Wireless access point

WEP-2ac, WEP-2ac Smart

User manual

Firmware version 1.23.0

IP address: 192.168.1.10

Username: admin

Password: password

Contents

1 Introduction

1.1 Annotation

Modern tendencies of telecommunication development necessitate operators to search for the most optimal technologies, allowing you to satisfy drastically growing needs of subscribers, maintaining at the same time consistency of business processes, development flexibility and reduction of costs of various services provision. Wireless technologies are spinning up more and more and have paced a huge way for short time from unstable low-speed communication networks of low radius to broadband networks equitable to speed of wired networks with high criteria to the quality of provided services. WEP-2ac and WEP-2ac Smart are Wi-Fi access points of the Enterprise class. The devices are dedicated to be installed inside buildings as access points and to create a seamless wireless network using several identical access points (roaming) on a large area.
This manual specifies intended purpose, main technical parameters, design, installation procedure, safe operation rules and installation recommendations for these devices.

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

WEP-2ac and WEP-2ac Smart wireless access points (hereinafter the devices) are designed to provide users with access to a high-speed and safe network.

The device is dedicated to create L2 wireless networks interfacing with a wired network. WEP-2ac and WEP-2ac Smart are connected to a wired network via 10/100/1000M Ethernet interface and arrange high-speed access to the Internet for devices supporting Wi-Fi technology at 2.4 and 5 GHz.

The devices have two radio interfaces to organize two physical wireless networks.

WEP-2ac and WEP-2ac Smart support up-to-date requirements to service quality and allows transmitting more important traffic in higher priorities queues. Prioritization is based on main QoS technologies: CoS (special tags in VLAN packet field) and ToS (tags in IP packet field). Besides the standard methods of prioritization, devices allow assigning demands for traffic transmission almost in every packet field from MAC to TCP/UDP port. The ACL rules and shaping allow controlling access, quality of service and restrictions for all subscribers as well as for each subscriber individually.
The devices are designed to be installed in offices, state buildings, conference halls, laboratories, hotels, etc. The creation of virtual access points with different types of encryption allows clients to delimit access rights among users and groups of users.

2.2 Device specifications

Interfaces:

- 1 port of Ethernet 10/100/1000BASE-T (RJ-45) with PoE+ support;
- Wi-Fi 2.4 GHz IEEE 802.11b/g/n;
- Wi-Fi 5 GHz IEEE 802.11a/n/ac;
- Console RJ-45.

Functions:

WLAN capabilities:

- support for IEEE 802.11a/b/g/n/ac standards;
- data aggregation, including A-MPDU (Tx/Rx) and A-MSDU (Rx);
- WMM-based priorities and packet planning;
- Dynamic Frequency Selection (DFS);
- support for hidden SSID;
- 32 virtual access points;
- third-party access point detection;
- Workgroup Bridge;
- WDS;
- MESH;
- APSD.

Network functions:

- autonegotiation of speed, duplex mode and switching between MDI and MDI-X modes;
- support for VLAN;
- support for 802.11k/r;
- DHCP client;
- support for IPv6;
- LLDP;
- ACL;

- SNMP;
- GRE.

Cluster operating mode:

- organizing a cluster with capacity of up to 64 access points;
- auto synchronization of access point configurations in a cluster;
- auto update of access points firmware in a cluster;
- Single Management IP – united address to control access points in a cluster;
- automatic distribution of frequency channels among access points;
- automatic distribution of output power level among access points.

QoS functions:

- priority and profile-based packet scheduling;
- bandwidth limiting for each SSID;
- changing WMM parameters for each radio interface.

Security:

- e-mail notification about system events;
- centralized authorization via RADIUS server (802.1X WPA/WPA2 Enterprise);
- WPA/WPA2;
- Captive Portal;
- support for Internet Protocol Security (IPSec);
- support for WIDS/WIPS.

The figure below shows WEP-2ac application scheme.

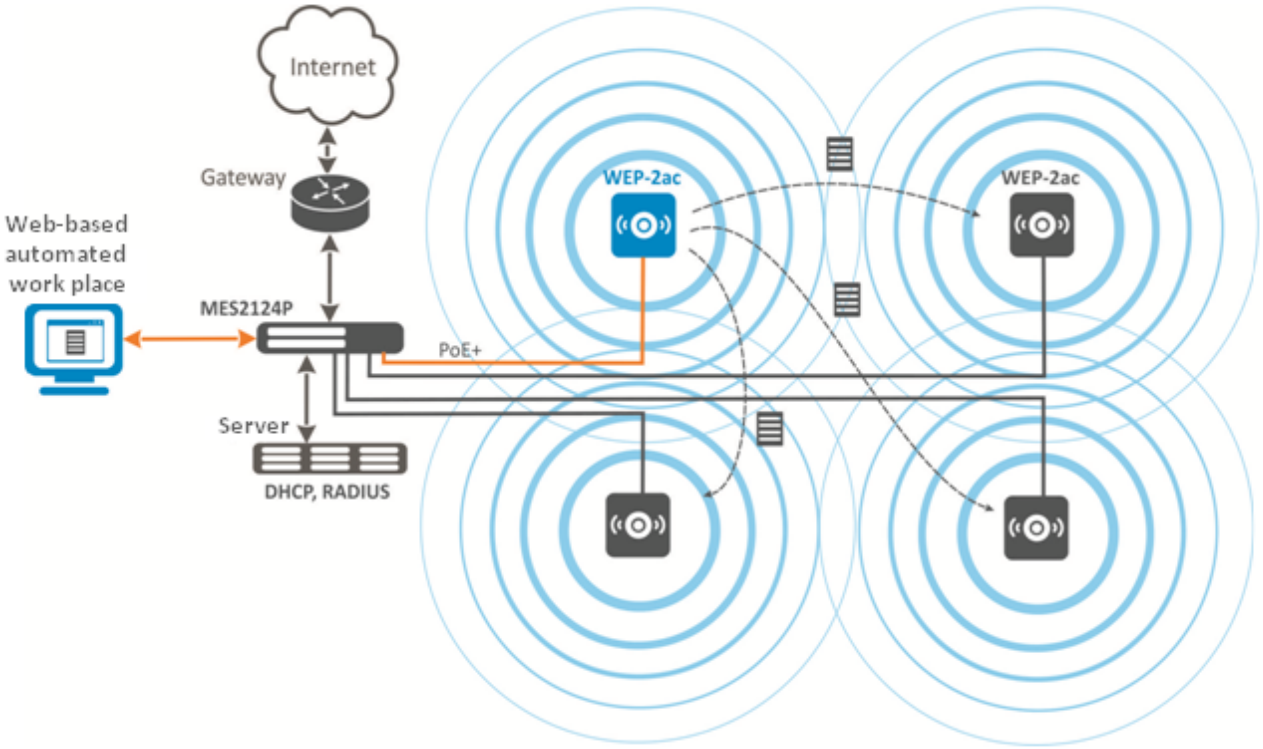


Figure 1 – WEP-2ac application scheme

2.3 Device technical parameters

Table 1 — Main specifications

WAN Ethernet interface parameters	
Number of ports	1
Electrical connector	RJ-45
Data rate, Mbps	10/100/1000, autonegotiation
Standards	BASE-T
Wireless interface parameters	
Standards	802.11a/b/g/n/ac
Frequency range, MHz	2400–2483.5 MHz; 5350 MHz, 5470–5850 MHz
Modulation	BPSK, QPSK, 16QAM, 64QAM, 256QAM
Operating channels	802.11b/g/n: 1-13 (2412–2472 MHz) 802.11a/ac: 36-64 (5170–5330 MHz) 100-144 (5490–5730 MHz) 149-165 (5735–5835 MHz)
Speed of data transmission, Mbps	6, 9, 12, 18, 24, 36, 48, 54, MCS0-MCS15, MCS0-9 NSS1, MCS0-9 NSS2 802.11n: up to 144,4 Mbps (20 MHz channel), up to 300 Mbps (40 MHz channel) 802.11ac: up to 866,7 Mbps (80 MHz)
Maximum output power of the transmitter	2.4 GHz up to 18 dBm[1] 5 GHz: up to 21 dBm[1]
Built-in antenna gain	2.4 GHz up to 5 dBi 5 GHz up to 5 dBi
Receiver sensitivity	2.4 GHz up to -98 dBm 5 GHz up to -94 dBm
Security	centralized authorization via RADIUS server (802.1X WPA/WPA2 Enterprise); 64/128/152-bit WEP data encryption, WPA/WPA2 support for Captive Portal e-mail notifying on system events
Support for 2x2 MIMO	
Control	
Remote control	web interface, Telnet, SSH, SNMP, EMS management system firmware updating and configuring by DHCP Autoprovisioning
Access restriction	by password, by IP address
General parameters	
NAND	128 MB NAND Flash
RAM	256 MB RAM DDR3
Power supply	PoE+ 48 V/54 V (IEEE 802.3at-2009)

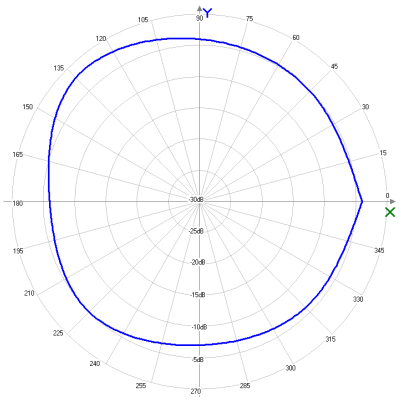
Power consumption	up to 13 W
Operating temperature	from +5 to +40 °C
Relative humidity at 25 °C	up to 80 %
WEP-2ac dimensions	200 × 40 mm
WEP-2ac Smart dimensions	200 × 43 mm
Weight	0.4 kg

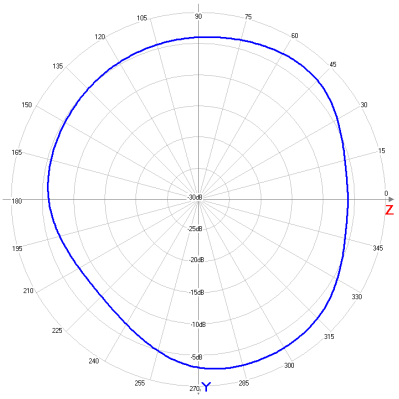
[1]Defined by Transmit Power Limit and Transmit Power Control regulators

2.4 Radiation patterns

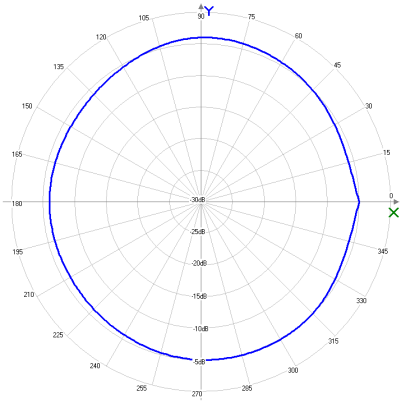
Radiation patterns for the embedded antennas are given below.

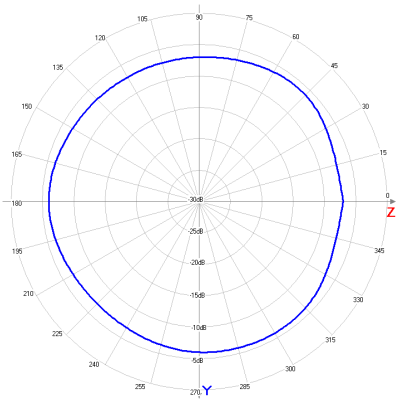
2.4 GHz





5 GHz





For WEP-2ac Smart in the 5 GHz band, the Smart Antenna uses the beam switching method — this is more than 700 radiation patterns that dynamically change during the operation of the access point. WEP-2ac Smart constantly evaluates the location of customers and sources of radio interference, and then selects the optimal radiation pattern for each moment in time from 700 templates.

2.5 Design

WEP-2ac and WEP-2ac Smart are housed in a plastic case.

2.5.1 Device main panel

The main panel layout of the device is depicted in Fig. 2.

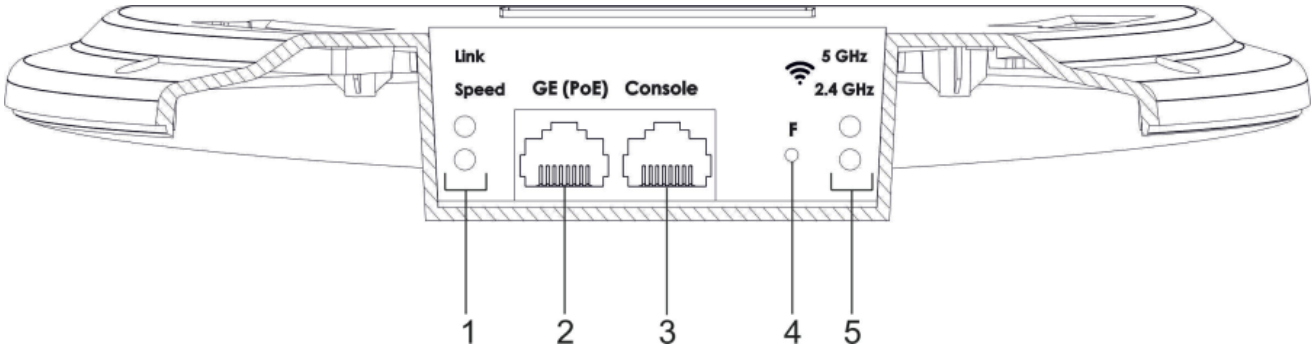


Figure 2 – Main panel layout of the device

The following light indicators, connectors and controls are located on the main panel of WEP-2ac and WEP-2ac Smart:

Table 2 – Description of ports and controls

Main panel elements		Description
1	Link/Speed	GE (PoE) port status light indication
2	GE (PoE)	GE port for PoE+ power supply connection
3	Console	RS-232 console port for local control of the device
4	F	Functional key
5	Wi-Fi	Operation indicators of corresponding Wi-Fi modules

2.6 Light indication

The current device state is displayed by **Wi-Fi**, **LAN, Power** indicators. The list of possible LED states is given below.

Table 3 – Light indication of device state

LED	LED status	Device state
Wi-Fi	solid green	Wi-Fi network is active
	flashing green	the process of data transmission trough a wireless network
LAN	solid green (10, 100 Mbps)/ solid orange (1000 Mbps)	the link with the connected network device is established
	flashing green	the process of packet data transmission through LAN interface
Power	solid green	the device power supply is enabled, normal operation, IP address is obtained
	solid orange	the device is loaded but IP address is not received via DHCP
	solid red	the device is loading

2.7 Reset to the default settings

In order to reset the device to factory settings, press and hold the 'F' button until Power indicator starts flashing. Device will be rebooted automatically. DHCP client will be launched by default. If the address is not received via DHCP the device will have IP address — *192.168.1.10*, subnet mask — *255.255.255.0* and User Name/Password to access via Web interface: admin/password.

2.8 Delivery package

The delivery package includes:

- Wireless access point WEP-2ac/WEP-2ac Smart;
- Mounting kit;
- User manual on a CD (optional);
- Technical passport.

3 Installation order

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

3.1 Safety rules

1. Do not install the device close to heat sources or in rooms with temperature below 5 °C or above 40 °C.
2. Do not use the device in places with high humidity. Do not expose the device to smoke, dust, water, mechanical vibrations or shocks.
3. Do not open the device case. There are no user serviceable parts inside.

Do not cover ventilation holes and do not put other objects on the device in order to prevent overheating of device components.

3.2 Installation recommendations

1. The recommended mounting position: horizontal, on a ceiling.
2. Before installing and enabling the device, check it for visible mechanical defects. If defects are observed, stop the device installation, draw up corresponding act and contact the supplier.
3. If the device has been exposed for a long time at a low temperature, it must be left to stand for two hours at room temperature before use. After a long stay of the device in conditions of high humidity, let it stand under normal conditions for at least 12 hours before switching on.
4. During the device installation, follow these rules to ensure the best Wi-Fi coverage:
    a. Install the device at the center of a wireless network;
    b. Minimize the number of obstacles (walls, roof, furniture and etc.) between access point and other wireless network devices;
    c. Do not install the device near (about 2 m) electrical and radio devices;
    d. It is not recommended to use radiophone and other equipment operating on the frequency of 2.4 GHz, 5 GHz in Wi-Fi effective radius;
    e. Obstacles 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. During the installation of several access points, cell action radius must overlap with action radius of a neighbouring cell at level of -65 ÷ -70 dBm. Decreasing of the signal level on cells borders to -75 dBm is permitted if it involves the use of VoIP, streaming video and other traffic that is sensitive to losses in wireless network.

3.3 Calculating the number of required access points

To calculate the required number of access points, evaluate the required coverage zone. For a more accurate assessment, it is necessary to make a radio examination of the room. Approximate radius of coverage area of WEP-2ac with a good-quality signal in case of mounting on a ceiling in typical office: 2.4 GHz 40-50 m, 5 GHz: 20-30 m. In the absence of obstacles, the coverage radius: 2.4 GHz up to 100 m; 5 GHz up to 60 m.
The table below describes rough attenuation values.

Table 4 – Attenuation values

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

3.4 Channel selection for neighboring access points

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

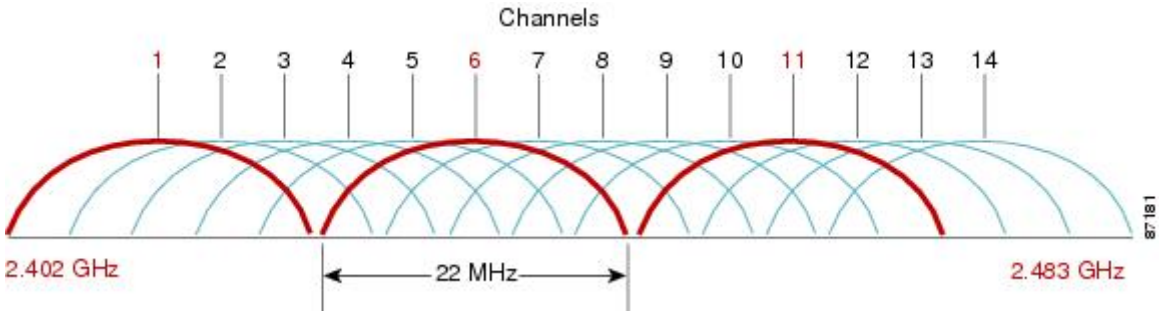


Figure 3 – General diagram of frequency channel closure in the range of 2.4 GHz

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

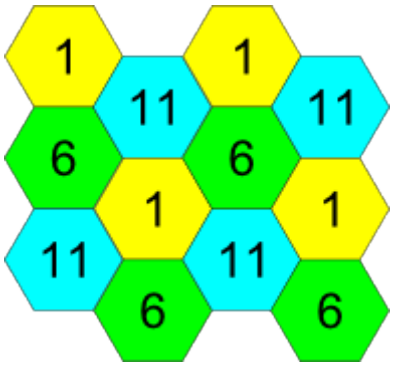


Figure 4 – Diagram of channel allocation among neighboring access points in the frequency range of 2.4 GHz when channel width is 20 MHz

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

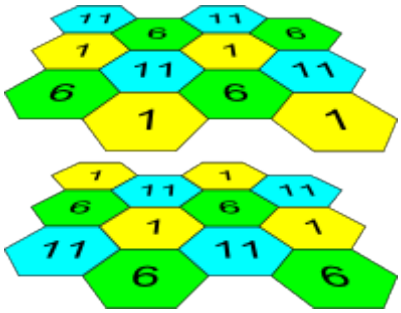


Figure 5 – Diagram of channel allocation between neighboring access points that are located between floors

When width of used channel is 40 MHz there is no non-overlapping channels in frequency range of 2.4 GHz. In such cases, select channels maximally separated from each other.

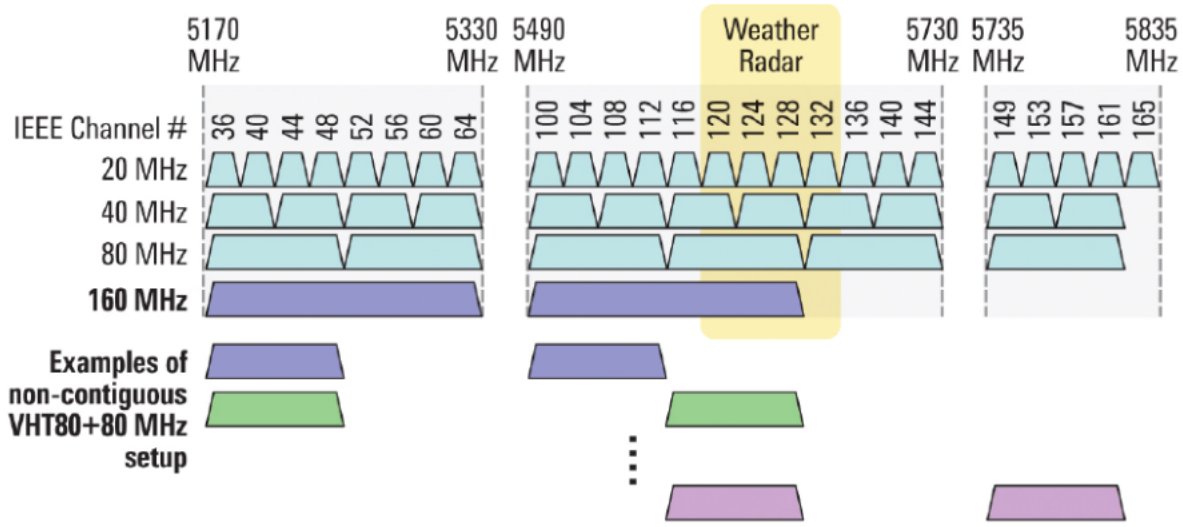


Figure 6 – Channels used in range of 5 GHz when channel width is 20, 40 or 80 MHz

3.5 Device installation

The device should be attached to plain surface (wall or ceiling) in accordance with the safety instruction and recommendations listed above.
The device delivery package includes required mounting kit to attach the device to plain surface.

3.5.1 Wall mounting

1. Fix the bracket (included in the delivery package) to the wall:

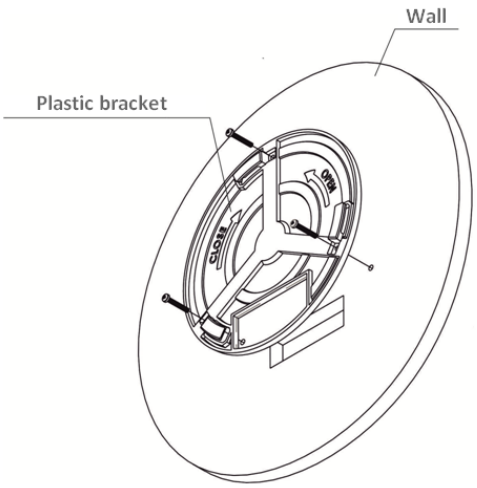


Figure 7 – Attaching the bracket to a wall

a. The figure shows the bracket allocation;
b. When installing the bracket, pass wires through the corresponding grooves of the bracket, see figure 7;
c. Pass the wires into the corresponding grooves on the bracket while installing the bracket. Screw the brackets to the device surface by using screwdriver.

2. Install the device.

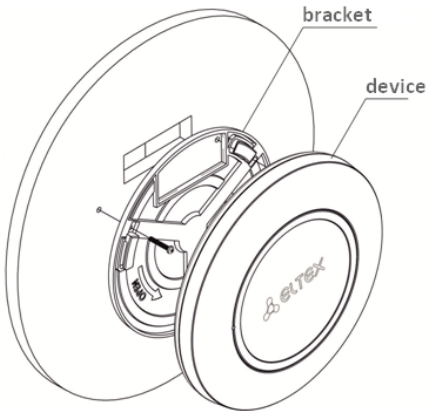
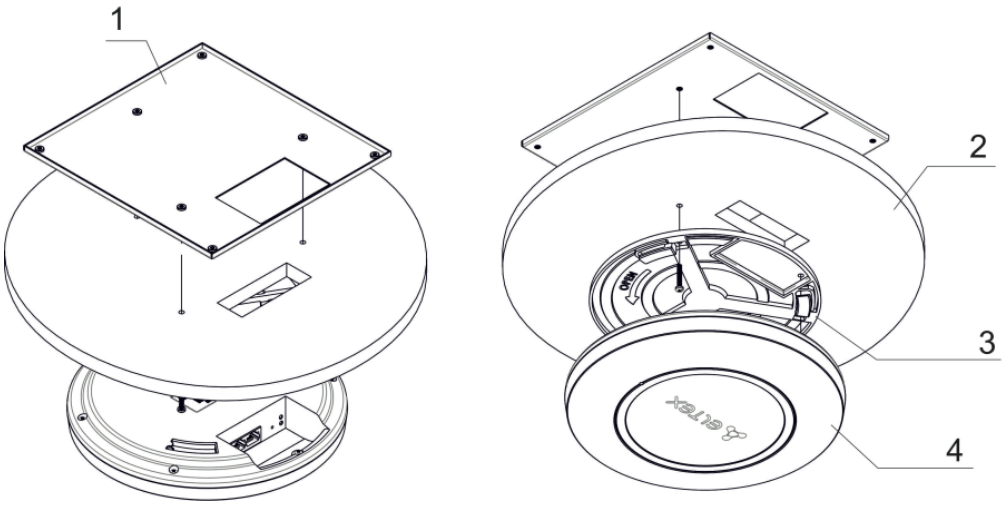


Figure 8 – Device installation (front view)

1. Connect cables to corresponding connector of the device.
   Description of the connectors is given in Design section.
2. Align the device and bracket together, fix the position, turning clockwise.

