | 6
frequency     | 2437 MHz
bandwidth     | 20 MHz
utilization   | 5%
thermal       | 41

```

```

name           | wlan1
rfid           | 1
status        | on
band           | 5 GHz
hwaddr        | 0C:EE:20:xx:xx:xx
tx-power      | 19 dBm
connection status | AP mode
operation mode | vap
mode          | a/n/ac/ax/be
noise-1       | -92 dBm
noise-2       | -92 dBm
channel       | 36
frequency     | 5180 MHz
bandwidth     | 20 MHz
utilization   | 1%
thermal       | 40

```

```

name           | wlan2
rfid           | 2
status        | on
band           | 6 GHz
hwaddr        | 0C:EE:20:xx:xx:xx
tx-power      | 19 dBm
connection status | AP mode
operation mode | vap
mode          | ax/be
noise-1       | -92 dBm
noise-2       | -92 dBm
channel       | 1
frequency     | 5955 MHz
bandwidth     | 20 MHz
utilization   | 0%
thermal       | 45

```

6.10.5 Event logging

WEP-550K(root):/# monitoring events

```
Jan  1 00:00:36 WEP-550K user.notice root: The AP startup configuration was updated
successfully by root
Jan  1 00:00:36 WEP-550K daemon.info networkd[4442]: DHCP-client: Interface br0 obtained
lease on 192.168.1.15.
Oct  1 06:03:13 WEP-550K daemon.info configd[4390]: The AP running configuration was updated
successfully by admin
Oct  1 06:08:42 WEP-550K auth.info login[24431]: root login on 'pts/0'
Oct  1 06:16:41 WEP-550K daemon.info hostapd: wlan0-vap2: STA 16:40:ee:xx:xx:xx IEEE 802.11:
associated
Oct  1 06:16:41 WEP-550K daemon.info hostapd: Client '16:40:ee:xx:xx:xx' successfull
authorized with 'wlan0-vap2', SSID 'eltex', Domain '', RSSI '-34'
```

6.10.6 Environment scan

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

WEP-550K(root):/# monitoring scan-wifi

SSID	Mode	Security	BSSID	Channel	RSSI, dBm	Bandwidth, MHz
Eltex-WiFi-Client	AP	off	00:11:11:11:11:11	6	-37	20
WEP-550K-2-40	AP	wpa2	00:11:11:11:11:11	9	-51	40L
test_21_20	AP	wpa2	00:11:11:11:11:11	1	-54	20
Eltex-Device	AP	wpa2	00:11:11:11:11:11	11	-61	20
Virtual Access Point 1	AP	off	00:11:11:11:11:11	6	-62	40L
Eltex-WiFi	AP	off	00:11:11:11:11:11	6	-62	40L
test_2000	AP	wpa/wpa2	00:11:11:11:11:11	2	-79	40L
wifi_1000	AP	off	00:11:11:11:11:11	149	-79	80
WEP-550K-2-2000	AP	off	00:11:11:11:11:11	48	-79	20
11111111	AP	off	00:11:11:11:11:11	52	-79	20
test2000-2000	AP	wpa2	00:11:11:11:11:11	40	-79	20
test2000	AP	wpa/wpa2	00:11:11:11:11:11	11	-79	20
WEP-550K	AP	off	00:11:11:11:11:11	11	-80	20
test_2000-1x	AP	wpa2-1x	00:11:11:11:11:11	11	-80	20
test2000-test-portal	AP	off	00:11:11:11:11:11	1	-81	20
Eltex-Local	AP	wpa3-1x	00:11:11:11:11:11	77	-81	20
wifi_1000-1000-1000	AP	wpa2-1x	00:11:11:11:11:11	1	-82	20
WEP-550K	AP	off	00:11:11:11:11:11	64	-82	160
Eltex-Device	AP	wpa2	00:11:11:11:11:11	11	-82	20
Eltex-Device	AP	wpa2	00:11:11:11:11:11	11	-82	20
WEP-550K-2000	AP	owe	00:11:11:11:11:11	64	-83	160
test_2000-2000	AP	wpa2-1x	00:11:11:11:11:11	64	-83	80
WEP-550K	AP	wpa3	00:11:11:11:11:11	53	-83	320L

6.11 Obtaining troubleshooting information

Command for obtaining troubleshooting information

```
WEP-550K(root):/# get-troubleshooting-file
```

After the command is executed, an archive *troubleshooting.tar.gz* will be created, containing debug data and information about the device status.

The archive *troubleshooting.tar.gz* can be obtained from the device to a server via the TFTP protocol.

Command for obtaining troubleshooting information

```
WEP-550K(root):/# tftp -pl troubleshooting.tar.gz <IP address of TFTP server>
```

```
troubleshooting.tar. 100% |*****| 62755 0:00:00 ETA
```

The archive *troubleshooting.tar.gz* can be obtained from the device to a server/PC via the SCP protocol:

```
scp <user>@<IP address access point>:troubleshooting.tar.gz troubleshooting.tar.gz (example: scp admin@192.168.1.15:troubleshooting.tar.gz troubleshooting.tar.gz. This command is performed on the server/PC)
```

7 Auxiliary utilities

7.1 traceroute utility

This utility shows which nodes (routers) a packet passes through and how long packet processing takes at each node.

Traceroute command

```
WEP-550K(root):/# traceroute <test host>
```

7.2 tcpdump utility

The tcpdump utility allows capturing packets on the specified interface.

To get help on using the utility, enter the command:

```
WEP-550K(config):/# tcpdump --help
```

7.2.1 Capturing traffic from any active interface

For example, you can enable packet capturing on the Ethernet interface.

Command example

```
WEP-550K(root):/# tcpdump -i eth0
```

7.3 iperf utility

This utility is used to launch a traffic stream from one device to another. The sending side is called the client, the receiving side — server.

To get help on using the utility, enter the command:

```
WEP-550K(root):/# iperf --help
```

Example of launching a traffic stream from the access point to the server:

Configuring the server to receive traffic

```
root@server:/# iperf -s
```

Generating traffic from the AP client to the server

```
WEP-550K(root):/# iperf -c X.X.X.X (where X.X.X.X is the server IP address)
```

8 The list of changes

Document version	Release date	Change description
Version 1.1	05.2026	Synchronization with software version 1.3.0 Added: 5.6.3 "MLO" submenu 5.9.7 "Troubleshooting" submenu 6.3.6 Configuring an additional RADIUS server on VAP 6.9 Configuring DAS server Changed: 5.5.3 "Radio 6 GHz" submenu 5.6 "VAP" menu 6.3.5 Configuring VAP with external Captive Portal 6.3.7 Advanced VAP settings 6.7.2 Device configuration management 6.7.5 Setting the date and time 6.8 Configuring Captive Portal parameters 6.10 Monitoring 6.11 Obtaining troubleshooting information
Version 1.0	03.2026	First publication
Software version 1.3.0		

TECHNICAL SUPPORT

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

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

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

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

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