3.5.2 Installing to false ceiling

It is not recommended to place the device inside a false ceiling as metal frame causes multipath signal propagation and signal attenuation.



1 – metal bracket; 2 – Armstrong panel; 3 – plastic bracket; 4 – device.

Figure 9 – Mounting to a false ceiling

1. Fasten metal and plastic bracket on a ceiling as shown in the figure 9.
   a. The plastic bracket (**3**) should be joined with the metal one (**1**) on the ceiling in the following order: metal bracket -> Armstrong panel -> plastic bracket.
   b. Cut the hole in the Armstrong panel. The size of the hole should be equal to hole of metal bracket. Conduct wires through the hole.
   c. Align holes in metal bracket with holes of Armstrong panel and plastic bracket. Align together three screw holes on the plastic bracket and the screw holes on the metal bracket. Screw the brackets to the device surface by using a screwdriver.
2. Install the device.
   a. Connect cables to corresponding connector of the device. Description of the connectors is given in Design section.
   b. Align the device and plastic bracket together, fix the position, turning clockwise.

3.5.3 Removing the device from the bracket

For removing the device from the bracket:

1. Turn the device counterclockwise;
2. Remove the device.

4 Device management via the web interface

4.1 Getting started

Connect network cable to the PoE interface of the access point and to the PoE switch/injector. Next, connect a PC to the injector or switch:

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

   IP address by default: 192.168.1.10, subnet mask: 255.255.255.0.
   The device can obtain IP address via DHCP. Until then, it is available at the factory IP address.

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

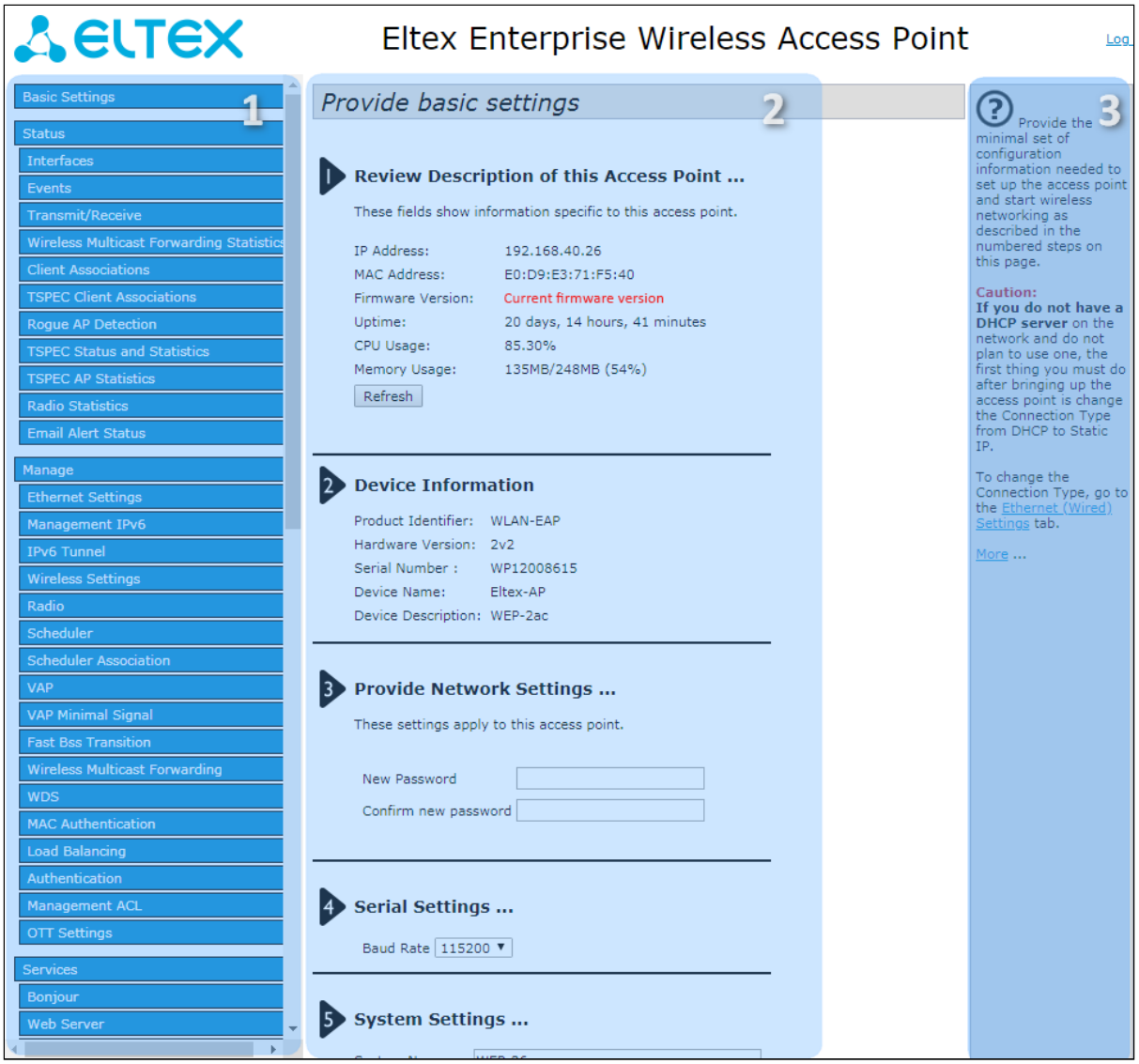
3. Enter username into 'User Name' and password into 'Password' field.

   Factory default authorization settings: User Name – *admin*, Password – *password*.

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

4.2 Web interface basic elements

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

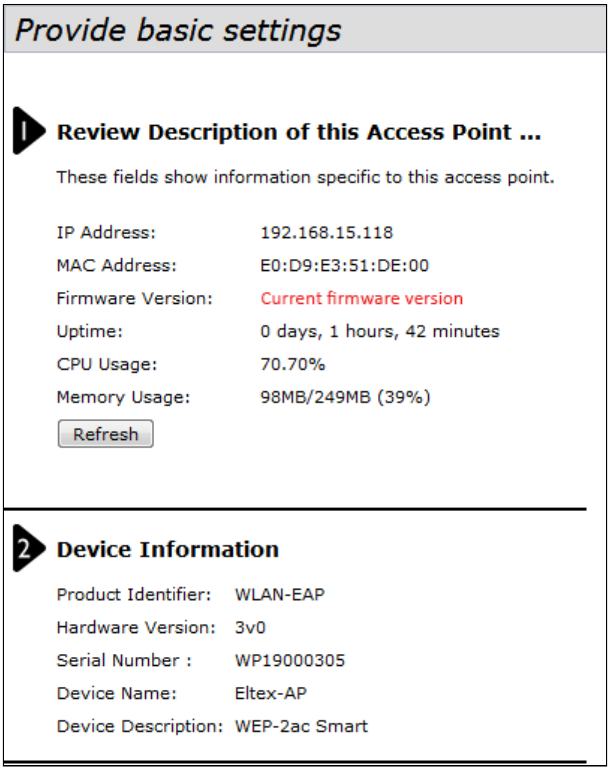


User interface window is divided into three general areas:

1. Tabs of the device settings menu.
2. Main configuration field of the selected tab.
3. Information on the selected menu section.

4.3 'Basic Settings' menu

In the **'Basic Settings'** menu, basic information about the device is displayed. This menu provides the ability to change the password for accessing the device and configure the speed of the Console port.

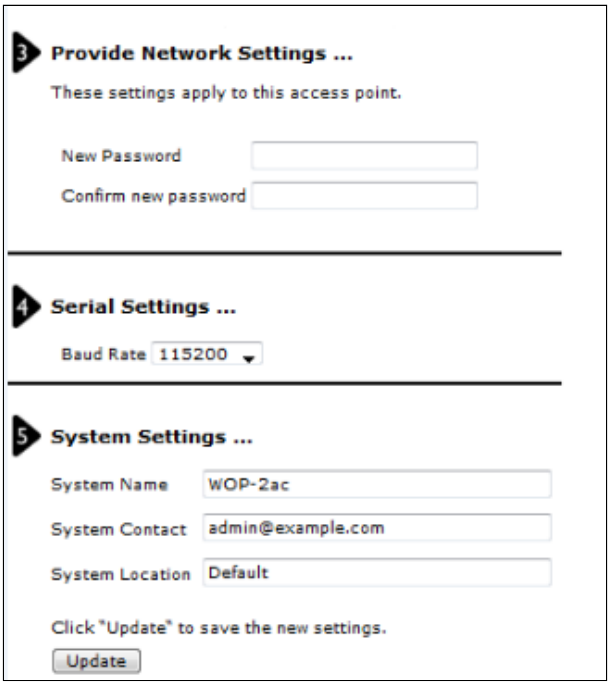


Review Description of this Access Point – this section provides information about network settings of the device and firmware version.

- *IP Address* – IP address of the device;
- *MAC Address* – MAC address of the device;
- *Firmware Version* – firmware version;
- *Uptime* – operation time;
- *CPU Usage* – average percentage of CPU usage over the last 10 seconds;
- *Memory Usage* – percentage of device physical memory usage.

Device Information – main information about the device.

- *Product Identifier* – device identifier;
- *Hardware Version* – hardware version;
- *Serial Number* – serial number of the device;
- *Device Name* – system name of the device;
- *Device Description* – device description.



Provide Network Settings – in this section, password for accessing the device web/CLI configurator can be changed.

- *New Password* – new password;
- *Confirm new password* – confirmation of new password.

Serial Settings – Console interface settings.

- *Baud Rate* – data transfer rate via Console interface, bps. By default, the parameter is 115200. May take values 9600, 19200, 38400, 57600, 115200.

System Settings – in this section, system settings of the device can be changed.

- *System Name* – system name of the device;
- *System Contact* – contact information for communication with the administrator;
- *System Location* – information about the physical location of the device.

To apply a new configuration and save setting to non-volatile memory, click 'Apply'.

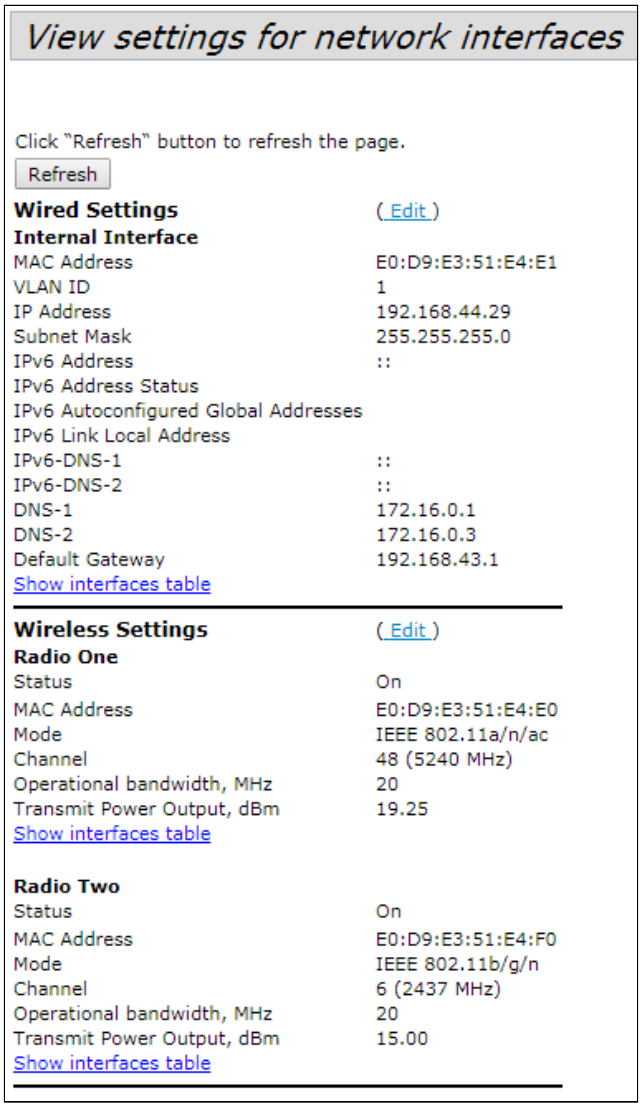
4.4 'Status' menu

The '**Status**' menu displays current state of the system, provides information about the state of the device interfaces, events registered on the device, connected clients, radio environment and device radio statistics.

4.4.1 'Interfaces' submenu

The **'Interfaces'** submenu provides information about the current state of wired interfaces and wireless network settings.

To quickly switch to the configuration menu of the wired interface '*Wired Settings*' or the wireless interface '*Wireless Settings*', click on the link 'Edit' in the corresponding section.



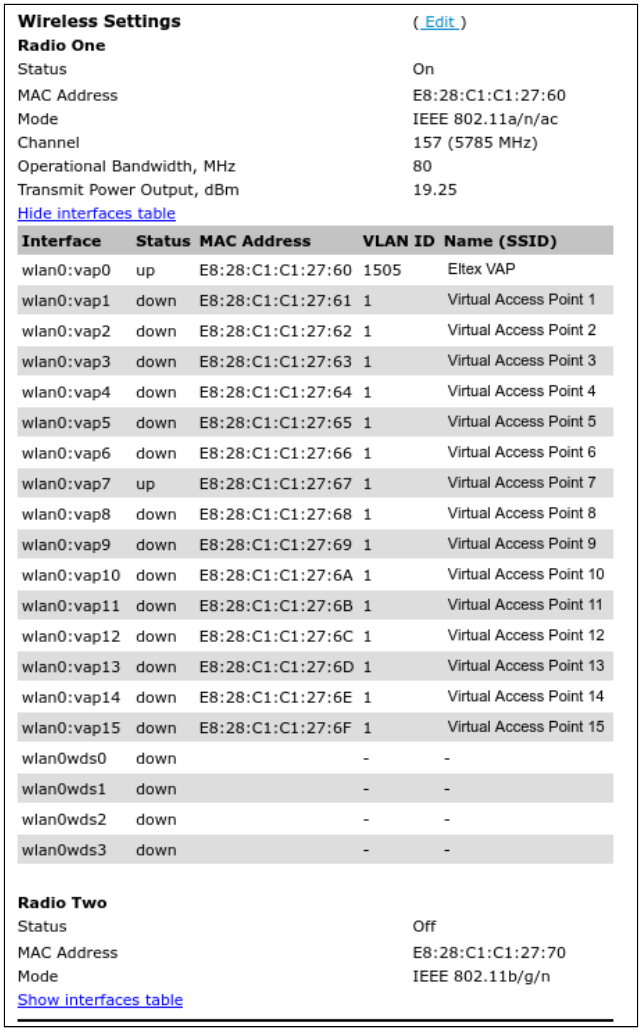
Wired Settings – provides information about the current state of the wired interface:

- *MAC Address* – MAC address of the Ethernet interface of the device;
- *VLAN ID* – VLAN number for device management;
- *IP Address* – IP address for device management;
- *Subnet Mask* – IPv4 network management mask;
- *IPv6 Address* – IPv6 network management mask;
- *IPv6 Autoconfigured Global Addresses* – the list of automatically configured IPv6 addresses;
- *IPv6 Link Local Address* – automatically configured local IPv6 address;
- *IPv6-DNS-1* – address of the first DNS server in IPv6 network;
- *IPv6-DNS-2* – address of the second DNS server in IPv6 network;

- *DNS-1* – address of the first DNS server in IPv4 network;
- *DNS-2* – address of the second DNS server in IPv4 network;
- *Default Gateway* – default gateway in IPv4 network.

Wireless Settings – provides information about the current state of wireless interfaces:

- *Radio One Status* – operation state of the first radio interface;
- *Radio Two Status* – operation state of the second radio interface;
- *MAC Address* – MAC address of the interface;
- *Mode* – radio interface operating mode according to IEEE 802.11 standards;
- *Channel* – number of the wireless channel on which the radio interface operates;
- *Operational bandwidth* – bandwidth of the channel on which the radio interface operates, MHz;
- *Transmit Power Output* – actual radiated transmitter power, dBm.



Wireless Settings (Edit)

Radio One

Status	On
MAC Address	E8:28:C1:C1:27:60
Mode	IEEE 802.11a/n/ac
Channel	157 (5785 MHz)
Operational Bandwidth, MHz	80
Transmit Power Output, dBm	19.25

Hide interfaces table

Interface	Status	MAC Address	VLAN ID	Name (SSID)
wlan0:vap0	up	E8:28:C1:C1:27:60	1505	Eltex VAP
wlan0:vap1	down	E8:28:C1:C1:27:61	1	Virtual Access Point 1
wlan0:vap2	down	E8:28:C1:C1:27:62	1	Virtual Access Point 2
wlan0:vap3	down	E8:28:C1:C1:27:63	1	Virtual Access Point 3
wlan0:vap4	down	E8:28:C1:C1:27:64	1	Virtual Access Point 4
wlan0:vap5	down	E8:28:C1:C1:27:65	1	Virtual Access Point 5
wlan0:vap6	down	E8:28:C1:C1:27:66	1	Virtual Access Point 6
wlan0:vap7	up	E8:28:C1:C1:27:67	1	Virtual Access Point 7
wlan0:vap8	down	E8:28:C1:C1:27:68	1	Virtual Access Point 8
wlan0:vap9	down	E8:28:C1:C1:27:69	1	Virtual Access Point 9
wlan0:vap10	down	E8:28:C1:C1:27:6A	1	Virtual Access Point 10
wlan0:vap11	down	E8:28:C1:C1:27:6B	1	Virtual Access Point 11
wlan0:vap12	down	E8:28:C1:C1:27:6C	1	Virtual Access Point 12
wlan0:vap13	down	E8:28:C1:C1:27:6D	1	Virtual Access Point 13
wlan0:vap14	down	E8:28:C1:C1:27:6E	1	Virtual Access Point 14
wlan0:vap15	down	E8:28:C1:C1:27:6F	1	Virtual Access Point 15
wlan0wds0	down		-	-
wlan0wds1	down		-	-
wlan0wds2	down		-	-
wlan0wds3	down		-	-

Radio Two

Status	Off
MAC Address	E8:28:C1:C1:27:70
Mode	IEEE 802.11b/g/n

Show interfaces table

When clicking the **'Show interfaces table'** link in *'Wired Settings'* and *'Wireless Settings'* sections, an interface table becomes available containing the following information:

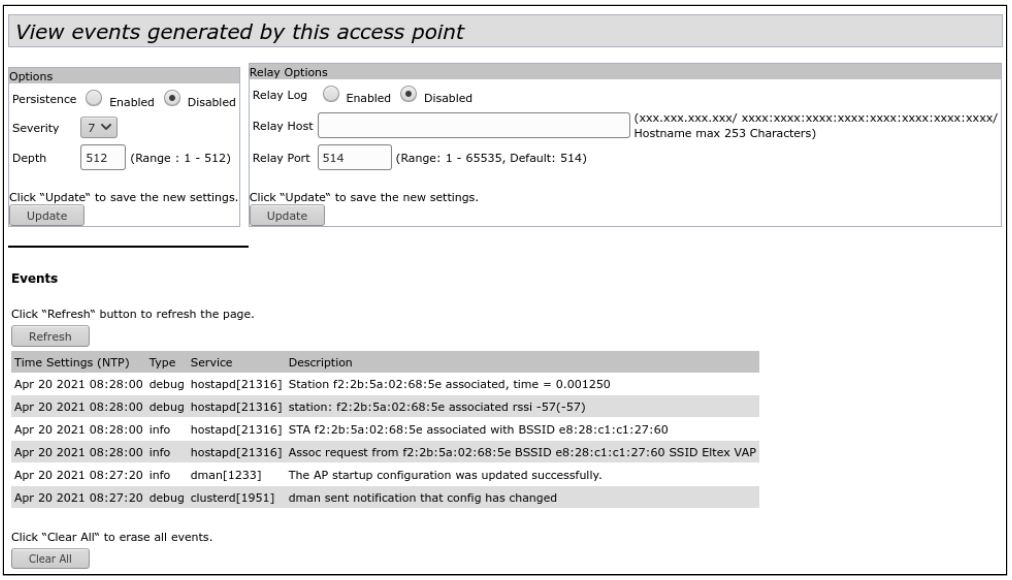
- *Interface* – name of the access point interface;
- *Status* – interface status;
- *MAC Address* – interface MAC address;
- *VLAN ID* – VLAN identifier used on the interface;
- *Name (SSID)* – wireless network name.

To hide the table, click the **'Hide interfaces table'** link.

To update information on the page, click the 'Refresh' button.

4.4.2 'Events' submenu

'Events' submenu displays a list of events that occur with the device, as well as configure event redirection to a third-party SYSLOG server.



Options – in this section, the following message log parameters can be configured: severity level and number of messages stored in the non-volatile memory of the device.

- *Persistence* – way to save informational messages:
  - *Enabled* – when this flag is set, log events will be saved to non-volatile memory.
  - *Disabled* – when this flag is set, the events will be saved in volatile memory. Messages in volatile memory will be cleared when the system is rebooted.
- *Severity* – the severity level of the message to be saved in non-volatile memory. Description of severity levels is given in table below.

Table 5 – Description of event severity categories

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 on the system
3	error	an error has occurred on the system
4	warning	warning, non-emergency message
5	notice	system notice, non-emergency message
6	informational	informational system message
7	debug	debugging messages provide the user with information to correctly configure the system

- *Depth* – maximum number of messages that can be stored in volatile memory. When this threshold is exceeded, the message that is stored in the system the longest is overwritten with a new message. The parameter takes values in the range from 1 to 512. The default value is 512.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

Relay Options – in this section, sending informational messages from the device to a third-party server is configured.

- *Relay Log* – enable/disable sending informational messages from the device to a third-party server:
  - *Enabled* – when the flag is set, sending is enabled;
  - *Disabled* – when the flag is set, sending is disabled.
- *Relay Host* – the address of the server to which the messages are redirected. The IPv4 address, IPv6 address, or domain name of the remote server can be set.
- *Relay Port* – number of the port (layer 4), to which messages are redirected. The parameter may take values in range from 1 to 65535. Default value – 514.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

Events – in this section, a list of real-time information messages containing the following information can be viewed:

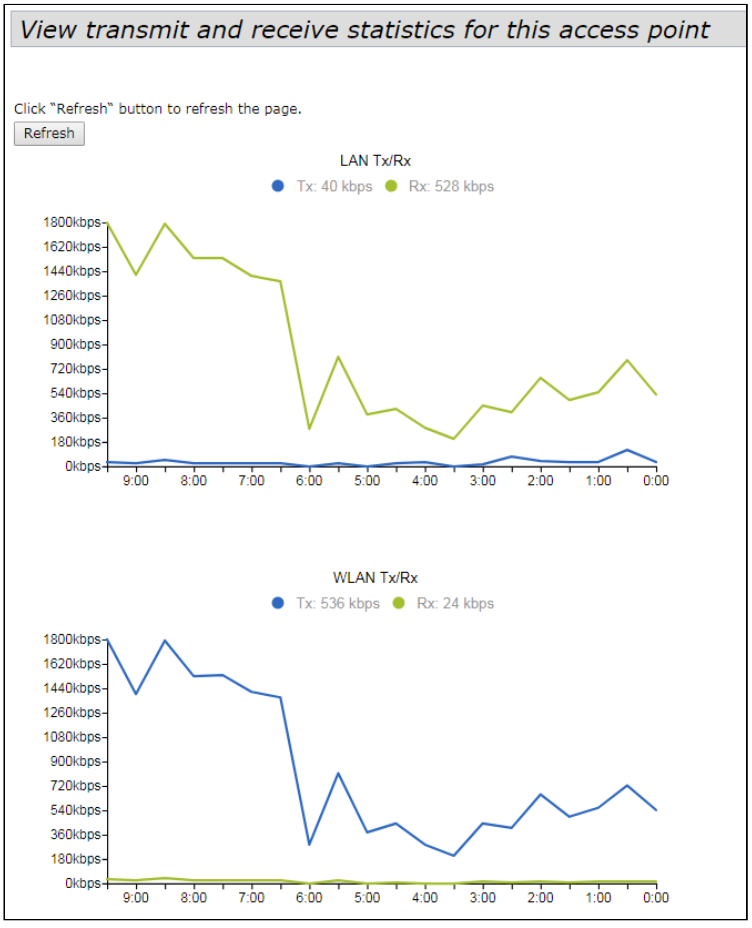
- *Time Setting (NTP)* – time when event was generated;
- *Type* – event severity level (table 5);
- *Service* – the name of the process that generated the message;
- *Description* – event description.

To update information in the 'Events' section, click 'Refresh'.

To clear all messages, click 'Clear All'.

4.4.3 'Transmit/Receive' submenu

In the **'Transmit/Receive'** submenu graphs of the speed of receiving/transmitting traffic for the last 10 minutes are displayed, as well as information on the amount of transmitted/received traffic since the access point was turned on.



'Transmit/Receive' graphs description

The LAN Tx/Rx diagram displays the speed of the transmitted/received traffic via the access point's Ethernet interface over the last 10 minutes. The diagram is automatically updated every 30 seconds.
The WLAN Tx/Rx displays the speed of transmitted/received traffic via radio interfaces of the access point over the last 10 minutes. The diagram is automatically updated every 30 seconds.

Transmit

Interface	Total packets	Total bytes	Total Drop Packets	Total Drop Bytes	Errors
LAN	8715267	1529876381	0	0	0
isatap0	0	0	0	0	0
wlan0:vap0	5163390	4117748340	0	0	0
wlan0:vap1	0	0	0	0	0
wlan0:vap2	29704	11964655	0	0	0
wlan0:vap3	196384	58061993	2050	3094107	0
wlan0:vap4	0	0	0	0	0
wlan0:vap5	0	0	0	0	0
wlan0:vap6	11045	9274028	0	0	0
wlan0:vap7	0	0	0	0	0
wlan0:vap8	0	0	0	0	0
wlan0:vap9	0	0	0	0	0
wlan0:vap10	0	0	0	0	0
wlan0:vap11	0	0	0	0	0
wlan0:vap12	0	0	0	0	0
wlan0:vap13	0	0	0	0	0
wlan0:vap14	0	0	0	0	0
wlan0:vap15	0	0	0	0	0
wlan1:vap0	0	0	0	0	0
wlan1:vap1	313121	415719017	0	0	0
wlan1:vap2	7473043	10448367916	576124	869642147	0
wlan1:vap3	1563879	745541384	0	0	0

'Transmit' table description:

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

Receive

Interface	Total packets	Total bytes	Total Drop Packets	Total Drop Bytes	Errors
LAN	20095269	17273106147	28727	0	16
isatap0	0	0	0	0	0
wlan0:vap0	1589456	244114016	0	0	0
wlan0:vap1	0	0	0	0	0
wlan0:vap2	6437	814291	0	0	0
wlan0:vap3	39272	6695565	0	0	0
wlan0:vap4	0	0	0	0	0
wlan0:vap5	0	0	0	0	0
wlan0:vap6	4486	434660	0	0	0
wlan0:vap7	0	0	0	0	0
wlan0:vap8	0	0	0	0	0
wlan0:vap9	0	0	0	0	0
wlan0:vap10	0	0	0	0	0
wlan0:vap11	0	0	0	0	0
wlan0:vap12	0	0	0	0	0
wlan0:vap13	0	0	0	0	0
wlan0:vap14	0	0	0	0	0
wlan0:vap15	0	0	0	0	0
wlan1:vap0	0	0	0	0	0
wlan1:vap1	282058	21248406	0	0	0
wlan1:vap2	5041611	714677115	3525	4954835	0
wlan1:vap3	482182	69990869	0	0	0

'Receive' table description:

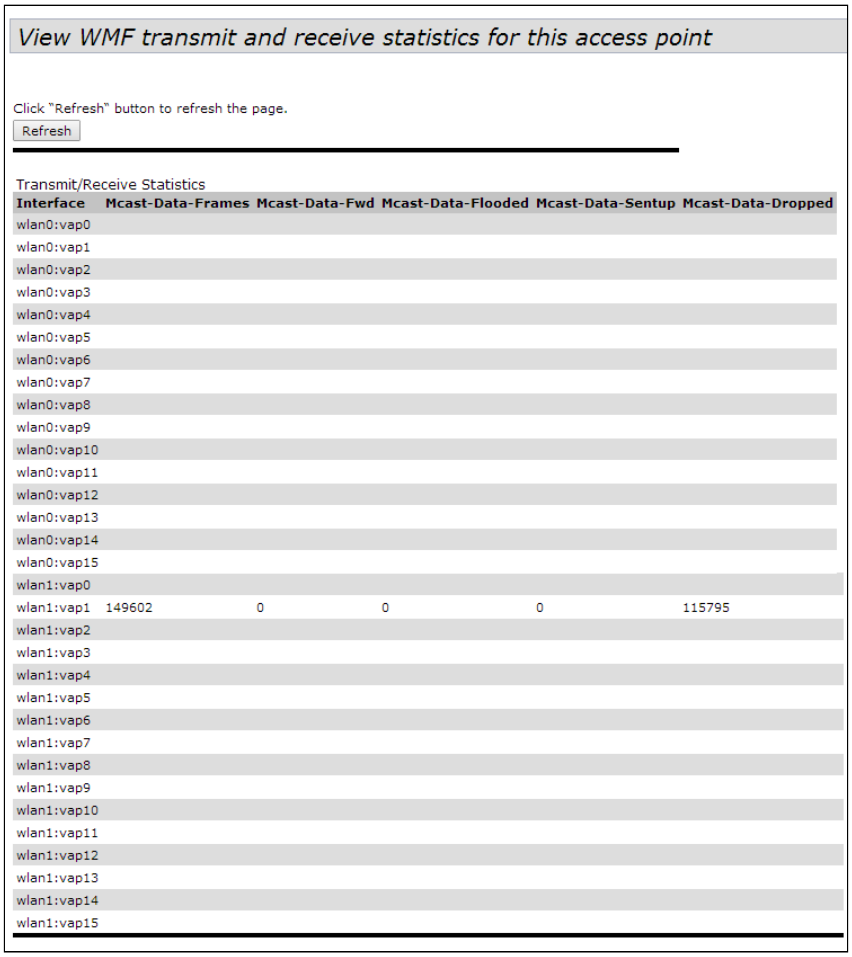
- *Interface* – name of the interface;
- *Total packets* – number of successfully received packets;
- *Total bytes* – number of successfully received bytes;

- *Total Drop Packets* – number of packets dropped on receipt;
- *Total Drop Bytes* – number of bytes dropped on receipt;
- *Errors* – number of errors.

To update information on the page, click 'Refresh'.

4.4.4 'Wireless Multicast Forwarding Statistic' submenu

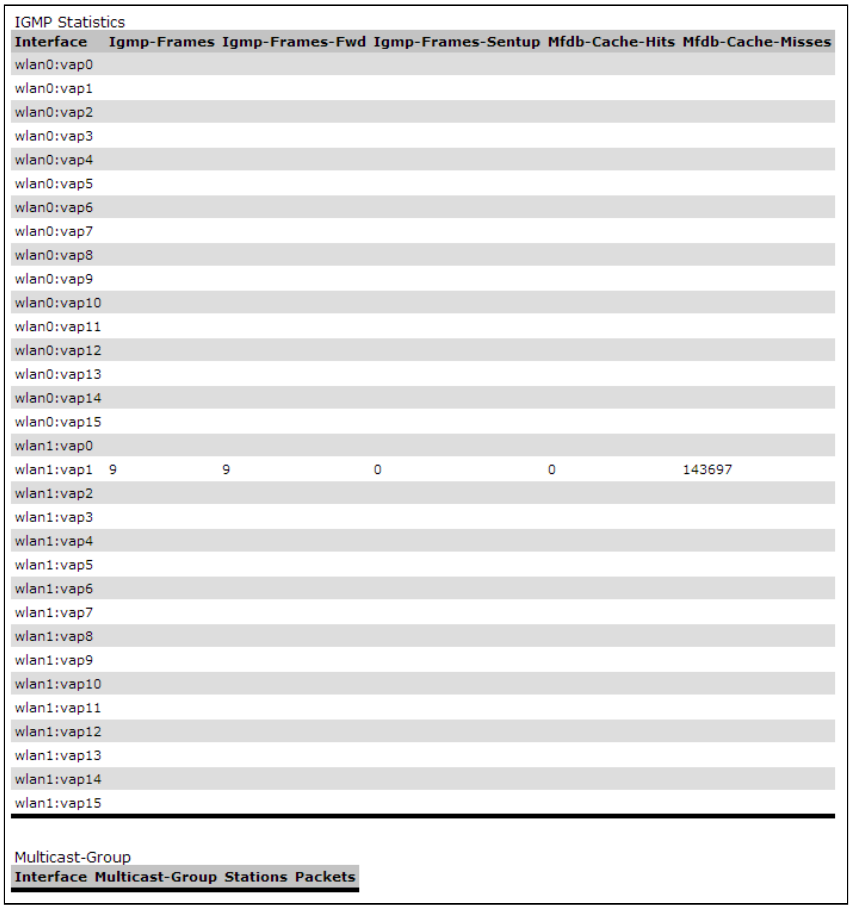
In the '**Wireless Multicast Forwarding Statistic**' submenu statistics on the operation of Wireless Multicast Forwarding is displayed.



Interface	Mcast-Data-Frames	Mcast-Data-Fwd	Mcast-Data-Flooded	Mcast-Data-Sentup	Mcast-Data-Dropped
wlan0:vap0					
wlan0:vap1					
wlan0:vap2					
wlan0:vap3					
wlan0:vap4					
wlan0:vap5					
wlan0:vap6					
wlan0:vap7					
wlan0:vap8					
wlan0:vap9					
wlan0:vap10					
wlan0:vap11					
wlan0:vap12					
wlan0:vap13					
wlan0:vap14					
wlan0:vap15					
wlan1:vap0					
wlan1:vap1	149602	0	0	0	115795
wlan1:vap2					
wlan1:vap3					
wlan1:vap4					
wlan1:vap5					
wlan1:vap6					
wlan1:vap7					
wlan1:vap8					
wlan1:vap9					
wlan1:vap10					
wlan1:vap11					
wlan1:vap12					
wlan1:vap13					
wlan1:vap14					
wlan1:vap15					

'Transmit/Receive Statistics' table description:

- *Interface* – name of the interface.
- *Mcast-Data-Frames* – number of the multicast frames received by access point;
- *Mcast-Data-Fwd* – number of the multicast frames received by clients;
- *Mcast-Data-Flooded* – number of the multicast frames sent to all ports;
- *Mcast-Data-Sentup* – number of the multicast frames sent;
- *Mcast-Data-Dropped* – number of the multicast frames dropped.



IGMP Statistics

Interface	Igmp-Frames	Igmp-Frames-Fwd	Igmp-Frames-Sentup	Mfdb-Cache-Hits	Mfdb-Cache-Misses
wlan0:vap0					
wlan0:vap1					
wlan0:vap2					
wlan0:vap3					
wlan0:vap4					
wlan0:vap5					
wlan0:vap6					
wlan0:vap7					
wlan0:vap8					
wlan0:vap9					
wlan0:vap10					
wlan0:vap11					
wlan0:vap12					
wlan0:vap13					
wlan0:vap14					
wlan0:vap15					
wlan1:vap0					
wlan1:vap1	9	9	0	0	143697
wlan1:vap2					
wlan1:vap3					
wlan1:vap4					
wlan1:vap5					
wlan1:vap6					
wlan1:vap7					
wlan1:vap8					
wlan1:vap9					
wlan1:vap10					
wlan1:vap11					
wlan1:vap12					
wlan1:vap13					
wlan1:vap14					
wlan1:vap15					

Multicast-Group

Interface	Multicast-Group	Stations	Packets

'IGMP Statictics' table description:

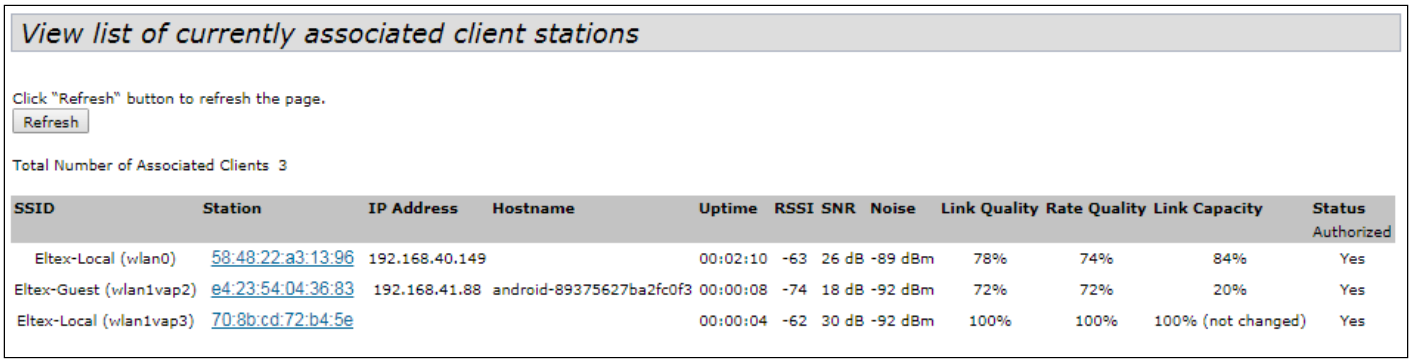
- *Interface* – name of the interface;
- *Igmp-Frames* – number of IGMP frames received by access point;
- *Igmp-Frames-Fwd* – number of IGMP frames received by clients;
- *Igmp-Frames-Sentup* – number of IGMP frames sent to all ports;
- *Mfdb-Cache-Hits* – number of packets sent to known multicast address;
- *Mfdb-Cache-Misses* – number of packets sent to unknown multicast address.

'Multicast-Group' table description:

- *Interface* – name of the interface;
- *Multicast-Group* – IP address of the multicast group;
- *Stations* – MAC address of the multicast group client;
- *Packets* – number of received packets of multicast group clients.

4.4.5 'Client Associations' submenu

In the **'Client Associations'** submenu information about clients connected to the access point and statistics of transmitted/received traffic for each client is displayed.



View list of currently associated client stations

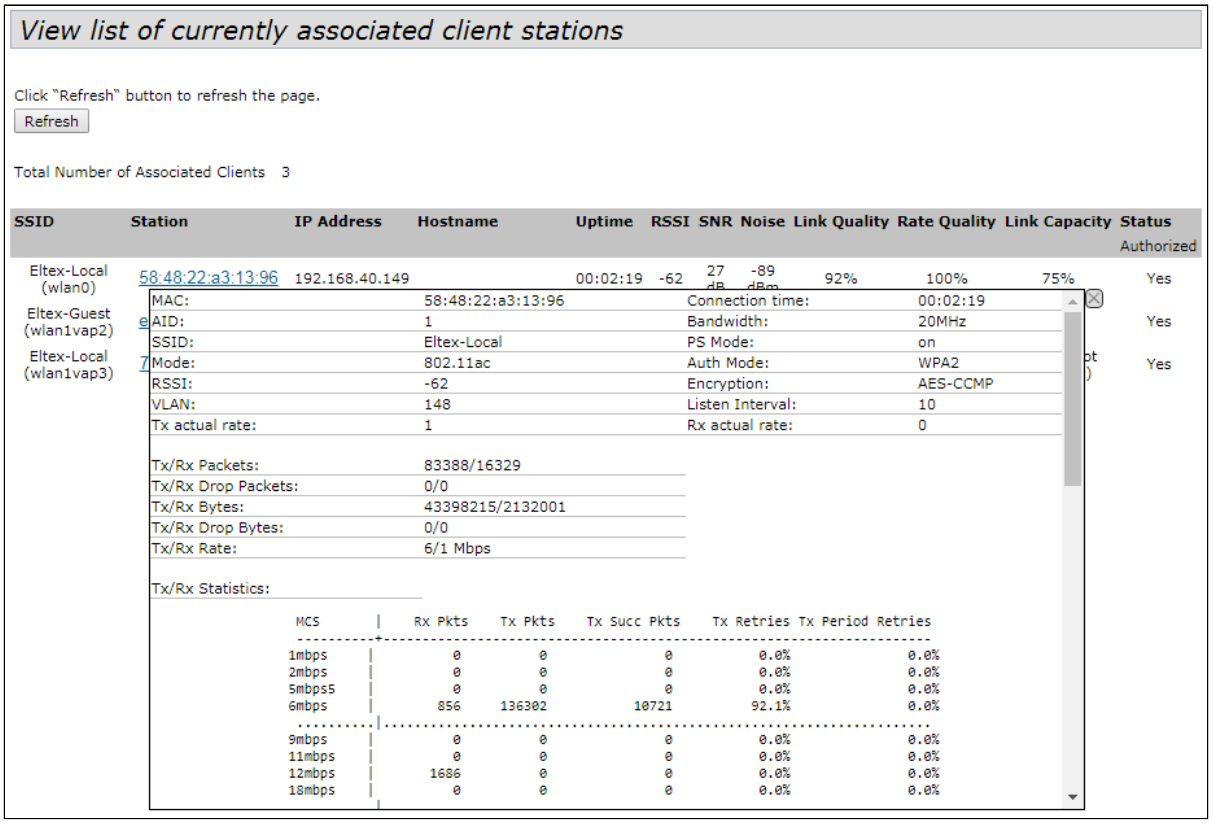
Click "Refresh" button to refresh the page.
Refresh

Total Number of Associated Clients 3

SSID	Station	IP Address	Hostname	Uptime	RSSI	SNR	Noise	Link Quality	Rate Quality	Link Capacity	Status Authorized
Eltex-Local (wlan0)	58:48:22:a3:13:96	192.168.40.149		00:02:10	-63	26 dB	-89 dBm	78%	74%	84%	Yes
Eltex-Guest (wlan1vap2)	e4:23:54:04:36:83	192.168.41.88	android-89375627ba2fc0f3	00:00:08	-74	18 dB	-92 dBm	72%	72%	20%	Yes
Eltex-Local (wlan1vap3)	70:8b:cd:72:b4:5e			00:00:04	-62	30 dB	-92 dBm	100%	100%	100% (not changed)	Yes

- *SSID* – wireless interface name and virtual access point name on the interface to which the client is connected. For example, wlan0vap2 means that the client is associated with Radio 1 VAP2; the entry wlan1 means that the client is associated with VAP0 on Radio2;
- *Station* – MAC address of the client;
- *IP Address* – IP address of the client;
- *Hostname* – device network name;
- *Uptime* – duration of the client session;
- *RSSI* – received signal level, dBm;
- *SNR* – signal/noise ratio, dB;
- *Noise* – noise level, dBm;
- *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);
- *Rate Quality* – parameter that displays the status of the link to the client, calculated based on the number of retransmit packets sent to the client for the modulation that is currently in use. The maximum value is 100% (all transmitted packets on this modulation were sent on the first attempt), the minimum value is 0% (none of the packets on this modulation to the client was successfully sent);
- *Link Capacity* – parameter that reflects the effectiveness of the use of a modulation access point on the transmission. It is calculated based on the number of packets transmitted on each modulation to the client, and the reduction factors. The maximum value is 100% (means that all packets are transmitted to the client at maximum modulation for the maximum nss type supported by the client). The minimum value is 2% (in the case when the packets are transmitted to the modulation nss1mcs0 for a client with MIMO 3x3 support). For clients connected without using AMPDU, the parameter is not supported;
- *Status Authorized* – authorization status.

Clicking on the MAC address of a client reveals detailed information about its operation and statistics of transmitted/received traffic for this client.



- *MAC* – MAC address of the client;
- *AID* – unique connection identifier;
- *SSID* – name of the network to which the client is connected;
- *Mode* – IEEE 802.11 standard in which the client operates;
- *RSSI* – signal level from the client, dBm;
- *VLAN* – VLAN number of the virtual access point;
- *Tx actual rate* – current data transfer rate towards the client, kbps;
- *Tx/Rx Packets* – number of packets sent and received from the client;
- *Tx/Rx Drop Packets* – number of dropped packets in both directions (for transmission and reception);
- *Tx/Rx Bytes* – number of transmitted and received information (in bytes);
- *Tx/Rx Drop Bytes* – number of dropped information in both directions (for transmission and reception, in bytes);
- *Tx/Rx Rate* – channel rate in two directions, Mbps;
- *Connection time* – session duration;
- *Bandwidth* – channel bandwidth, on which the client operates, MHz;
- *PS Mode* – sleep mode: off – the client is up, on – the client is in sleep mode;
- *Auth Mode* – security type;
- *Encryption* – encryption type;
- *Listen Interval* – number of beacon frames after which the client should check for traffic for (in case of sleep);
- *Rx actual rate* – current data transfer rate towards the access point, kbps.

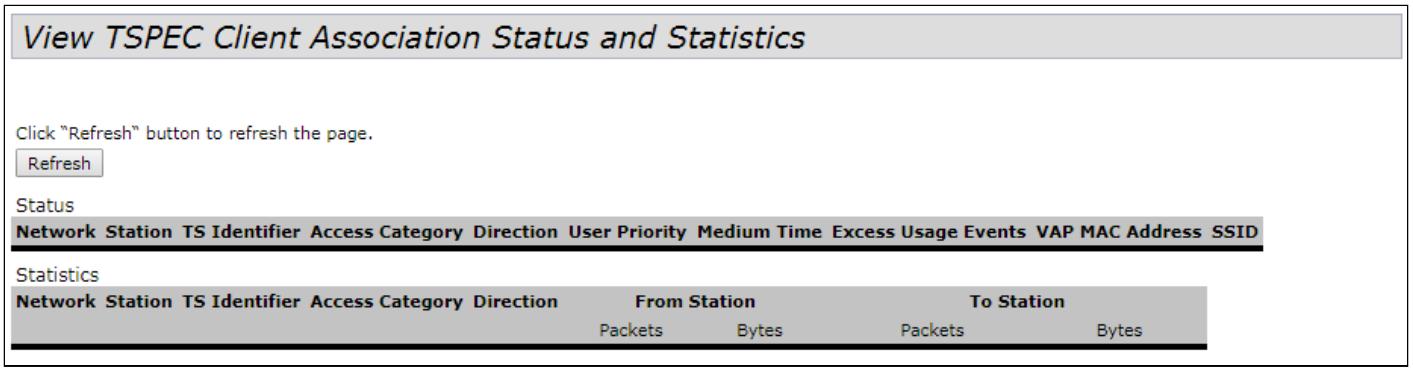
'Tx/Rx Statistics' table description:

- *MCS* – modulation;
- *Rx Pkts* – number of packets received from the client on each modulation;
- *Tx Pkts* – number of packets transmitted to the client on each modulation;
- *Tx Succ Pkts* – number of packets successfully transmitted to the client;
- *Tx Retries* – percentage of duplicated packets towards the client;
- *Tx Period Retries* – percentage of retransmitted packets in the last period (10 seconds).

To update information on the page, click 'Refresh'.

4.4.6 'TSPEC Client Associations' submenu

In the '**TSPEC Client Associations**' submenu information about client Tspec data transmitted and received using this access point is displayed.

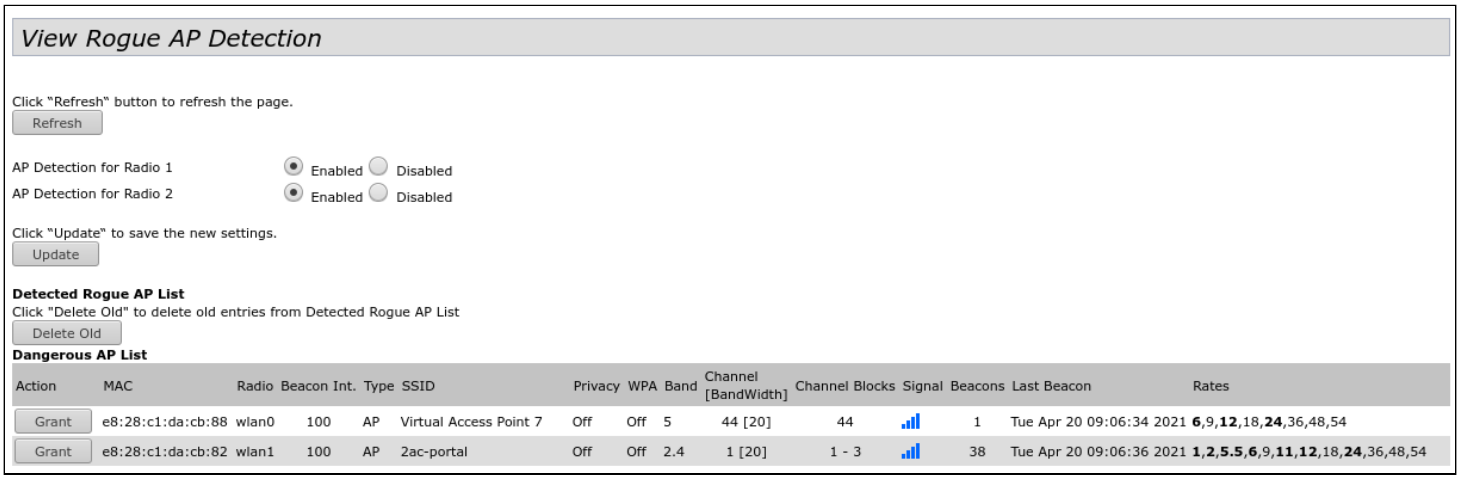


- *Network* – wireless interface name and name of the virtual access point on the interface the client is connected to. For example, wlan0vap2 entry means that the client is associated with Radio1 through VAP2 virtual access point; wlan1 entry means that the client is associated with VAP0 on Radio2;
- *Station* – MAC address of the client;
- *TS Identifier* – TSPEC traffic flow identifier. May take values from 0 to 7;
- *Access Category* – access category (Voice or Video);
- *Direction* – traffic direction (Uplink/Downlink/Bidirectional);
- *User Priority* – user priority;
- *Medium Time* – average time that a traffic flow occupies a transmission medium;
- *Excess Usage Events* – amount of time the client exceeded the average transfer time;
- *VAP* – number of the virtual access point;
- *MAC Address* – MAC address of the access point;
- *SSID* – name of the wireless network;
- *From Station* – information about traffic transmitted from wireless client to access point;
- *To Station* – information about the traffic transmitted from access point to client:
    - *Packets* – number of transmitted packets;
    - *Bytes* – number of transmitted bytes.

To update information on the page, click 'Refresh'.

4.4.7 'Rogue AP Detection' submenu

In the **'Rogue AP Detection'** submenu, information about all wireless access points that the device detects in its network is displayed.



To update information on the page, click 'Refresh'.

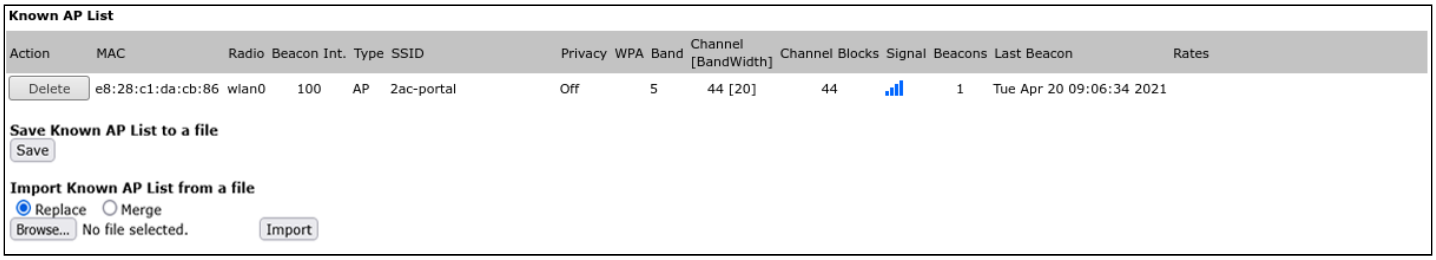
- *AP Detection for Radio 1/AP Detection for Radio 2* – enable detection of third-party access points in the background for Radio1 and Radio2.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

Detected Rogue AP List – this section provides information about all wireless access points that the device detects in its network.

Button 'Delete Old' is used to delete records of inactive devices in a radio environment.

- *Action* – if access point is in the list of discovered, then clicking 'Grant' button will transfer it to the list of trusted access points 'Known AP List';
- *MAC* – MAC address of the access point;
- *Radio* – radio interface that was used to discover rogue access point;
- *Beacon Int.* – interval for sending a beacon packet by access point;
- *Type* – type of detected device:
  - *AP* – access point;
  - *Ad hoc* – decentralized client device.
- *SSID* – name of the wireless network;
- *Privacy* – access point security mode operation status:
  - *On* – security mode is disabled;
  - *Off* – security mode is enabled.
- *WPA* – WPA encryption state: Off – disabled, On – enabled;
- *Band* – frequency spectrum of the access point: 2.4 GHz or 5 GHz;
- *Channel [BandWidth]* – used frequency channel and bandwidth;
- *Channel Blocks* – range of channels used by the access point;
- *Signal* – signal level received from the access point, dBm. Hovering the pointer over a graphical representation of a signal displays the numerical indicators of this signal;
- *Beacons* – total number of beacon packets received from the access point since it was discovered;
- *Last Beacon* – date and time when the last beacon packet was received from the access point;
- *Rates* – list of channel rates supported by this access point.



Known AP List – the table lists the trusted access points.

To remove access point from the black list, click 'Delete', after removing from the 'Known AP List', access point will be added to the list of detected access points.

Save Known AP List to a file – in this section, 'Known AP List' is saved to the file. To save click 'Save'.

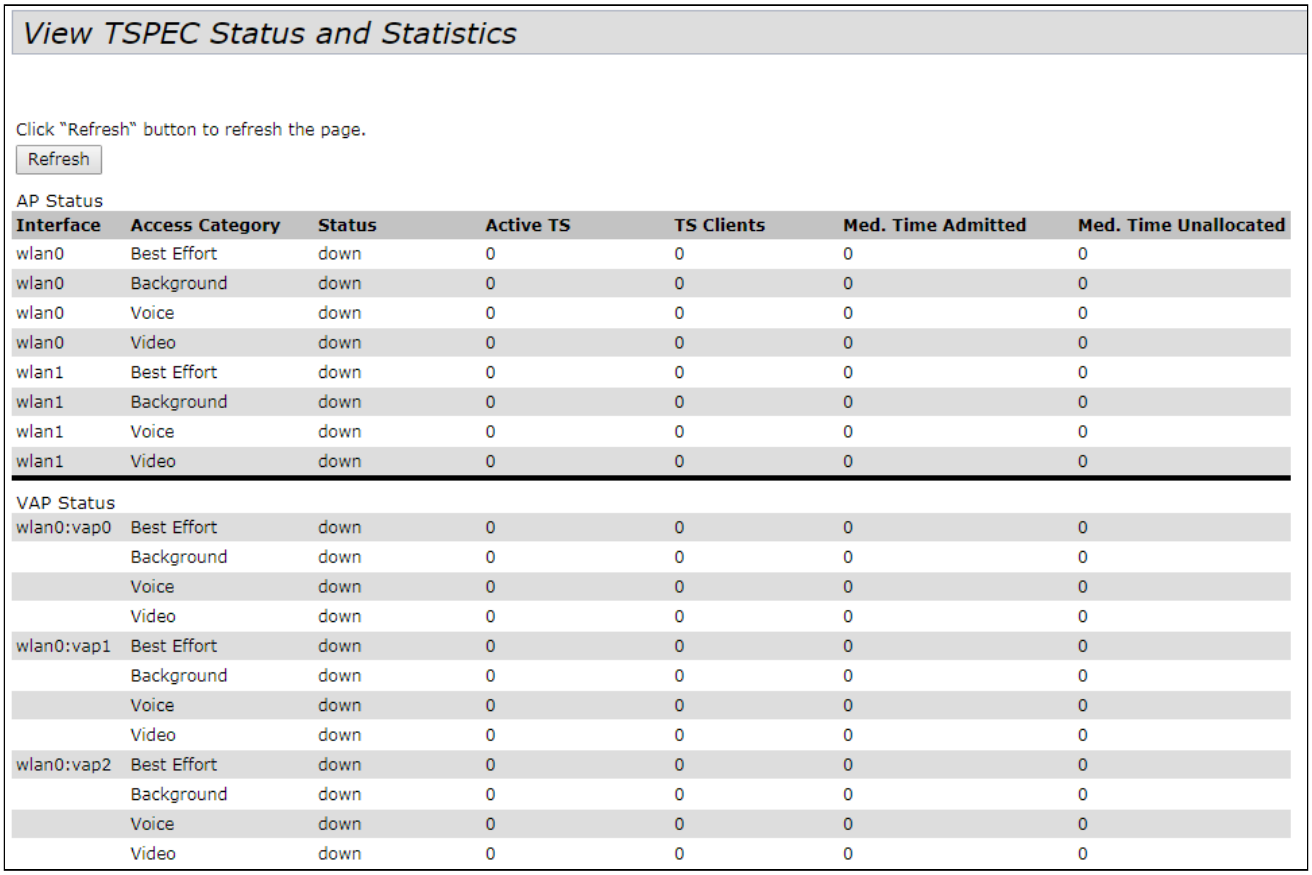
Import Known AP List from a file – in this section, 'Known AP List' is loaded from file.

- *Replace* – imported list of trusted access points will completely replace the current list of trusted access points;
- *Merge* – trusted access points from the imported list will be added to access points currently in the imported list.

To load the file, click 'Browse', select a file to upload and click 'Import'.

4.4.8 'TSPEC Status and Statistics' submenu

In the '**TSPEC Status and Statistics**' submenu, information about TSPEC sessions on radio interfaces is displayed.



Interface	Access Category	Status	Active TS	TS Clients	Med. Time Admitted	Med. Time Unallocated
wlan0	Best Effort	down	0	0	0	0
wlan0	Background	down	0	0	0	0
wlan0	Voice	down	0	0	0	0
wlan0	Video	down	0	0	0	0
wlan1	Best Effort	down	0	0	0	0
wlan1	Background	down	0	0	0	0
wlan1	Voice	down	0	0	0	0
wlan1	Video	down	0	0	0	0
wlan0:vap0	Best Effort	down	0	0	0	0
	Background	down	0	0	0	0
	Voice	down	0	0	0	0
	Video	down	0	0	0	0
wlan0:vap1	Best Effort	down	0	0	0	0
	Background	down	0	0	0	0
	Voice	down	0	0	0	0
	Video	down	0	0	0	0
wlan0:vap2	Best Effort	down	0	0	0	0
	Background	down	0	0	0	0
	Voice	down	0	0	0	0
	Video	down	0	0	0	0

'AP Status' and 'VAP Status' tables description:

- *Interface* – name of the interface;
- *Access Category* – access category (Voice, Video, Best Effort, Background);
- *Status* – session status;
- *Active TS* – number of current active traffic flows;
- *TS Clients* – number of clients;
- *Medium Time Admitted* – average time that a traffic flow occupies a transmission medium;
- *Medium Time Unallocated* – average band idle time in this category.

Transmit

Radio	Access Category	Total Packets	Total Bytes
wlan0	Best Effort	0	0
wlan0	Background	0	0
wlan0	Voice	0	0
wlan0	Video	0	0
wlan1	Best Effort	0	0
wlan1	Background	0	0
wlan1	Voice	0	0
wlan1	Video	0	0

Interface	Total Voice Packets	Total Voice Bytes	Total Video Packets	Total Video Bytes	Total Best Effort Packets	Total Best Effort Bytes	Total Background Packets	Total Background Bytes
wlan0:vap0	0	0	0	0	0	0	0	0
wlan0:vap1	0	0	0	0	0	0	0	0
wlan0:vap2	0	0	0	0	0	0	0	0
wlan0:vap3	0	0	0	0	0	0	0	0
wlan0:vap4	0	0	0	0	0	0	0	0
wlan0:vap5	0	0	0	0	0	0	0	0
wlan0:vap6	0	0	0	0	0	0	0	0
wlan0:vap7	0	0	0	0	0	0	0	0
wlan0:vap8	0	0	0	0	0	0	0	0
wlan0:vap9	0	0	0	0	0	0	0	0
wlan0:vap10	0	0	0	0	0	0	0	0
wlan0:vap11	0	0	0	0	0	0	0	0
wlan0:vap12	0	0	0	0	0	0	0	0
wlan0:vap13	0	0	0	0	0	0	0	0
wlan0:vap14	0	0	0	0	0	0	0	0
wlan0:vap15	0	0	0	0	0	0	0	0
wlan1:vap0	0	0	0	0	0	0	0	0
wlan1:vap1	0	0	0	0	0	0	0	0

'Transmit' table description:

- *Radio* – name of the radio interface;
- *Access Category* – access category (Voice, Video, Best Effort, Background);
- *Total Packets* – total number of packets of this access category sent by radio interface;
- *Total Bytes* – total number of bytes of this access category sent by radio interface;
- *Interface* – number of the virtual access point;
- *Total Voice Packets* – total number of packets of Voice category sent from this VAP;
- *Total Voice Bytes* – total number of bytes of Voice category sent from this VAP;
- *Total Video Packets* – total number of packets of Video category sent from this VAP;
- *Total Video Bytes* – total number of bytes of Video category sent from this VAP;
- *Total Best Effort Packets* – total number of packets of Best Effort category sent from this VAP;
- *Total Best Effort Bytes* – total number of bytes of Best Effort category sent from this VAP;
- *Total Background Packets* – total number of packets of Background category sent from this VAP;
- *Total Background Bytes* – total number of bytes of Background category sent from this VAP.

Receive

Radio	Access Category	Total Packets	Total Bytes
wlan0	Best Effort	0	0
wlan0	Background	0	0
wlan0	Voice	0	0
wlan0	Video	0	0
wlan1	Best Effort	0	0
wlan1	Background	0	0
wlan1	Voice	0	0
wlan1	Video	0	0

Interface	Total Voice Packets	Total Voice Bytes	Total Video Packets	Total Video Bytes	Total Best Effort Packets	Total Best Effort Bytes	Total Background Packets	Total Background Bytes
wlan0:vap0	0	0	0	0	0	0	0	0
wlan0:vap1	0	0	0	0	0	0	0	0
wlan0:vap2	0	0	0	0	0	0	0	0
wlan0:vap3	0	0	0	0	0	0	0	0
wlan0:vap4	0	0	0	0	0	0	0	0
wlan0:vap5	0	0	0	0	0	0	0	0
wlan0:vap6	0	0	0	0	0	0	0	0
wlan0:vap7	0	0	0	0	0	0	0	0
wlan0:vap8	0	0	0	0	0	0	0	0
wlan0:vap9	0	0	0	0	0	0	0	0
wlan0:vap10	0	0	0	0	0	0	0	0
wlan0:vap11	0	0	0	0	0	0	0	0
wlan0:vap12	0	0	0	0	0	0	0	0
wlan0:vap13	0	0	0	0	0	0	0	0
wlan0:vap14	0	0	0	0	0	0	0	0
wlan0:vap15	0	0	0	0	0	0	0	0
wlan1:vap0	0	0	0	0	0	0	0	0
wlan1:vap1	0	0	0	0	0	0	0	0

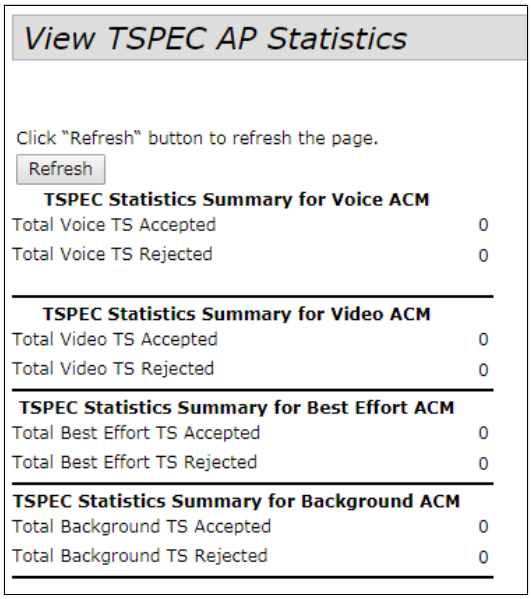
'Receive' table description:

- *Radio* – name of the radio interface;
- *Access Category* – access category (Voice, Video, Best Effort, Background);
- *Total Packets* – total number of packets of this access category received by radio interface;
- *Total Bytes* – total number of bytes of this access category received by radio interface;
- *Interface* – number of the virtual access point;
- *Total Voice Packets* – total number of packets of Voice category received on this VAP;
- *Total Voice Bytes* – total number of bytes of Voice category received on this VAP;
- *Total Video Packets* – total number of packets of Video category received on this VAP;
- *Total Video Bytes* – total number of bytes of Video category received on this VAP;
- *Total Best Effort Packets* – total number of packets of Best Effort category received on this VAP;
- *Total Best Effort Bytes* – total number of bytes of Best Effort category received on this VAP;
- *Total Background Packets* – total number of packets of Background category received on this VAP;
- *Total Background Bytes* – total number of bytes of Background category received on this VAP.

To update information on the page, click 'Refresh'.

4.4.9 'TSPEC AP Statistics' submenu

In the '**TSPEC AP Statistics**' submenu, statistics on the number of transmitted/received traffic flows of various categories is displayed (Voice, Video, Best Effort, Background).

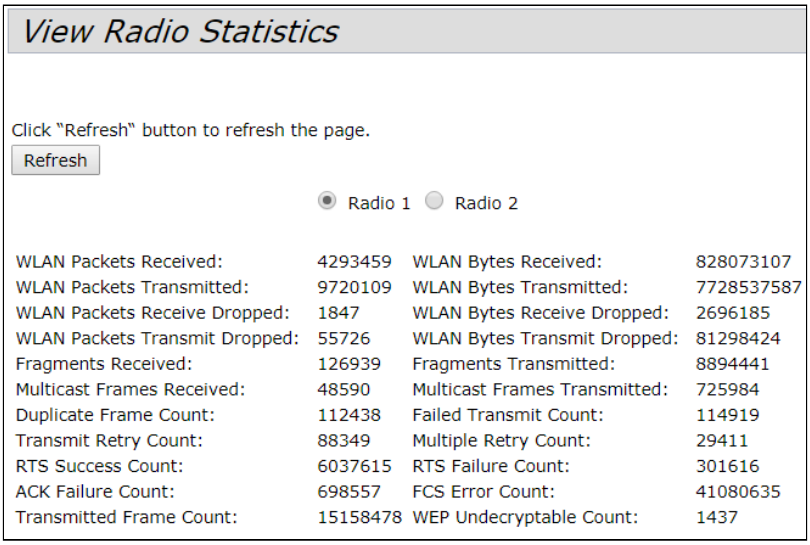


- *TSPEC Statistics Summary for Voice ACM* – total number of accepted and rejected traffic flows of the Voice category;
- *TSPEC Statistics Summary for Video ACM* – total number of accepted and rejected traffic flows of the Video category;
- *TSPEC Statistics Summary for Best Effort ACM* – total number of accepted and rejected traffic flows of the Best Effort category;
- *TSPEC Statistics Summary for Background ACM* – total number of accepted and rejected traffic flows of the Background category.

To update information on the page, click 'Refresh'.

4.4.10 'Radio Statistics' submenu

In the '**Radio Statistics**' submenu detailed information about packets and bytes transmitted/received over the wireless interface is displayed.



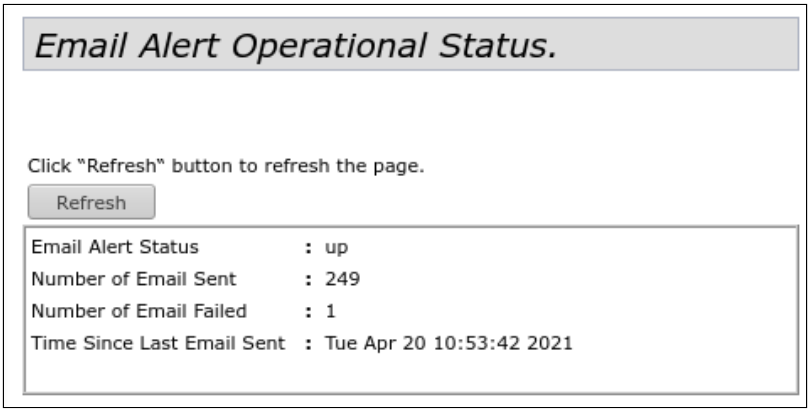
Set the flag next to the name of the radio interface for which detailed information should be displayed (Radio 1 or Radio 2):

- *WLAN Packets Received* – total number of packets received by the access point through this radio interface;
- *WLAN Bytes Received* – total number of bytes received by the access point through this radio interface;
- *WLAN Packets Transmitted* – total number of packets transmitted by the access point through this radio interface;
- *WLAN Bytes Transmitted* – total number of bytes transmitted by the access point through this radio interface;
- *WLAN Packets Receive Dropped* – number of packets received by the access point through this radio interface that were dropped;
- *WLAN Bytes Receive Dropped* – number of bytes received by the access point through this radio interface that were dropped;
- *WLAN Packets Transmit Dropped* – number of packets transmitted by the access point through this radio interface that were dropped;
- *WLAN Bytes Transmit Dropped* – number of bytes transmitted by the access point through this radio interface that were dropped;;
- *Fragments Received* – number of received packets fragments;
- *Fragments Transmitted* – number of transmitted packets fragments;
- *Multicast Frames Received* – number of received multicast frames;
- *Multicast Frames Transmitted* – number of transmitted multicast frames;
- *Duplicate Frame Count* – number of duplicate frames;
- *Failed Transmit Count* – number of packets not transmitted due to error;
- *Transmit Retry Count* – number of resent packets;
- *Multiple Retry Count* – number of packets resent multiple times;
- *RTS Success Count* –number of confirmation packets of readiness to receive traffic (CTS);
- *RTS Failure Count* – number of packets that did not receive confirmation of readiness to receive (CTS);
- *ACK Failure Count* – number of packets that did not receive confirmation of successful reception (ACK);
- *FCS Error Count* – number of frames that failed the checksum check;
- *Transmitted Frame Count* – number of successfully transmitted frames;
- *WEP Undecryptable Count* – number of packets that failed to decrypt (WEP).

To update information on the page, click 'Refresh'.

4.4.11 'Email Alert Status' submenu

In the '**Email Alert Status**' submenu information about sent e-mail messages generated based on the event log is displayed.
Messages sending can be configured in the 'Email Alert' submenu located in the 'Services' menu.



- *Email Alert Status* – status of the e-mail notification on the device operation:
  - *Up* – notification is enabled;
  - *Down* – notification is disabled.

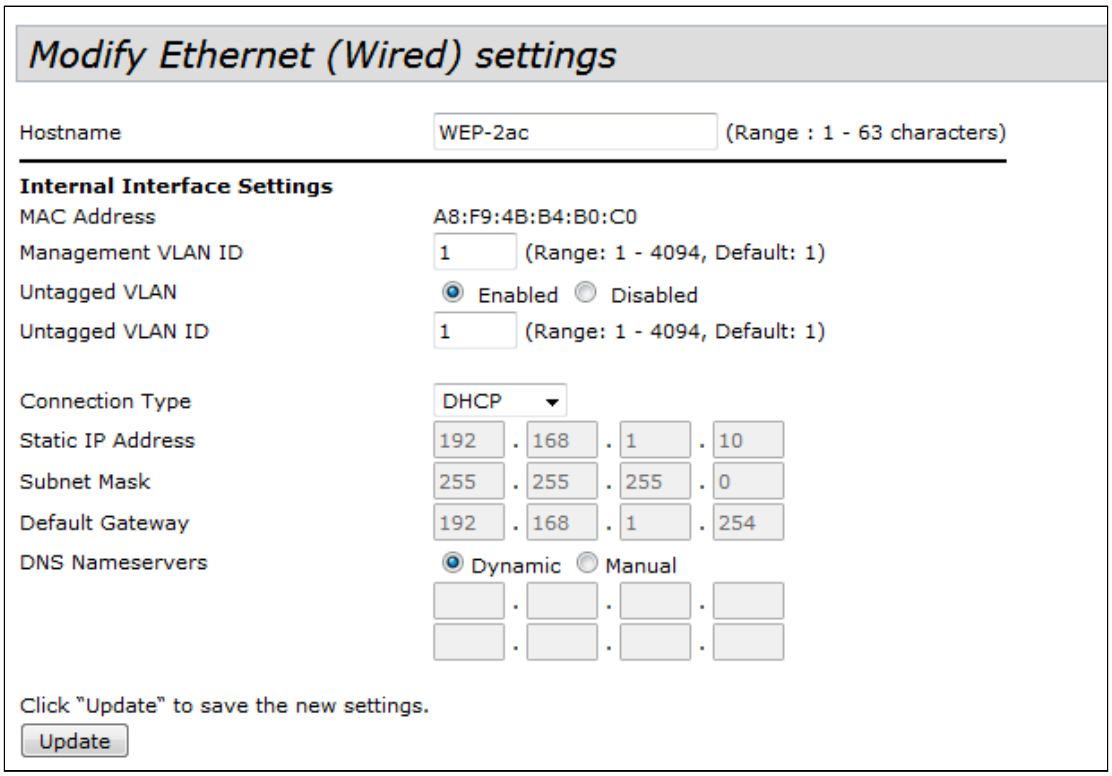
- *Number of Email Sent* – total number of messages sent at the moment;
- *Number of Email Failed* – total number of messages failed at the moment;
- *Time Since Last Email Sent* – date and time the last message was sent.

To update information on the page, click 'Refresh'.

4.5 'Manage' menu

4.5.1 'Ethernet Settings' submenu

In the '**Ethernet Settings**' submenu network settings of the device are performed.



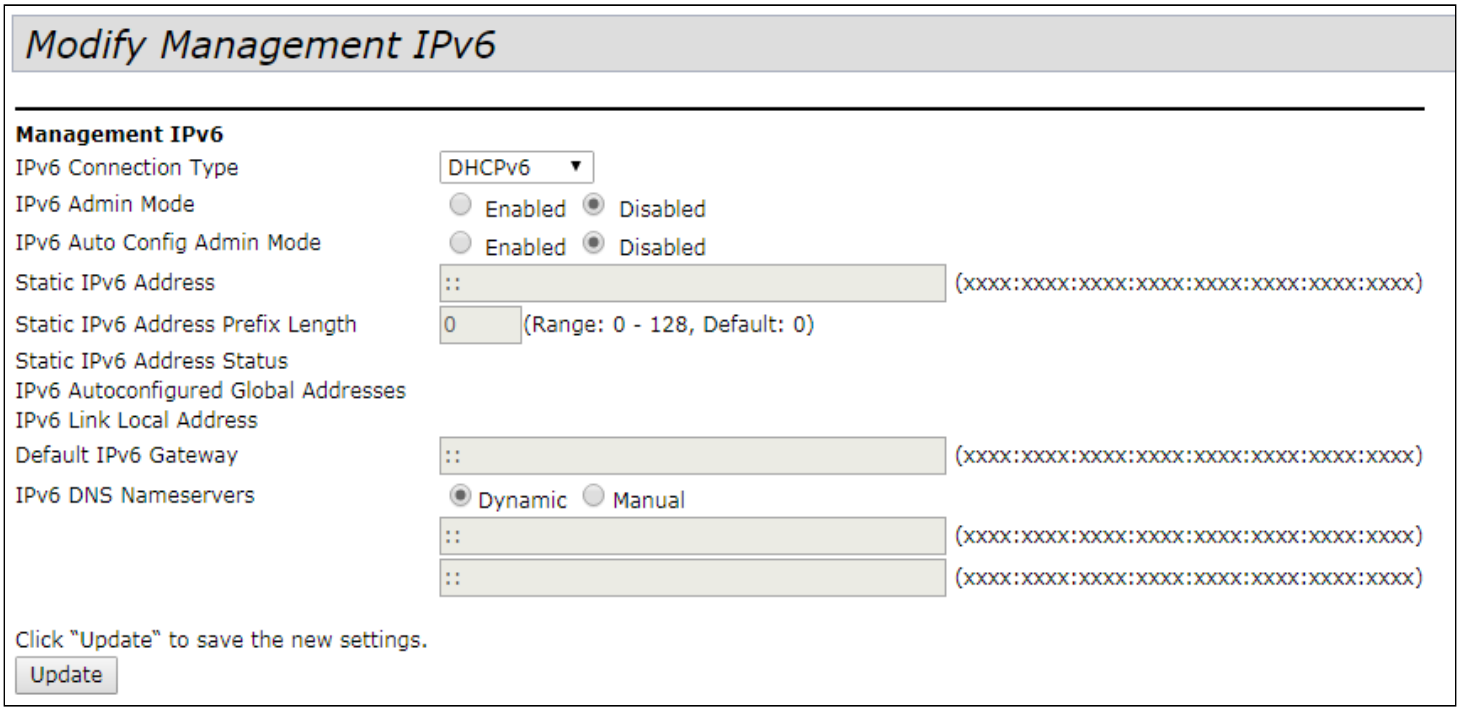
- *Hostname* – network name of the device. May contain from 1 to 63 characters and consist of Latin uppercase and lowercase letters, numbers, hyphen '-' (the hyphen cannot be the last character in the device network name);
- *MAC Address* – MAC address of the device Ethernet interface;
- *Management VLAN ID* – VLAN identifier used to access the device. May take values from 1 to 4094. By default – 1;
- *Untagged VLAN* – switch LAN ports to access mode, in which a VLAN tag is added for incoming untagged traffic and removed from outgoing:
  - *Enabled* – enable access mode for LAN ports;
  - Disabled – disable access mode for LAN ports.
- *Untagged VLAN ID* – VLAN identifier that will be assigned to untagged traffic received on the device and removed from outgoing traffic. May take values from 1 to 4094. By default – 1;
- *Connection Type* – selection of the method for setting IP address on the management interface which will be used to connect the WAN interface of the device to the carrier's service network:
  - *DHCP* – operating mode when IP address, subnet, DNS server address, default gateway and other parameters required for networking will be obtained from the DHCP server automatically;
  - *Static IP* – operating mode when IP address and all parameters required for networking assigned to WAN interface statically. When selecting the 'Static IP' type, the following parameters will become available for editing:
    - *Static IP Address* – IP address of the device in carrier's network;

- *Subnet Mask* – external subnet mask;
- *Default Gateway* – IP address to which the packet is sent if no route is found for it in the routing table;
- *DNS Nameservers* – domain name server addresses (used to determine IP address of the device from its domain name):
  - *Dynamic* – DNS servers obtained via DHCP will be used;
  - *Manual* – DNS servers have to be manually specified.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

4.5.2 'Management IPv6' submenu

In the '**Management IPv6'** submenu IPv6 address for device management access is configured.



- *IPv6 Connection Type* – choice of using static (Static IPv6) or dynamic (DHCPv6) IPv6 address of the device;;
- *IPv6 Admin Mode* – access to the device via IPv6 protocol:
  - *Enable* – access is allowed;
  - *Disable* – access is denied.
- *IPv6 Auto Config Admin Mode* – IPv6 address configuration mode:
  - *Enable* – used;
  - *Disable* – not used.

When setting '*Static IPv6*' type in '*IPv6 Connection Type*' parameter, the following parameters will become available for editing:

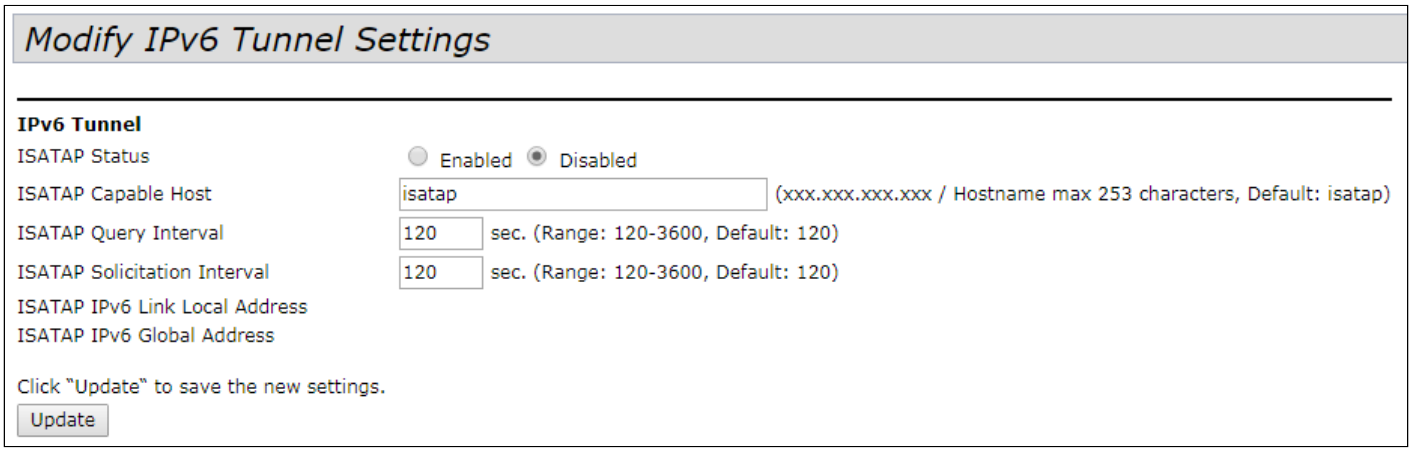
- *Static IPv6 Address* – static IPv6 address of the device. Access point can have a static IPv6 address, even if the addresses have already been configured automatically through 'Auto Config';
- *Static IPv6 Address Prefix Length* – static IPv6 address prefix. May take value from 0 to 128. By default – 0;
- *Static IPv6 Address Status* – view status of statically configured IPv6 address. The parameter takes the following values:
  - *Operational* – current operational;
  - *Tentative* – backup.
- *IPv6 Autoconfigured global Addresses* – list of valid IPv6 addresses on the device;

- *IPv6 Link Local Address* – local IPv6 address set on LAN interface. This address is not configurable and is assigned automatically;
- *Default IPv6 Gateway* – default gateway for IPv6;
- *IPV6 DNS Nameservers* – domain name server addresses (used to determine the IP address of a device from its domain name):
  - *Dynamic* – DNS servers obtained via DHCP will be used;
  - *Manual* – DNS servers have to be specified manually.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

4.5.3 'IPv6 Tunnel' submenu

In the **'IPv6 Tunnel'** submenu IPv6 tunneling inside IPv4 is configured. ISATAP protocol is used (Intra-Site Automatic Tunnel Addressing Protocol – intra-site tunneling protocol). The ISATAP protocol encapsulates IPv6 packets into IPv4 packets for transmission over an IPv4 network. Support for this functionality allows the device to communicate with remote IPv6 hosts.



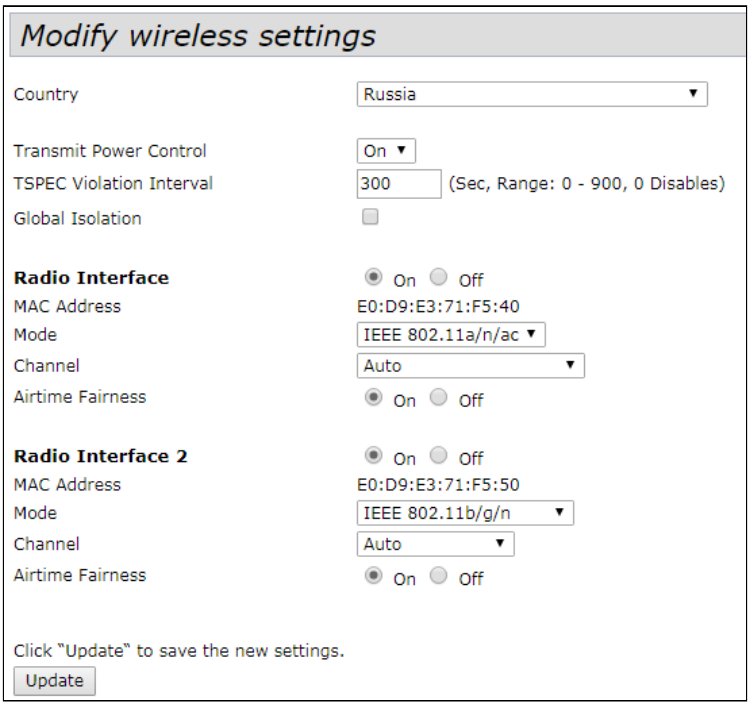
- *ISATAP Status* – ISATAP operating mode:
  - *Enabled* – operation via ISATAP is allowed;
  - *Disabled* – operation via ISATAP is denied.
- *ISATAP Capable Host* – IP address or DNS name of ISATAP router. Value – isatap;
- *ISATAP Query Interval* – time interval between DNS queries. May take value from 120 to 3600 seconds. By default – 120 seconds;
- *ISATAP Solicitation Interval* – time interval between ISATAP router poll messages. May take value from 120 to 3600 seconds. By default – 120 seconds;
- *ISATAP IPv6 Link Local Address* – local IPv6 address of the device;
- *ISATAP IPv6 Global Address* – global IPv6 address of the device.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

4.5.4 'Wireless Settings' submenu

In the **'Wireless Settings'** submenu, wireless Wi-Fi network is configured. The device has 2 independent physical radio interfaces, each of which operates in its own mode and range. Radio 1 operates in 5 GHz, Radio 2 in 2.4 GHz.

This section of the menu provides separate settings for each radio interface.



- *Country* – name of the country where access point operates. Depending on the value set, the frequency band and transmitter power restrictions applicable in that country will be applied. The list of available frequency channels depends on the set country, which affects the automatic channel selection in the Channel = Auto mode. If the client equipment is licensed for use in another region, it will not be possible to establish a connection with the access point.

  Selecting the wrong region can lead to compatibility issues with different client devices.

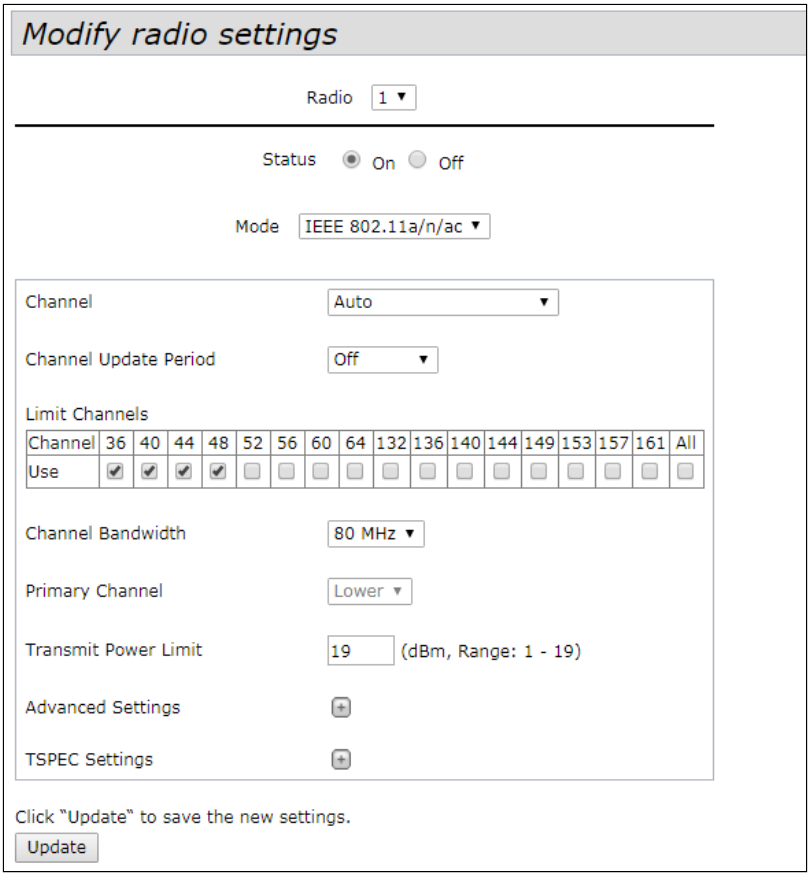
- *Transmit Power Control* – setting the limit mode of the Transmit Power Limit parameter (the parameter available for Russia):
  - *On* – maximum EIRP value is limited in accordance with the legislation of the Russian Federation and does not exceed 100 mW (16 dBm transmitter power for the 2.4 GHz band, 19 dBm transmitter power for the 5 GHz band);
  - *Off* – maximum EIRP value is limited by the physical characteristics of the transmitter. For WEP-2ac and WEP-2ac Smart maximum EIRP value for the 2.4 GHz band – 18 dBm, for 5 GHz band – 21 dBm.
- *TSPEC Violation Interval* – time interval, in seconds, for which the access point should report via the event log or SNMP trap about attached clients that do not support the required admission procedures. May take value from 0 to 900 seconds. By default – 300 seconds;
- *Global Isolation* – when checked, traffic isolation between clients of different VAP and different radio interfaces is enabled;
- *Radio Interface* – radio interface status:
  - *On* – when the flag is set, radio interface is active;
  - *Off* – when the flag is set, radio interface is disabled.
- *MAC Address* – MAC address of the radio interface;
- *Mode* – selection of the wireless interface operating mode according to IEEE 802.11 standards;

- *Channel* – channel number for wireless network operation. When 'auto' is selected, a channel with a lower level of interference is automatically detected;
- *Airtime Fairness* – radio accessibility function:
  - *On* – when the flag is set, the function is active. Airtime is evenly distributed among users;
  - *Off* – the function is disabled.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

4.5.5 'Radio' submenu

In the **'Radio'** submenu, advanced settings of the wireless Wi-Fi network are performed for each radio interface.



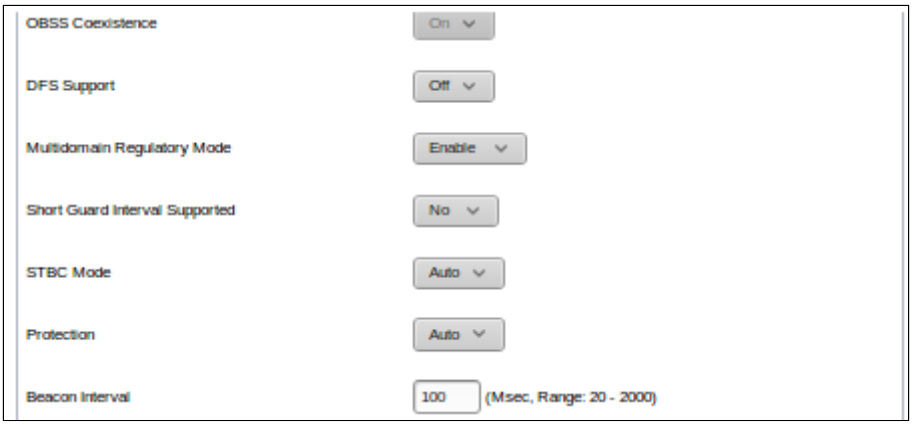
- *Radio* – wireless Wi-Fi interface selection. Radio 1 operates in 5 GHz band, Radio 2 operates in 2.4 GHz band;
- *Status* – state of configured Wi-Fi interface:
  - *On* – when the Wi-Fi flag is set, the interface is enabled;
  - *Off* – when the Wi-Fi flag is set, the interface is disabled.
- *Mode* – selection of the wireless interface operating mode according to IEEE 802.11 standards.
  - For Radio 1, operating in 5 GHz:
    - *IEEE 802.11a* – 5 GHz frequency band, maximum transmission rate is 54Mbps;
    - *IEEE 802.11a/n/ac* – 5 GHz frequency band, maximum transmission rate is 866 Mbps;
    - *IEEE 802.11n/ac* – 5 GHz frequency band, maximum transmission rate is 866 Mbps. Only IEEE 802.11n/ac compatible clients can be connected.
  - For Radio 2, operating in 2.4 GHz:
    - *IEEE 802.11b/g* – 2.4 GHz frequency band, maximum transmission rate is 54 Mbps;
    - *IEEE 802.11b/g/n* – 2.4 GHz frequency band, maximum transmission rate is 300 Mbps;
    - *2.4 GHz IEEE 802.11n* – 2.4 GHz frequency band, maximum transmission rate is 300 Mbps. Only IEEE 802.11n compatible clients can be connected.

- *Channel* – radio channel selection for Wi-Fi interface operation. When 'auto' is selected, a channel with a lower level of interference is automatically detected (taking into account selected region), which runs the least number of access points;
- *Channel Update Period* – time period after which the optimal channel will be automatically selected;
- *Limit Channels* – list of channels from which the access point can choose the best channel for operating in the 'Auto' mode;
- *Channel Bandwidth* – channel bandwidth;
- *Primary Channel* – the parameter can only be changed if the bandwidth of a statically specified channel is equal to 40 MHz.The 40 MHz channel can be considered as consisting of two 20 MHz channels, which border in the frequency range. These two 20 MHz channels are called primary and secondary channels. The primary channel is used by IEEE 802.11n clients which support only 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* – transmitting Wi-Fi signal power adjustment, dBm.
  - When *Transmit Power Control* is enabled, the parameter may take the following values:
    - in 2.4 GHz frequency range (Radio 2) – from 8 to 16, by default – 16;
    - in 5 GHz frequency range (Radio 1) on WEP-2ac – from 1 to 19, on WEP-2ac Smart – from 11 to 19, by default – 19.
  - When *Transmit Power Control* is disabled, the parameter may take the following values:
    - in 2.4 GHz frequency range (Radio 2) – from 8 to 18, by default – 18;
    - in 5 GHz frequency range (Radio 1) on WEP-2ac – from 1 to 21, on WEP-2ac Smart – from 11 to 21, by default – 21.

Wi-Fi client devices may not support some frequency channels. If there is no information about the channels supported by clients, it is recommended to assign frequency channels 1-11 for the 2.4 GHz band and 36-48 for the 5 GHz band.

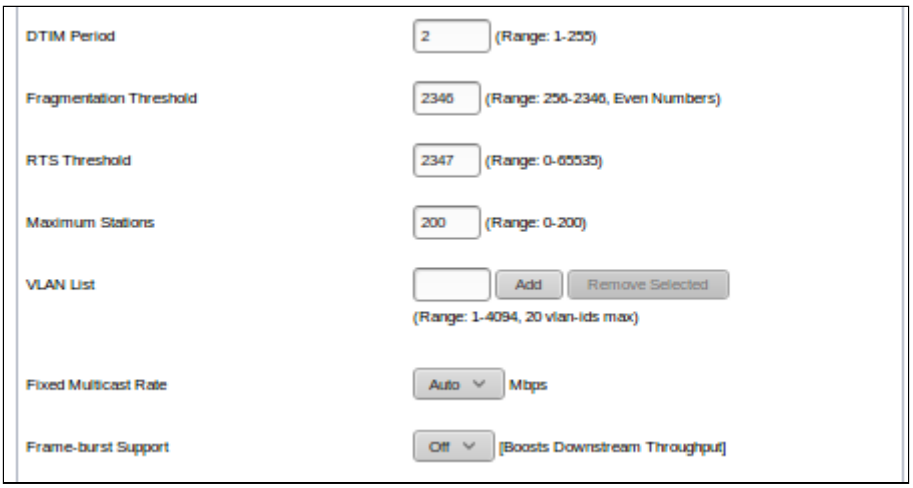
When setting a frequency channel from the DFS band 52-144, the Wi-Fi interface will be turned on after 1 minute.

To go to the extended parameters list, click the button with the '+' symbol next to 'Advanced settings':

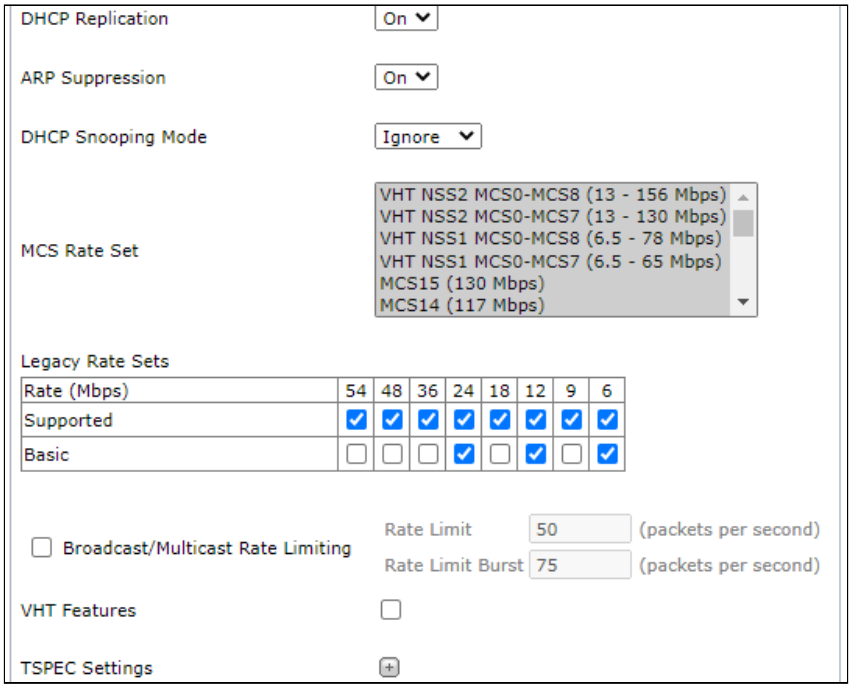


- *OBSS Coexistence* – mode of automatic change of channel width from 40 MHz to 20 MHz when radio is loaded:
  - *On* – the mode is enabled;
  - *Off* – the mode is disabled.
- *DFS Support* – dynamic frequency selection mechanism. he mechanism demands wireless devices to scan environment and avoid using channels which coincide with radiolocation system's channels at 5 GHz. The field is available for editing only in the settings of the Radio 1 interface operating in the 5 GHz frequency band. The parameter may take the following values:
  - *On* – DFS support is enabled;
  - *Off* – DFS support is disabled.

- *Multidomain Regulatory Mode* – the mode of information transmission by the device about the set region in Beacon frame service messages:
  - *Enable* – the mode is enabled;
  - *Disable* – the mode is disabled.
- *Short Guard Interval Supported* – support for Short Guard Interval. Reducing the guard interval increases throughput. The field is available for editing when selected radio interface operating mode includes the IEEE 802.11n standard. The parameter may take the following values:
  - *Yes* – access point transmits data using a 400 ns guard interval when communicating with clients that also support a short guard interval;
  - *No* – access point transmits data using a 800 ns guard interval;
- *STBC Mode* – method of space-time block coding aimed at improving the reliability of data transmission. The field is available for editing when selected radio interface operating mode includes the IEEE 802.11n standard. The parameter may take the following values:
  - *Yes* – the device transmits one data flow through several antennas;
  - *No* – the device does not transmit one data flow through several antennas.
- *Protection* – inter-station interference prevention operating mode:
  - *Auto* – the mode is enabled;
  - *Off* – the mode is disabled.
- *Beacon Interval* – beacon frames transmission period. The frames are sent to detect access points. The parameter may take values from 20 to 2000 ms. By default – 100 ms.



- *DTIM Period* – time interval before sending a signal to a wireless client in sleep mode to indicate that a data packet is awaiting delivery. The parameter may take values from 1 to 255 ms. By default – 2 ms;
- *Fragmentation Threshold* – frame fragmentation threshold in bytes. The parameter may take values from 256 to 2346. By default – 2346;
- *RTS Threshold* – specifies the number of bytes over which the transfer request is sent (Request to Send). Decreasing this value may improve the performance of the access point when there are a large number of connected clients, but it reduces the overall throughput of the wireless network. The parameter may take values from 0 to 2347. By default – 2347;
- *Maximum Stations* – maximum allowable number of clients connected to radio interface. The parameter may take values from 0 to 200. By default – 200;
- *VLAN List* – list of VLANs allowed to broadcast (used in conjunction with VlanTrunk mode on VAP). VLAN List setting is used if more than one VLAN needs to be transmitted towards the client device. The setting is relevant for the VAP–VlanTrunk operating mode. Maximum number of VLANs that can be specified in the list– 20;
- *Fixed Multicast Rate* – selection of a fixed transmission rate for multicast traffic. If 'Auto' is selected, speed selection is automatic;
- *Frame-burst Support* – mode to increase downstream throughput.



- *DHCP Replication* – replication of DHCP packets towards the client:
  - *On* – unicast;
  - *Off* – broadcast.
- *ARP Suppression* – ARP request conversion mechanism from Broadcast to Unicast;
- *DHCP Snooping Mode* – option 82 processing policy control:
  - *Ignore* – option 82 processing is disabled on the access point. Set by default;
  - *Remove* – access point deletes option 82 value;
  - *Replace* – access point substitutes or replaces option 82 value. When this value is set, the following parameters become available for editing:
    - *DHCP Option 82 CID Format:*
      - *String* – access point changes the contents of the Circuit-ID to a value that is manually configured in the 'DHCP Option 82 CID String' field;
      - *APMAC-SSID* – access point changes the contents of the Circuit-ID to entry of the <MAC address of the access point> type; <name of the SSID to which the client is connected>. Set by default;
      - *SSID* – access point changes the contents of the Circuit-ID to the SSID the client is connected to.
    - *DHCP Option 82 CID String* – value from 1 to 52 characters which will be transmitted in the Circuit-ID if 'String' is specified in the 'DHCP Option 82 CID Format' parameter. Only Latin letters and numbers are allowed, and '.', '-', '_' characters;

      If 'DHCP Option 82 CID Format' is set to 'String' and the 'DHCP Option 82 CID String' field is left blank, then the access point will change the contents of the Circuit-ID to the default value: 'APMAC-SSID'.

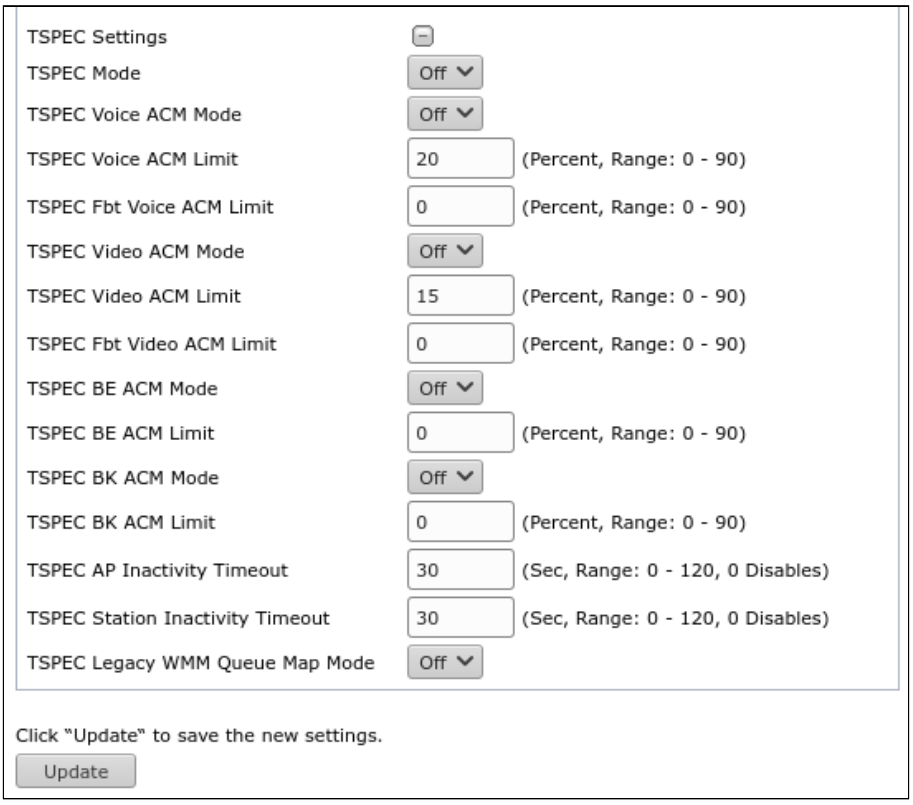
    - *DHCP Option 82 RID Format:*
      - *String* – access point changes the contents of the Remote-ID to the value that is configured manually in the 'DHCP Option 82 RID String' field;
      - *ClientMAC* – access point changes the contents of the Remote-ID to MAC address of the client device. Default value;
      - *APMAC* – access point changes the contents of the Remote-ID to its MAC address;
      - *APdomain* – access point changes the contents of the Remote-ID to the name of the last domain in the tree, specified in the AP-Location parameter in the device settings.

- *DHCP Option 82 RID String* – value from 1 to 63 characters, which will be sent to Remote-ID if in 'DHCP Option 82 RID Format' parameter 'String' is specified. Only Latin letters and numbers are allowed, and '.', '-', '_' characters.

  If 'DHCP Option 82 CID Format' is set to 'String' and the 'DHCP Option 82 CID String' field is left blank, then the access point will change the contents of the Circuit-ID to the default value: 'ClientMAC'.

- *DHCP Option 82 MAC Format* – parameter defines the format of MAC addresses that are sent to CID and RID. May take values:
  - *default* – MAC address is sent in the usual format, the same as in the 'Client-Ethernet-Address' option of the DHCP packet. In this case, the MAC address is usually in lower case letters and the separator is ':', for example 'aa:bb:cc:dd:ee:ff'. In the packet, it will be sent in ASCII encoding. The value is set by default;
  - *radius* – MAC address is sent in the RADIUS format. In this case, all letters are converted to uppercase, and '-' acts as a separator. Example 'AA-BB-CC-DD-EE-FF'. In the packet, it will be sent in ASCII encoding.

- *MCS Rate Set* – selection of supported wireless data transmission channel rates determined by IEEE 802.11n/ac standards specifications;
- *Legacy Rate Sets* – supported and broadcast by the access point sets of channel rates;
- *Broadcast/Multicast Rate Limit* – when the flag is set, the transmission of broadcast/multicast traffic over the wireless network is restricted. When the flag is set, the following fields become available for editing:
  - *Rate Limit* – data transfer rate threshold, pps. By default – 50 pps.;
  - *Rate Limit Burst* – maximum value of traffic burst, pps. By default – 75 pps.
- *VHT Features* – enable/disable support for VHT rates. VHT feature enables support for 256QAM. Supported for the IEEE 802.11ac standard.



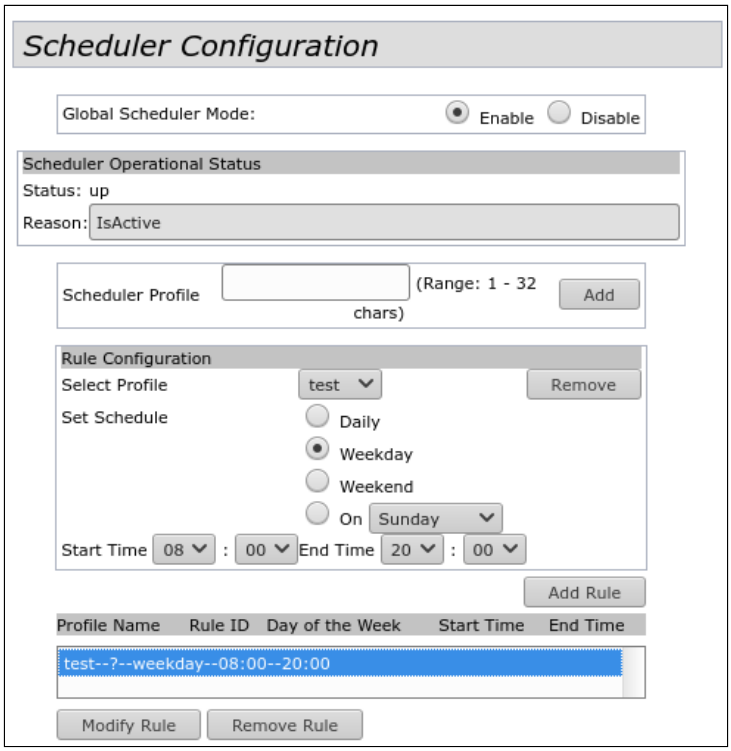
To go to the TSPEC settings, click the button with the '+' symbol next to 'TSPEC Settings':

- *TSPEC Mode* – selection of TSPEC operating mode. By default – off (disabled). May take the following values:
  - *On* – access point processes TSPEC requests from clients. Use this setting if the access point handles traffic from QoS-compliant devices such as certified Wi-Fi phones.
  - *Off* – access point ignores TSPEC requests from clients. Use this setting if you do not want to use TSPEC for QoS-compliant devices.
- *TSPEC Voice ACM Mode* – regulates mandatory admission control (ACM) for the Voice traffic category. By default – off. May take the following values:
  - *On* – the client needs to send a request to the access point before sending or receiving Voice traffic flow.
  - *Off* – the client can send and receive Voice traffic without requiring a valid TSPEC; access point ignores Voice TSPEC requests from clients.
- *TSPEC Voice ACM Limit* – defines the limit of Voice traffic volume. The parameter may take values from 0 to 90%. By default – 20%.
- *TSPEC FBT Voice ACM Limit* – defines an upper limit on Voice traffic volume for roaming clients on a given access point using a fast BSS transition. The parameter may take values from 0 to 90%. By default – 0%.
- *TSPEC Video ACM Mode* – regulates mandatory admission control (ACM) for the Video traffic category. By default – off. May take the following values:
  - *On* – the client needs to send a request to the access point before sending or receiving Video traffic flow.
  - *Off* – the client can send and receive Video traffic without need for a request.
- *TSPEC Video ACM Limit* – defines an upper limit on Video traffic volume. The parameter may take values from 0 to 90%. By default – 15%.
- *TSPEC FBT Video ACM Limit* – defines an upper limit on Video traffic volume for roaming clients on a given access point using a fast BSS transition. The parameter may take values from 0 to 90%. By default – 0%.
- *TSPEC BE ACM Mode* – regulates mandatory admission control for the Best Effort traffic category. By default – off. May take the following values:
  - *On* – the client needs to send a request to the access point before sending or receiving Best Effort traffic category;
  - *Off* – the client can send and receive Best Effort traffic category without need for a request.
- *TSPEC BE ACM Limit* – defines an upper limit on Best Effort traffic volume for roaming clients on a given access point using a fast BSS transition. The parameter may take values from 0 to 90%. By default – 0%.
- *TSPEC BK ACM Mode* – regulates mandatory admission control for the Background traffic category. By default – off. The parameter may take the following values:
  - *On* – the client needs to send a request to the access point before sending or receiving Backgroun d traffic category;
  - *Off* – the client can send and receive Background traffic category without need for a request.
- *TSPEC BK ACM Limit* – defines an upper limit on Background traffic volume for roaming clients on a given access point using a fast BSS transition. The parameter may take values from 0 to 90%. By default – 0%.
- *TSPEC AP Inactivity Timeout* – time after which inactive clients will be removed from the access point (the downlink flow is checked). The parameter may take values from 0 to 120 seconds. By default – 30 seconds.
- *TSPEC Station Inactivity Timeout* – time after which inactive clients will be removed from the access point (the uplink flow is checked). The parameter may take values from 0 to 120 seconds. By default – 30 seconds.
- *TSPEC Legacy WMM Queue Map Mode* – select *On* to receive traffic of various categories on queues operating in AKM.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

4.5.6 'Scheduler' submenu

In the '**Scheduler**' submenu, access point scheduler is configured. Using the settings of this menu, operating time of a specific radio interface or virtual access point can be configured.



- *Global Scheduler Mode* – enable/disable scheduler:
  - *Enable* – scheduler is enabled;
  - *Disable* – scheduler is disabled.

Scheduler Operational Status – this section provides information about the status of the scheduler:

- *Status* – scheduler operational status. The parameter may take the following values: Up (enabled) or Down (disabled). By default – Down;
- *Reason* – additional information about scheduler status:
  - *IsActive* – operational state;
  - *ConfigDown* – scheduler is disabled, no global settings;
  - *TimeNotSet* – scheduler is enabled, system time is not set on the device;
  - *ManagedMode* – scheduler is enabled, the device is in management mode;
- *Scheduler Profile* – name of the scheduler profile to create. May contain from 1 to 32 characters.

To add profile to the system, enter a name in the 'Scheduler Profile' field and click the 'Add' button.

Rule Configuration – in this section, scheduler profile parameters are configured:

- *Select Profile* – name of the previously created profile for which the settings will be configured;
- *Set Schedule* – day of the week the scheduler runs. The parameter may take the following values:
  - *Daily* – every day;
  - *Weekday* – working days;
  - *Weekend* – weekends;
  - *On* – specific day of the week, which is selected from the drop-down list. May take the following values: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday;
- *Start Time* – radio interface or VAP activation time. Specified as hh:mm;
- *End Time* – radio interface or VAP off time. Specified as hh:mm.

To add new profile rule, click the 'Add Rule' button.

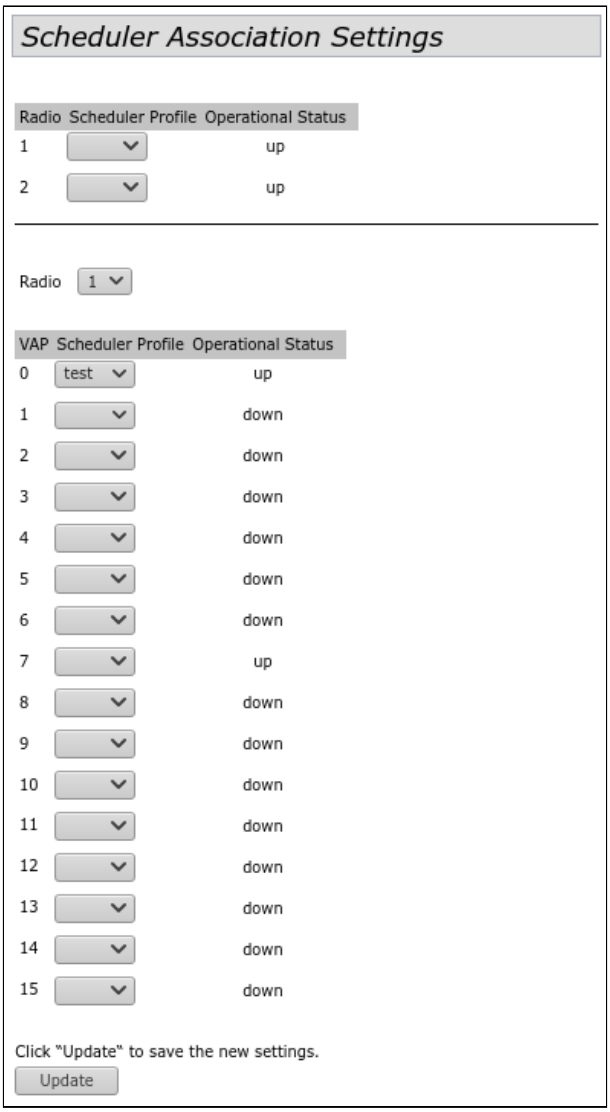
To delete a rule, select the rule in the list and click the 'Remove Rule' button.

To change the rule settings, select the rule and click the 'Modify Rule' button.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

4.5.7 'Scheduler Association' submenu

In the '**Scheduler Association**' submenu, scheduler rules created in the 'Scheduler' submenu are bound to VAPs or radio interfaces.



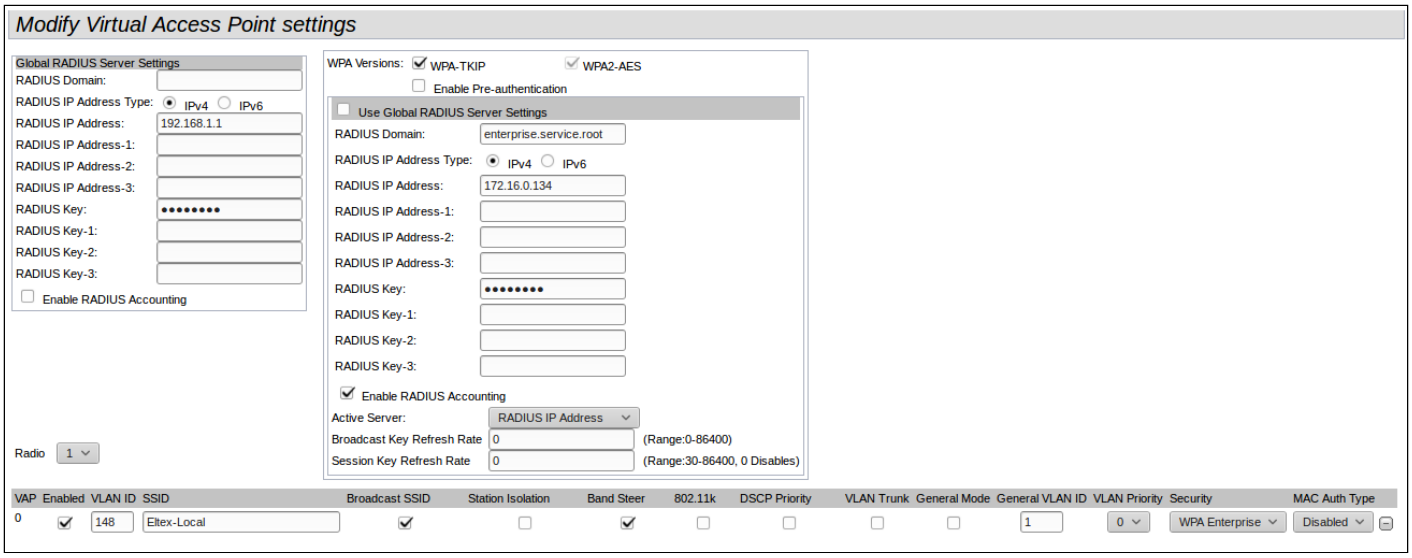
In the 'Scheduler Profile' column next to the Radio or VAP number to which you want to apply the previously created scheduler rule, set the name of the scheduler profile.

Values in the 'Operational Status' column are informational and indicate the status in which the VAP or the radio interface of the access point is located: up – enabled, down – disabled.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

4.5.8 'VAP' submenu

In the **'VAP'** submenu virtual access points on Wi-Fi interfaces are configured, as well as RADIUS server parameters. Up to 16 virtual access points can be configured on each radio interface.



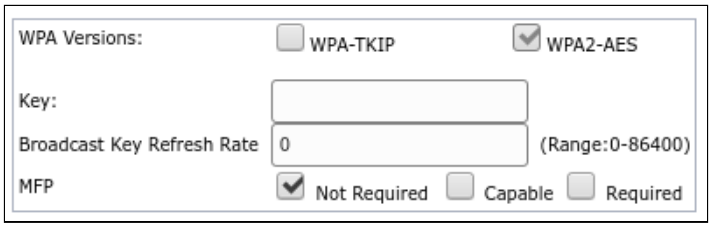
Global RADIUS Server Settings – in this section, global settings for authorization via the RADIUS protocol are performed:

- *RADIUS Domain* – user domain;
- *RADIUS IP Address Type* – selection of IPv4 or IPv6 for access to the RADIUS server;
- *RADIUS IP Address* – main RADIUS server address. If the main RADIUS server is unavailable, requests will be sent to the backup servers specified in the fields RADIUS IP Address-1, RADIUS IP Address-2, RADIUS IP Address-3;
- *RADIUS IP Address-1, 2, 3* – backup RADIUS server addresses. If the main RADIUS server is unavailable, requests will be sent to the backup servers;
- *RADIUS Key* – password for authorization on the main RADIUS server;
- RADIUS Key-1, 2, 3 – passwords for authorization on backup RADIUS servers;
- *Enable RADIUS Accounting* – when the flag is set, 'Accounting' messages will be sent to the RADIUS server.

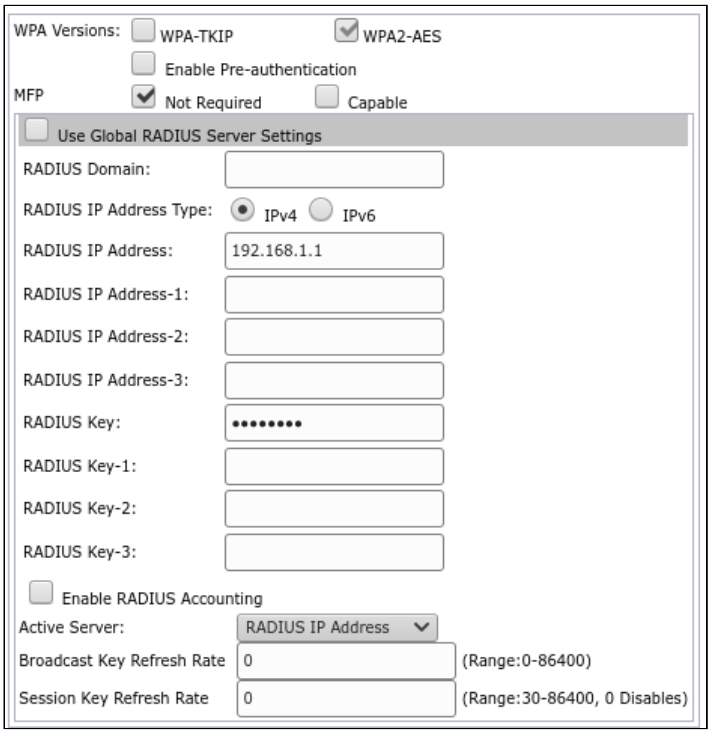
Configuring Virtual Access Points:

- *Radio* – selection of the radio interface for VAP configuration. Radio 1 – VAP configuration in 5 GHz band, Radio 2 – VAP configuration in 2.4 GHz band;
- *VAP* – number of the virtual access point on the radio interface;
- *Enabled* – when the flag is set, virtual access point is enabled, otherwise it is disabled:
- *VLAN ID* – VLAN number that will be tagged when transmitting Wi-Fi traffic to clients connected to this VAP. When traffic flows in the opposite direction, untagged traffic from clients will be tagged with VLAN ID (when VLAN Trunk mode is disabled);
- *SSID* – wireless network name;
- *Broadcast SSID* – when checked, SSID broadcasting is on, otherwise it is disabled;
- *Station Isolation* – when checked, traffic isolation between clients within the same VAP is enabled;
- *Band Steer* – when checked, priority client connection to 5 GHz network is active. For the functionality to work, create a VAP with the same SSID on each radio interface and activate the 'Band Steer' parameter on them;
- *802.11k* – enable support for 802.11k standard on VAP. 802.11k roaming requires client support for the standard. Using the functionality is possible only when using the Airtune service;
- DSCP Priority – when checked, analyzes priority from the DSCP field of the IP packet header; when unchecked, analyzes priority from the CoS (Class of Service) field of the tagged packets;
- *VLAN Trunk* – when checked, tagged traffic is transmitted to the subscriber;

- General Mode – when checked, transmission of untagged traffic jointly with tagged traffic is allowed (available when Trunk VLAN mode is enabled);
- *General VLAN ID* – a tag will be removed from the specified VLAN ID and the traffic of this VLAN will pass to the client without a tag. When traffic passes in the opposite direction, untagged traffic will be tagged with General VLAN ID;
- *VLAN Priority* – level 3 priority that will be assigned to packets coming from a client connected to this VAP and transmitted further to the wired network;
- *Security* – wireless access security mode:
  - *None* – no encryption for data transmission. Access point is available for connection of any client;
  - *WPA Personal* – WPA and WPA2 encryption. When this mode is selected, the following settings are available:



    - *WPA Versions* – encryption versions: WPA-TKIP, WPA2-AES;
    - *Key* – WPA key. The key length is from 8 to 63 characters.
    - *Broadcast Key Refresh Rate* – broadcast key update interval. May take values from 0 to 86400. By default – 0.
    - *MFP* – client frame protection mode configuration:
      - *Not Required* – do not use the protection;
      - *Capable* – use protection when possible;
      - *Required* – protection is mandatory, all clients must support CCX5.



- *WPA Enterprise* – wireless channel encryption mode, in which the client is authorized on the centralized RADIUS server. To configure this security mode, specify the parameters of the RADIUS server (it is possible to use up to 4 RADIUS servers simultaneously, but specifying one active at the moment). the domain, security mode protocol versions, and keys for each RADIUS server must also be specified. When this mode is selected, the following settings are available:
  - *WPA Versions* – encryption versions: WPA-TKIP, WPA2-AES;

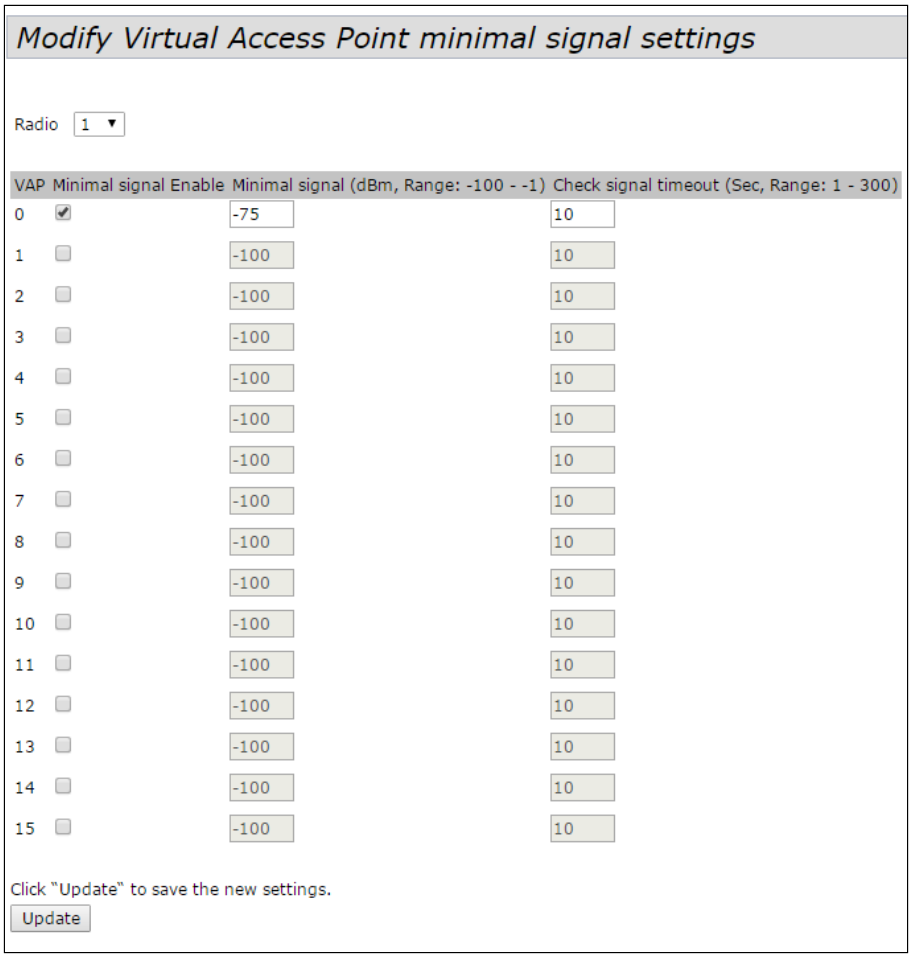
- *Enable Pre-authentication* – when checked, the pre-authentication procedure for WPA2 wireless clients is used. Pre-authentication allows a mobile client to authenticate to another nearby access point while remaining 'bound' to its primary access point. This reduces the amount of time communication is not available for a roaming client while waiting for RADIUS authentication in a forwarding process;
- *MFP* – client frame protection mode configuration:
  - *Not Required* – do not use the protection;
  - *Capable* – use protection when possible.
- *Use Global RADIUS Server Settings* – when checked, Global RADIUS Server Settings specified at the top of the page will be used. To use a separate RADIUS server for VAP, uncheck the box and enter the IP address, password of the RADIUS server, and other data in the following fields:
  - *RADIUS Domain* – user domain;
  - *RADIUS IP Address Type* – IPv4 or IPv6 protocol selection to access the RADIUS server;
  - *RADIUS IP Address* – main RADIUS server address. ΠIf the main RADIUS server is unavailable, requests will be sent to the backup servers specified in the fields *RADIUS IP Address-1, RADIUS IP Address-2, RADIUS IP Address-3*;
  - *RADIUS IP Address-1, 2, 3* – backup RADIUS server addresses. If the main RADIUS server is unavailable, requests will be sent to the backup servers;
  - *RADIUS Key* – password for authorization on the main RADIUS server;
  - *RADIUS Key-1, 2, 3* – passwords for authorization on backup RADIUS servers;
  - *Enable RADIUS Accounting* – when the flag is set, 'Accounting' messages will be sent to the RADIUS server.
- *Active Server* – select which of the four RADIUS servers the VAP should contact to authenticate wireless clients.
- *Broadcast Key Refresh Rate* – broadcast (group) key update interval for clients of this VAP. The parameter may take values from 0 to 86400 seconds. By default – 0. The 0 value indicates that the broadcast key is not updated. Broadcast key is not updated when Fast Transition is enabled on VAP (IEEE 802.11r).
- *Session Key Refresh Rate* – session key update interval for each client of this VAP. The parameter may take values from 30 to 86400 seconds. By default – 0. The 0 value indicates that the session key is not updated.

- *MAC Auth Type* – client authentication mode by MAC address:
  - *Disabled* – do not use client authentication by MAC address;
  - *RADIUS* – use client authentication by MAC address via RADIUS server;
  - *Local* – use client authentication by MAC address using the local address list generated on this access point.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

4.5.9 'VAP Minimal Signal' submenu

In the '**VAP Minimal Signal**' submenu, function of disabling client Wi-Fi equipment when signal level received from it is low can be configured. Used to optimize the seamlessness of roaming on the network.

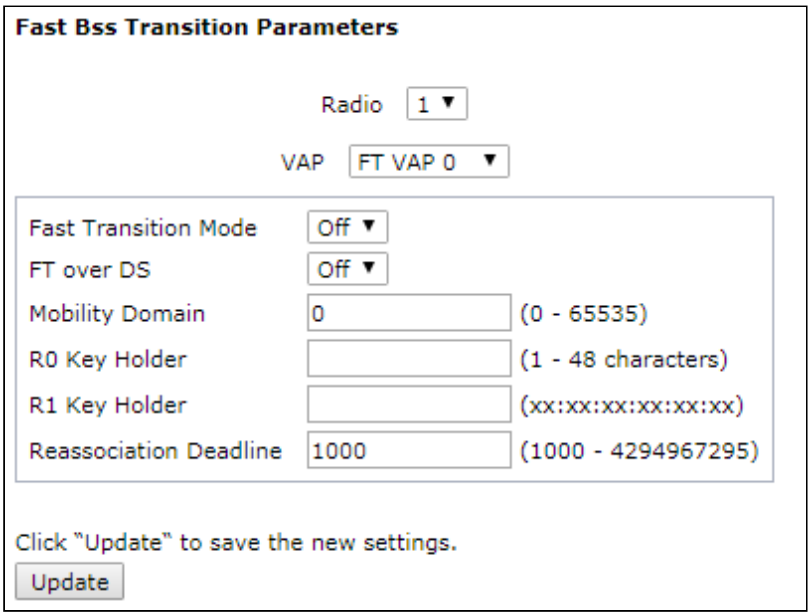


- *Radio* – select the configured radio interface;
- *VAP* – number of virtual access points;
- *Minimal signal Enabled* – when checked, Minimal Signal feature is enabled;
- *Minimal signal, dBm* – signal level in dBm, below which the client equipment is disconnected. May take values from -100 to -1;
- *Check signal timeout, s* – time interval, after which a decision is made to turn off client equipment. May take values from 1 to 300 seconds. By default – 10 seconds.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

4.5.10 'Fast Bss Transition' submenu

In the **'Fast Bss Transition'** submenu, 802.11r roaming between base stations is configured.

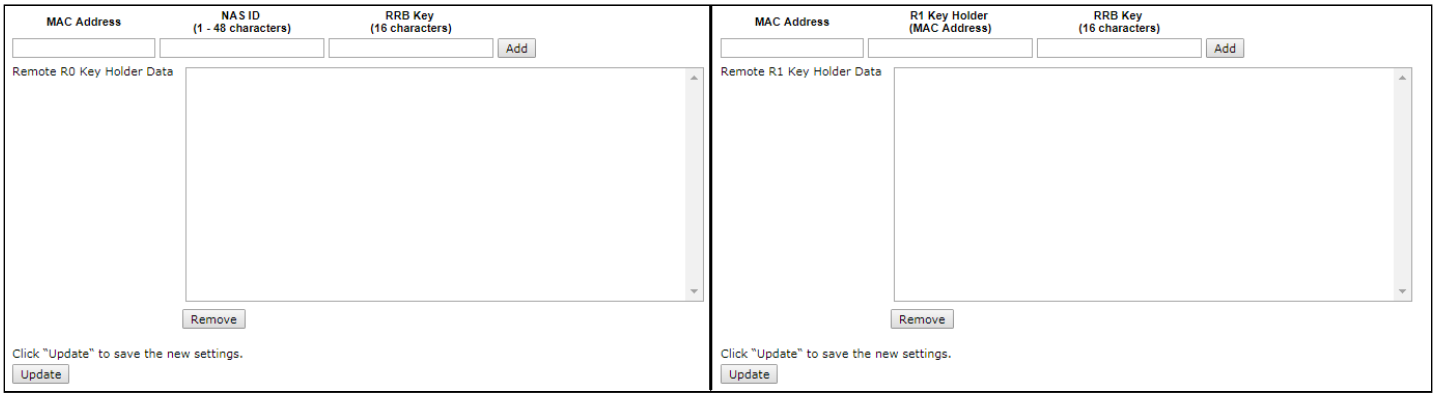


Fast Bss Transition parameters:

- *Radio* – radio interface selection on which FBT will be configured;
- *VAP* – number of the virtual access point on which FBT will be configured;
- *Fast Transition Mode* – activating the fast transfer of the basic set of services to speed up the authentication process on the access point:
  - *On* – function is enabled;
  - *Off* – function is disabled.
- *FT over DS* – enabling the exchange mechanism between base stations over wired network. If it is necessary to roam, the client sends an FT Action Request Frame to the current access point with the necessary authorization data. The current access point encapsulates the given frame and forwards to the target access point over the wired network. The target AP asserts fast authentication capability with an encapsulated message to the current access point FT Action Response Frame. Current access point forwards this message to the client. After the process is completed, the client sends a Reassociation request to the target access point. When the FT over DS function is disabled, FT over AIR works, in which case the client is authorized on the target access point using the following standard authentication frames:
  - *On* – function is enabled;
  - *Off* – function is disabled.
- *Mobility Domain* – number of the group within which roaming can be made. May take values from 0 to 65535. By default – 0;
- *R0 Key Holder* – PMK-R0 key. May contain from 1 to 48 characters. Optionally used as the identifier of the NAS that will be sent in the Radius Access Request message;
- *R1 Key Holder* – PMK-R1 key in the xx:xx:xx:xx:xx:xx MAC address format;
- *Reassociation Deadline* – maximum allowed 'Reassociation' request from the station waiting time. May take values from 1000 to 4294967295 ms. By default – 1000 ms.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

After specifying the basic parameters, it is necessary to configure interaction with access points between which roaming will be carried out by setting the MAC addresses of access points and keys.



- *MAC Address* – MAC address of access point participating in roaming;
- *NAS ID* – NAS identifier, takes the value specified in R0 Key Holder;
- *R1 Key Holder* – PMK-R1 key in the xx:xx:xx:xx:xx:xx MAC address format;
- *RRB Key* – key to encrypt RRM messages 16 characters long.

To add new entry to the table, click 'Add'.

To remove entry from the table, select the line and click 'Remove'.

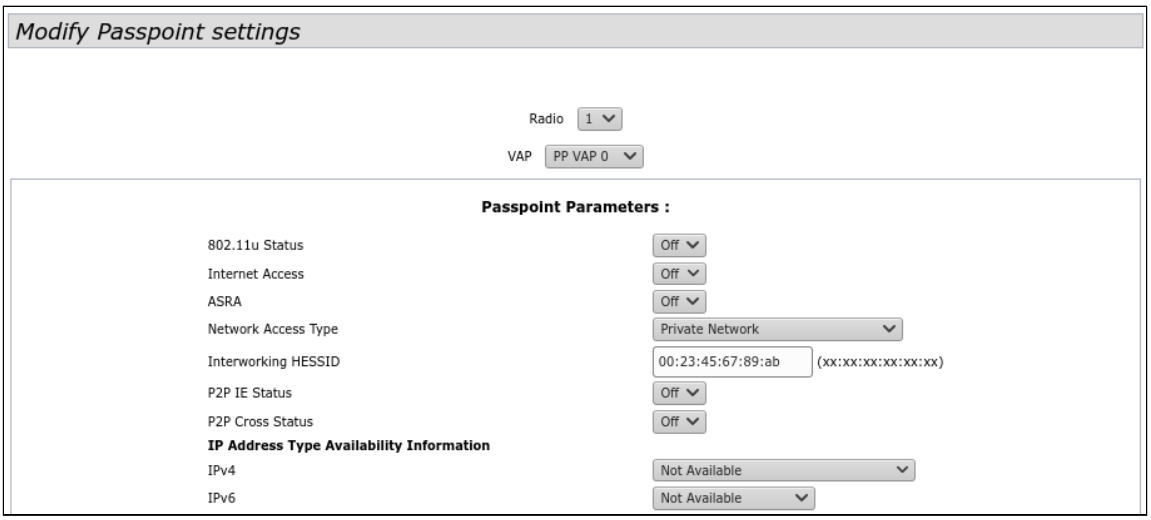
To apply a new configuration and save setting to non-volatile memory, click 'Update'.

4.5.11 'Passpoint' submenu

Passpoint is a feature that allows users to seamlessly migrate from 3G/4G networks to Wi-Fi networks.

Passpoint supports the following authentication types:

- EAP-TLS (certificate-based identification),
- EAP-SIM (identification based on GSM SIM card data),
- EAP-AKA (identification based on UMTS USIM data),
- EAP-TTLS with MS-CHAPv2 (username and password request, server certificate).



Select the radio interface and virtual access point on which Passpoint will run and fill in the fields below (if necessary).

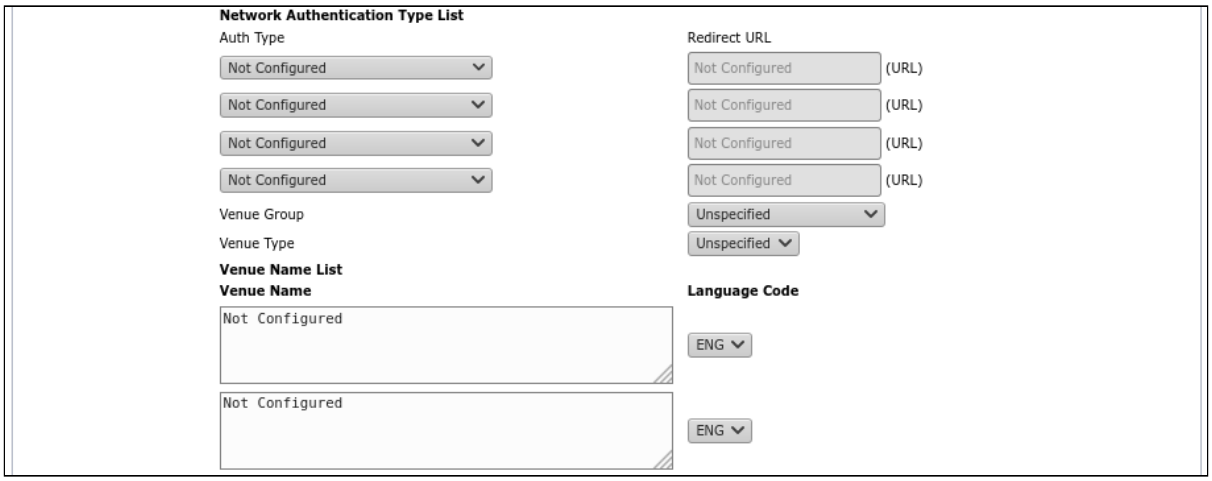
- *Radio* – radio interface on which to activate the Passpoint function;
- *VAP* – virtual access point (SSID), on which to activate the Passpoint function.

Internetwork parameters 802.11u (Passpoint parameters):

- *802.11u Status* – enable/disable Passpoint;
- *Internet Access* – enable/disable Internet Access;
- *ASRA* (Additional Step Required for Access) – add/remove additional authorization step when gaining access;
- *Network Access Type* – type of interaction with the access network:
  - *Private Network* – private network;
  - *Private Network with Guest Access* – private network with guest access;
  - *Chargeable Public Network* – chargeable public network;
  - *Free Public Network* – free public network;
  - *Emergency Services Only Network* – network for emergency services and ambulance services;
  - *Personal Device Network* – personal device network;
  - *Test or Experimental* – test network;
  - *Wildcard* – interaction through vouchers (wildcard certificate);
- *Interworking HESSID* – MAC address, the same for all access points of the same network.

Information about the access type (IP Address Type Availability Information):

- *IPv4* – access configuration via IPv4 protocol;
- *IPv6* – access configuration via IPv6 protocol.



Network Authentication Type List:

- *Auth Type* – select the type of authentication in the field:
  - *Not Configured* – authentication type not set;
  - *Acceptance of Term and Conditions* – authentication with acceptance of the user agreement;
  - *Online Enrollment* – online registration;
  - *HTTP/HTTPS Redirection* – HTTP/HTTPS redirect;
  - *DNS Redirection* – DNS redirect.
- *Redirect URL* – field for entering URL to which the redirect will be performed. Available with the following authentication types: *Acceptance of Term and Conditions, HTTP/HTTPS Redirection, DNS Redirection.*

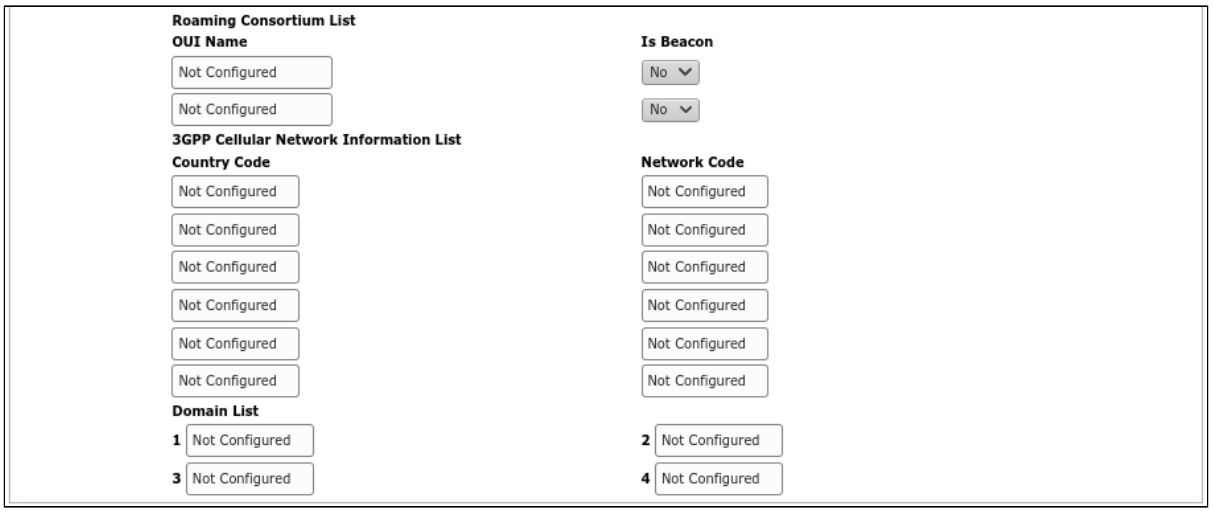
Information about the installation location (Venue Details):

- *Venue Group* – installation site category defined by the IEEE 802.11u standard:
  - *Unspecified* – not specified;
  - *Assembly* – crowded places (stadiums, theaters, restaurants, train stations, airports, etc.);
  - *Business* – banks, offices, research centers, etc.;
  - *Educational* – training centers;
  - *Factory and Industrial* – industrial buildings;
  - *Institutional* – state institutions;
  - *Mercantile* – commercial (trade) organizations;
  - *Residential* – housing estates;

  - *Storage* – storages/warehouses;
  - *Utility and Miscellaneous* – public services, etc.;
  - *Vehicular* – transport;
  - *Outdoor* – outdoor (city parks, recreation areas, stops, kiosks);
  - *Reserved* – private territories.
- *Venue Type* – location type. Available options depend on the location category selected above.

List of access point locations (Venue Name List):

- *Venue Name* – location name of the access point;
- *Language Code* – language.



List of organizations (Roaming Consortium List):

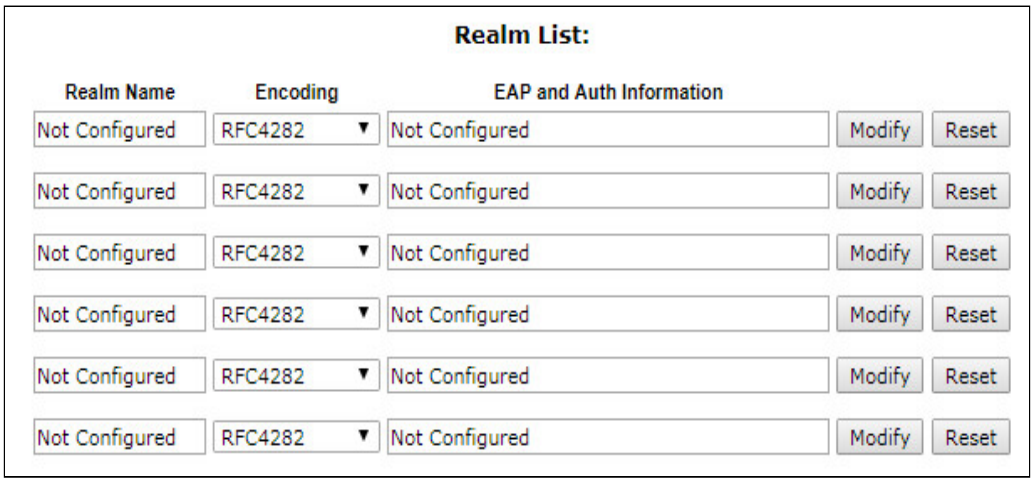
- *OUI Name* – organization unique identifier (OUI);
- *Is Beacon* – add OUI to beacon (Yes), do not add OUI to beacon (No).

3GPP Cellular Network Information List:

- *Country Code* – country code;
- *Network Code* – network code.

Domain List:

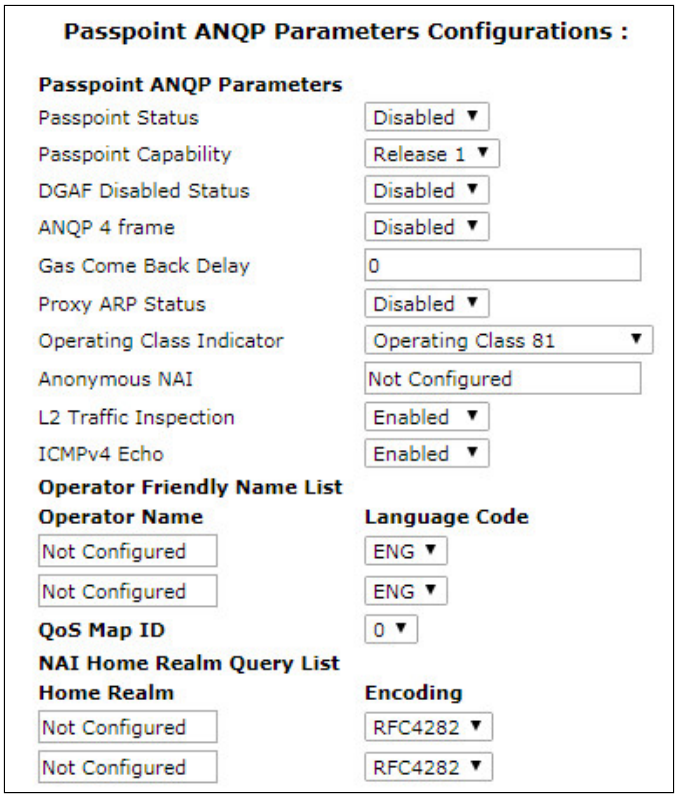
Enter domains in the free fields.



Realm list:

- *Realm Name* – name of the realm;
- *Encoding* – encoding (RFC4282, UTF8);
- *EAP and Auth Information* – protocol and authentication information;

- *Modify* – configure authentication type and parameters;
- *Reset* – reset settings.



Passpoint ANQP Parameters Configurations:

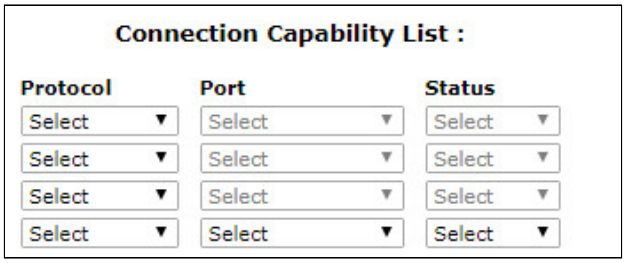
- *Passpoint Status* – enable/disable Passpoint;
- *Passpoint Capability* – determine if the device supports Passpoint;
- *DGAF Disabled Status* – enable/disable forwarding of downstream multicast address frames (for multicast). When an access point transmits frames containing HS2.0 indication element with DGAF Disable set to disable, the mobile device must discard all received Unicast IP packets that have been decrypted with the group key;
- *ANQP 4 frame* – enable/выключить disable 4 GAS frame exchange;
- *Gas Come Back Delay* – GAS Comeback in TU depends on ANQP 4 frame setting;
- *Proxy ARP Status* – enable/disable Proxy ARP;
- *Operating Class Indicator:*
  - *Operating Class 81* – operation in the 2.4 GHz band;
  - *Operating Class 115* – operation in the 5 GHz band;
  - *Operating Class 81&115* – simultaneous operation in the 2.4 and 5 GHz bands.
- *Anonymous NAI* – set anonymous network access ID (NAI – Network Access Identifier);
- *L2 Traffic Inspection* – enable/disable L2 traffic control and filtering (available for access points that have a built-in traffic control and filtering function);
- *ICMPv4 Echo* – filtering feature for ICMPv4 Echo requests.

Carriers who can connect Passpoint on this access point (Operator Friendly Name List):

- *Operator Name* – carrier name;
- *Language Code* – language;
- *QoS Map ID* – QoS Map identifier.

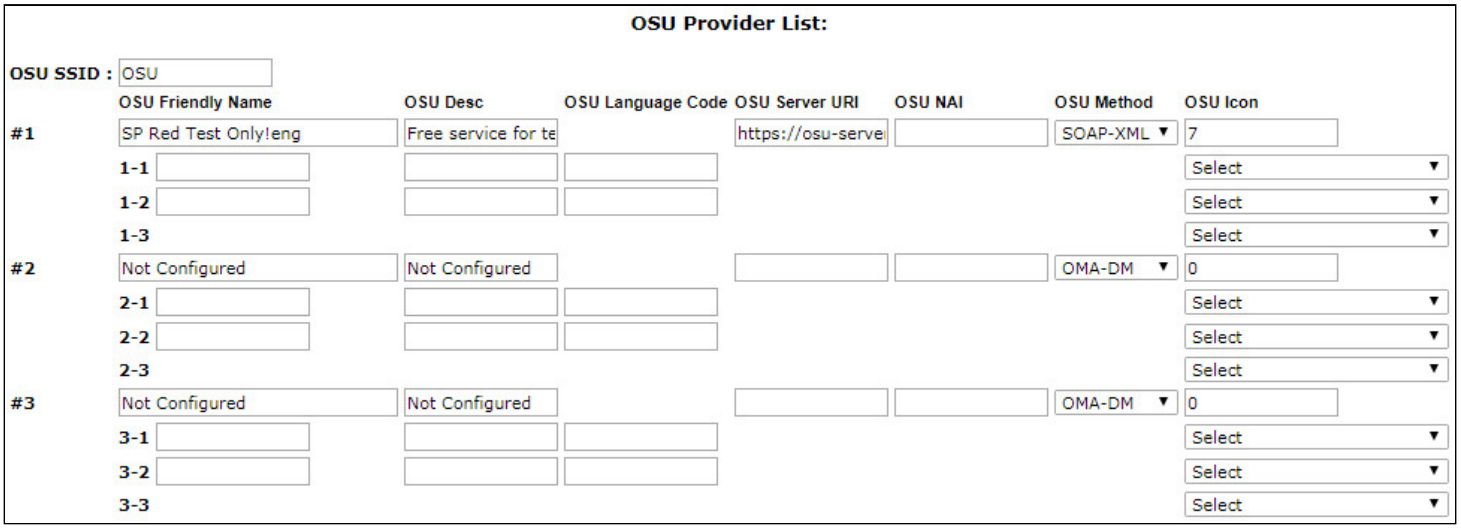
Home realms list (NAI Home Realm Query List):

- *Home Realm* – home realm;
- *Encoding* – encoding (RFC4282 or UTF8).



List of possible connections (Connection Capability List):

- *Protocol* – protocol that can be used for connection:
  - *ICMP (0x1)* – ICMP;
  - *TCP (0x6)* – TCP;
  - *UDP (0x11)* – UDP;
  - *ESP (0x32)* – ESP.
- *Port* – port that can be used for connection;
- *Status* – connection status:
  - *Closed* – connection with given parameters is closed;
  - *Open* – connection with given parameters is open;
  - *Unknown* – connection status is unknown.



List of providers for which online registration is available (OSU Provider List):

- *OSU SSID* – network identifier for online registration;
- *OSU Friendly Name* – internet provider name;
- *OSU Desc* – online registration server description;
- *OSU Language Code* – online registration language code;
- *OSU Server URI* – online registration server URL;
- *OSU NAI* – network access identifier for online registration;
- *OSU Method* – online registration method;
- *OSU Icon* – internet provider logo.

WAN Metrics Information:

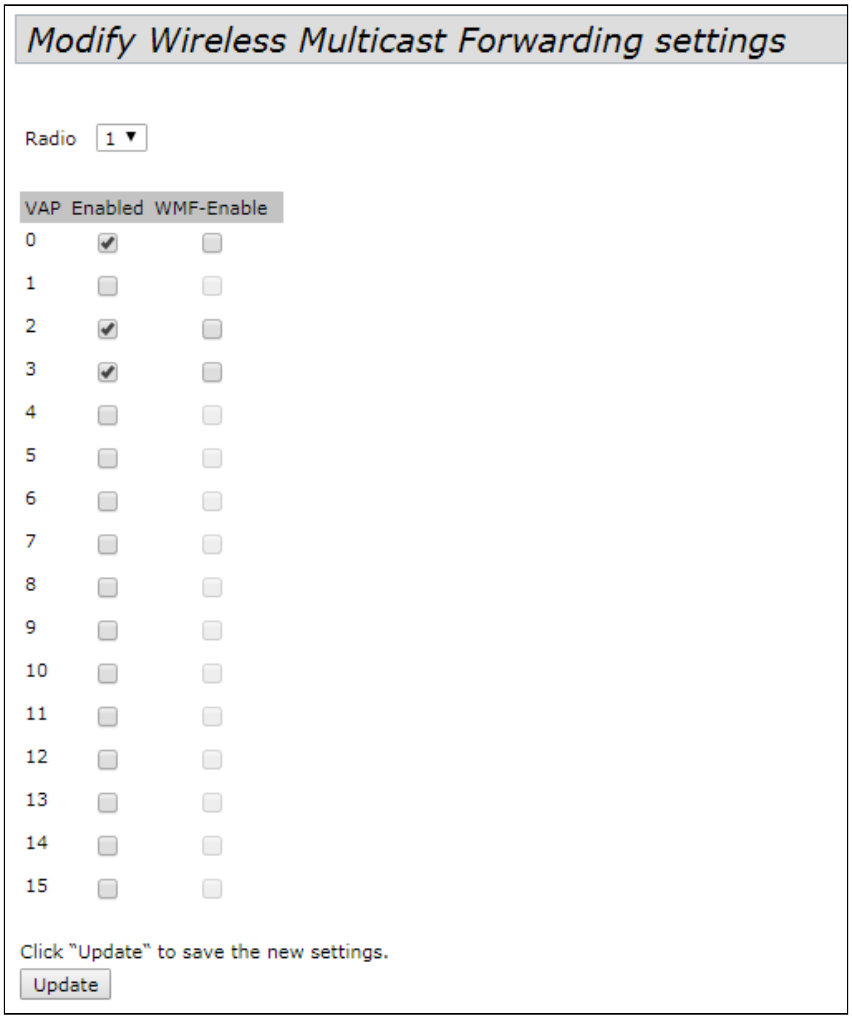
- *Link Status* – connection state:
  - *Link up* – connection is active;
  - *Link Down* – connection is inactive;
  - *Link Test* – connection is in test mode.

- *Symmetric Link* – connection is symmetrical (Symetric Link) or asymmetrical (Not Symmetric Link);
- *At Capacity* – throughput;
- *Down Link speed* – downstream speed;
- *Up Link speed* – upstream speed;
- *Down Link Load* – downstream load;
- *Up Link Load* – upstream load;
- *Lmd* – Load Measurement Duration.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

4.5.12 'Wireless Multicast Forwarding' submenu

In the **'Wireless Multicast Forwarding'** submenu, multicast packet redirection is configured.



- *Radio* – radio interface selection;
- *VAP* – number of the virtual access point;
- *Enabled* – if the flag is set, virtual access point is active, otherwise – inactive;
- *WMF-Enable* – if the flag is set, the function of redirecting multicast packets on the virtual access point is active, otherwise – inactive.

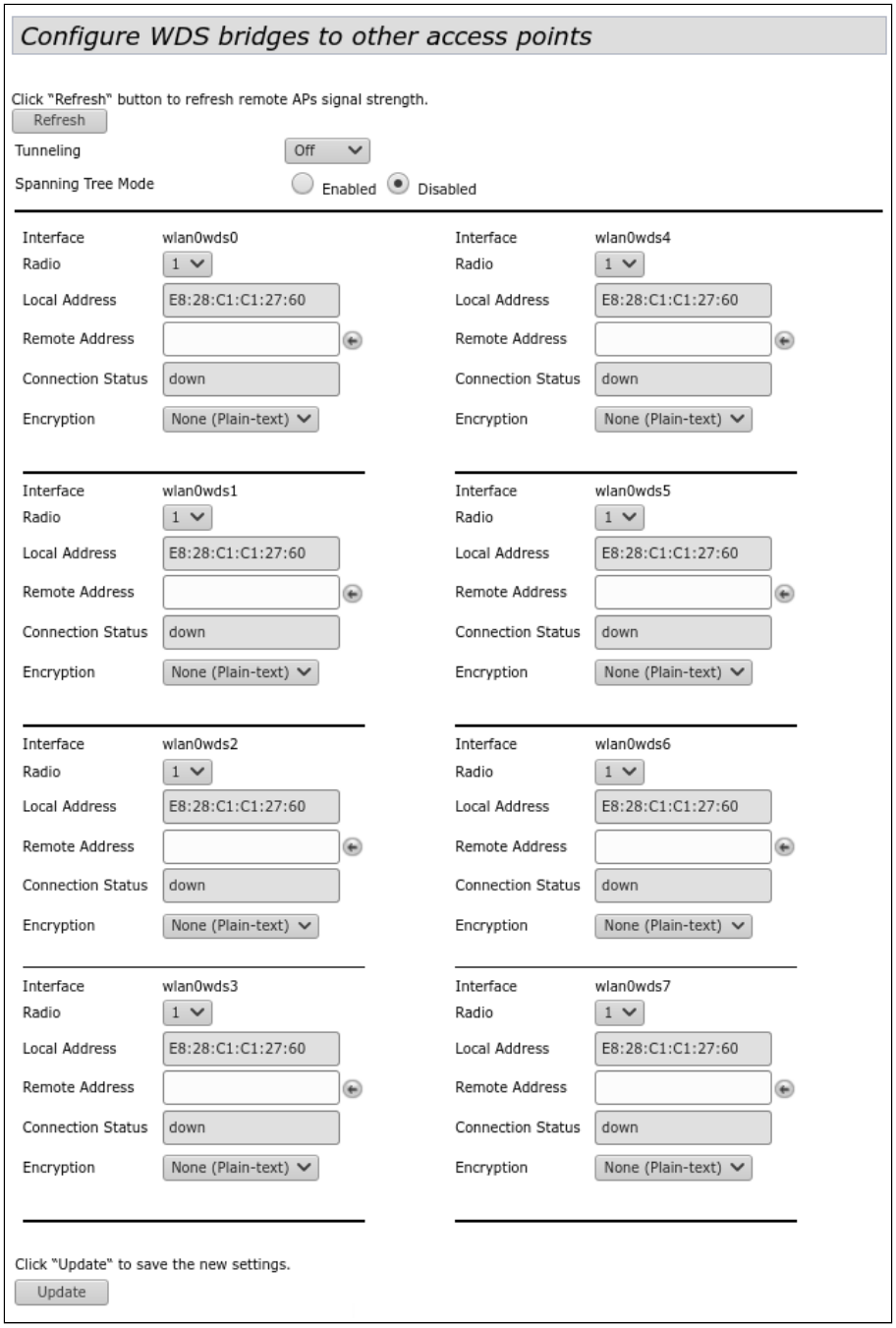
To apply a new configuration and save setting to non-volatile memory, click 'Update'.

4.5.13 'WDS' submenu

In the **'WDS'** submenu, communication between access points via a wireless network can be configured,

> WDS cannot be configured if WGB is configured on the point or cluster mode is enabled.

> For correct WDS operation, it is necessary that the same firmware version is installed on the access points.



- *Tunneling* – option available only when using GRE:
  - *Off* – GRE is not used, the Tunneling option is disabled;
  - *Master* – access point is connected to network via Ethernet interface;
  - *Slave* – access point is connected to Master via radio interface.

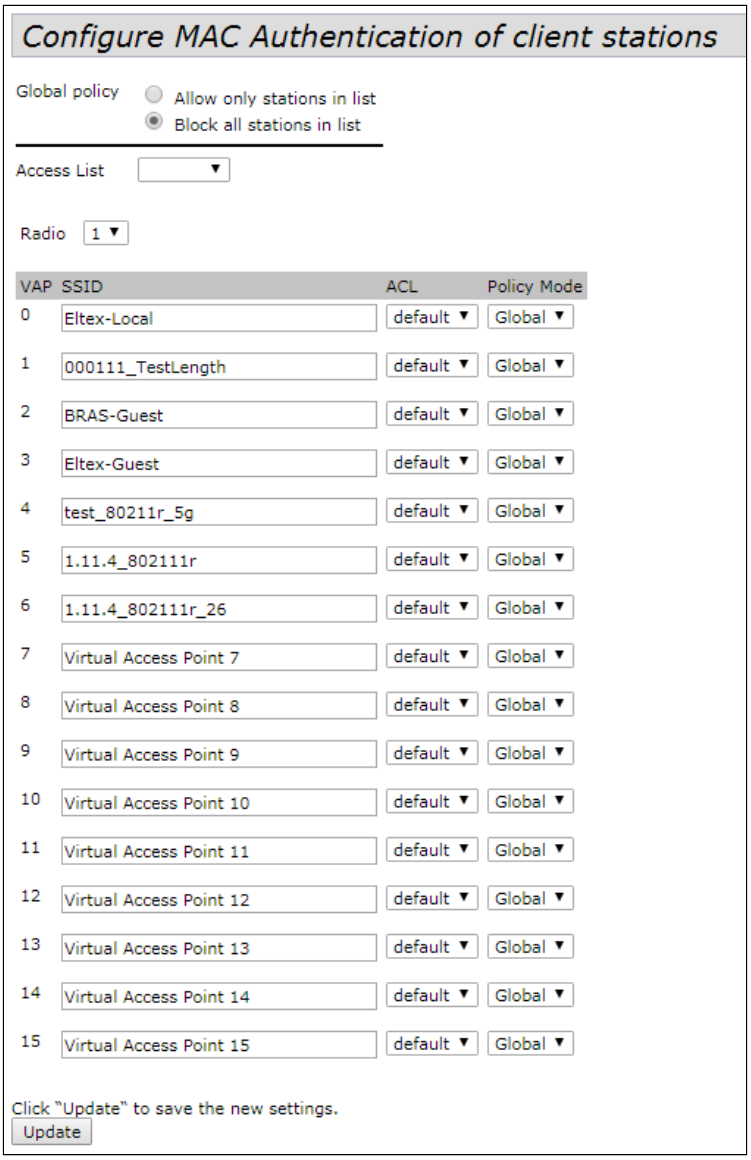
- *Spanning Tree Mode* – STP protocol operating mode to prevent network loops:
  - *Enabled* – when the flag is set, the STP protocol is allowed for use. Recommended to enable when using WDS;
  - *Disable* – when the flag is set, the STP protocol is disabled.
- *Radio* – radio interface selection. Radio 1 – WDS will be deployed in 5 GHz band, Radio 2 – WDS will be deployed in 2.4 GHz band;
- *Local Address* – view MAC address of the current radio interface;
- *Remote Address* – MAC address of the radio interface of the access point with which the collaboration is intended. MAC address of the radio interface can be viewed on the 'Status' / 'Interfaces' tab;
- *Connection Status* – connection status;
- *Signal* – signal level with which the current access point sees the opposite access point with which the WDS is configured, dBm;
- *Encryption* – select encryption mode:
  - *None* – do not use encryption;
  - *WPA (PSK)* – WPA and WPA2 encryption, when selected, the following settings will be available:
    - *SSID* – Wi-Fi network name;
    - *Key* – WPA key. The key length is from 8 to 63 characters.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

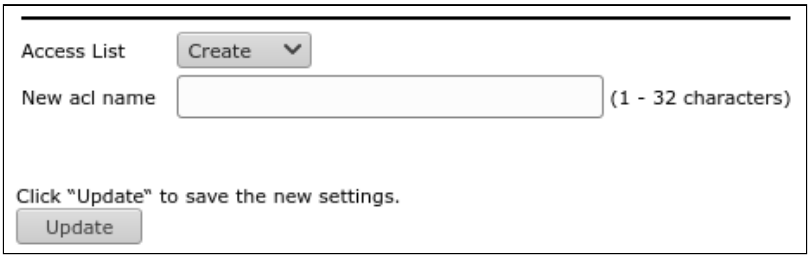
To update information on the page, click 'Refresh'.

4.5.14 'MAC Authentication' submenu

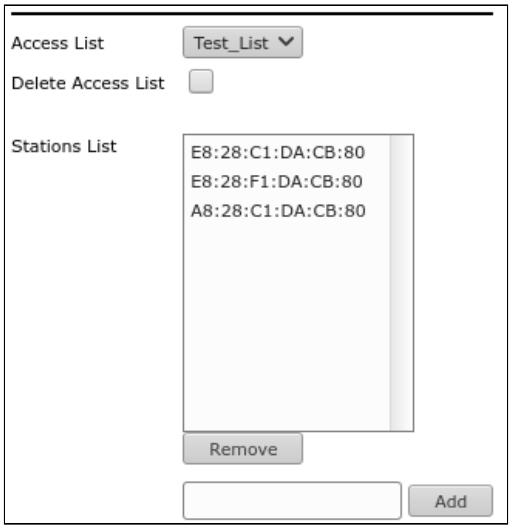
In the '**MAC Authentication**' submenu, white/black lists of MAC addresses of clients that are allowed/denied to connect to this access point can be configured.



- *Global policy* – selection of MAC address filtering list during authentication;
  - *Allow only stations in list* – when the flag is set, white list of MAC addresses will be formed;
  - *Block all stations in list* – when the flag is set, black list of MAC addresses will be formed.



- *Access List* – selecting existing lists of MAC addresses or creating a new list:
  - *Create* – creating a new list:
    - *New acl name* – enter a name for the new MAC address list and click the 'Update' button to create it.



- *Default* – standard empty list of MAC addresses. When this list or any other previously created list is selected, the following fields will be available for editing:
  - *Delete Access List* – when setting the flag and then clicking on the 'Update' button, the selected *Access List* will be deleted. The default list cannot be deleted;
  - *Stations List* – list of MAC addresses of clients that are allowed/denied access.

To add MAC address to the filtering list, in the 'Access List' parameter, select the desired list and enter the MAC address to add. Then click the 'Add' button. MAC address will appear in the 'Station List' section.

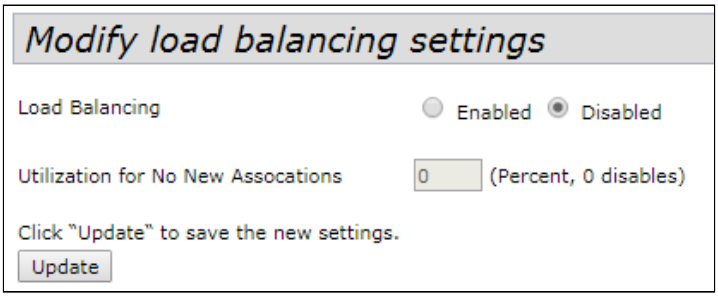
To remove MAC address from the list in the 'Station List' section, select the entry and click the 'Remove' button.

- *Radio* – radio interface selection;
- *VAP* – number of the virtual access point;
- SSID – name of the virtual access point;
- *ACL* – selecting a list of MAC addresses to bind to the selected SSID;
- *Policy Mode* – configuring white/black lists of MAC addresses:
  - *Global* – for the current SSID, the selected list of MAC addresses will match the global flag
  - *Allow* – for the current SSID, the selected list will be white (devices from the list are allowed access);
  - *Block* – for the current SSID, the selected list will be black (devices from the list are denied access).

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

4.5.15 'Load Balancing' submenu

In the '**Load Balancing**' submenu, the restriction of clients ability to connect to the access point is configured, depending on the utilization of the channel.



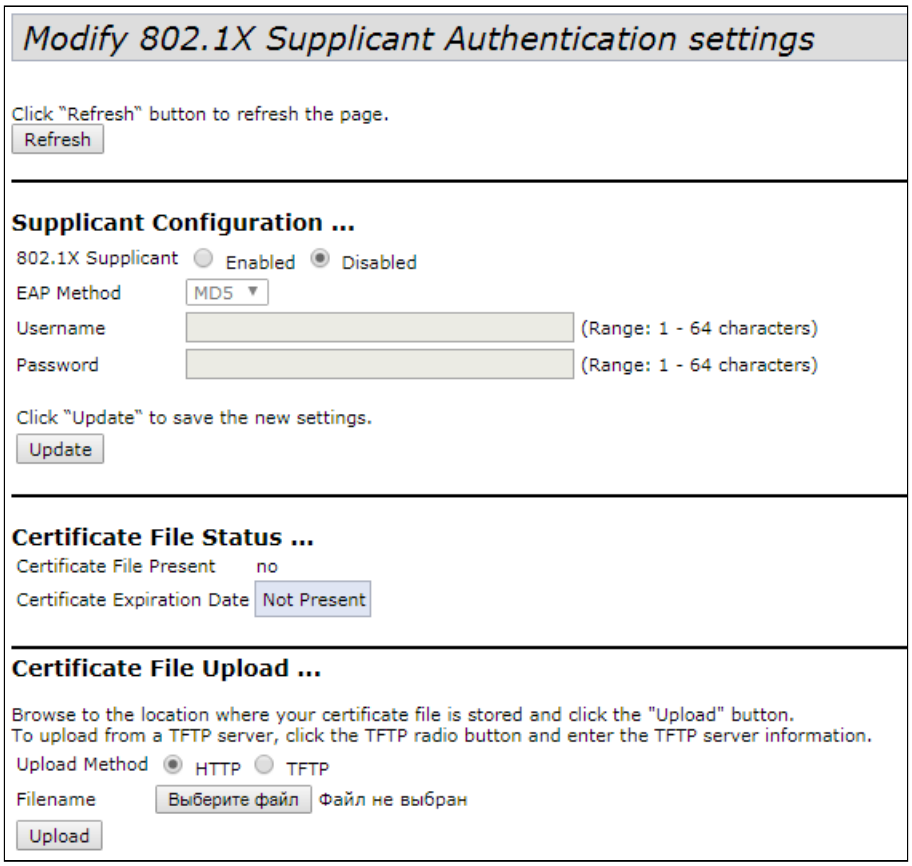
- *Load Balancing* – load balancing:
  - *Enabled* – load balancing is enabled;
  - *Disabled* – load balancing is disabled.

- *Utilization for No New Associations* – bandwidth utilization level of the access point, above which the connection of new clients is prohibited, set in%. By default – 0.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

4.5.16 'Authentication' submenu

In the '**Authentication**' submenu, the access point is configured in client mode using the 802.1X protocol to pass the authentication procedure on higher-level equipment.



Supplicant Configuration – in this section, the following authentication parameters are configured:

- *802.1X Supplicant* – enable/disable access point operation in client mode via 802.1X protocol:
  - *Enabled* – enable;
  - *Disabled* – disable.
- *EAP Method* – user authentication encryption algorithm. Possible values: MD5, PEAP, TLS;
- *Username* – user name. The parameter may contain from 1 to 64 characters;
- *Password* – password. The parameter may contain from 1 to 64 characters.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

Certificate File Status – in the section, information about HTTP SSL certificate status can be viewed:

- *Certificate File Present* – indicates if an HTTP SSL certificate file is present. Possible values: yes, no. By default there is no certificate – no.
- *Certificate Expiration Date* – date indicating when the HTTP SSL certificate file will expire. If the certificate is missing, the message 'Not Present' is displayed.

Certificate File Upload – in this section, the HTTP SSL Certificate file is loaded.

- *Upload Method* – HTTP SSL certificate file upload method:
  - *HTTP* – uploading certificate over HTTP. If choosing this method, click the 'Select File' button, select the file to load to the device;
  - *TFTP* – uploading certificate over TFTP. If choosing this method, fill in the following fields:

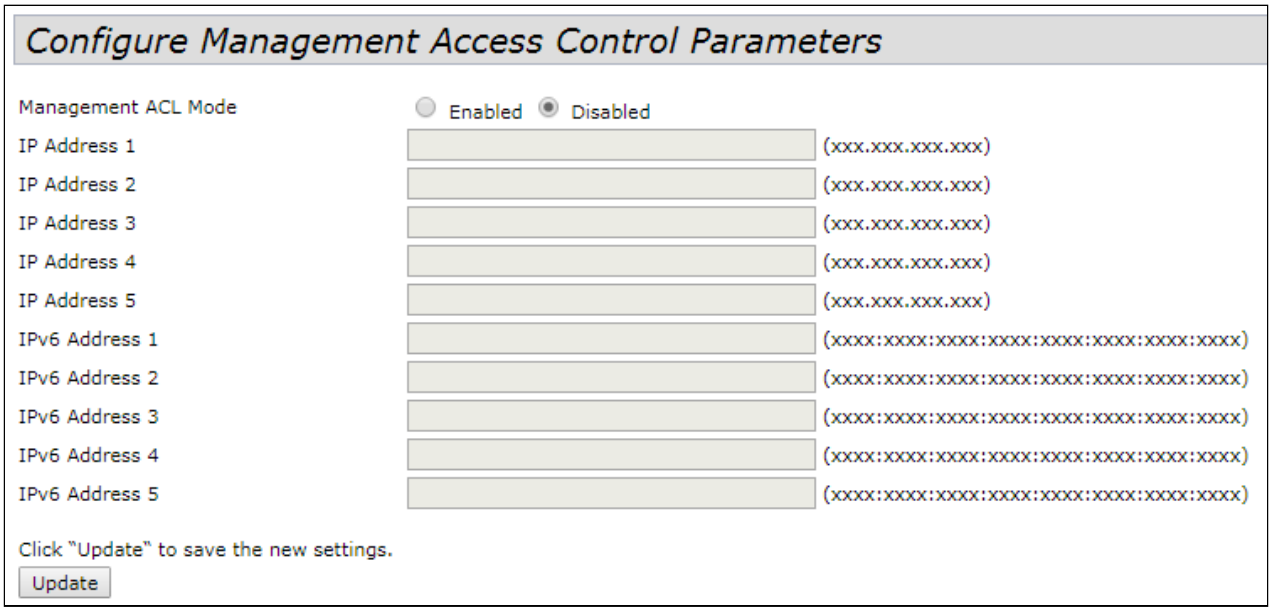
- *Filename* – certificate file name;
- *Server IP* – server IP address.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

To update information on the page, click 'Refresh'.

4.5.17 'Management ACL' submenu

In the **'Management ACL'** submenu, device management access lists are configured via Web, Telnet, SSH, SNMP.

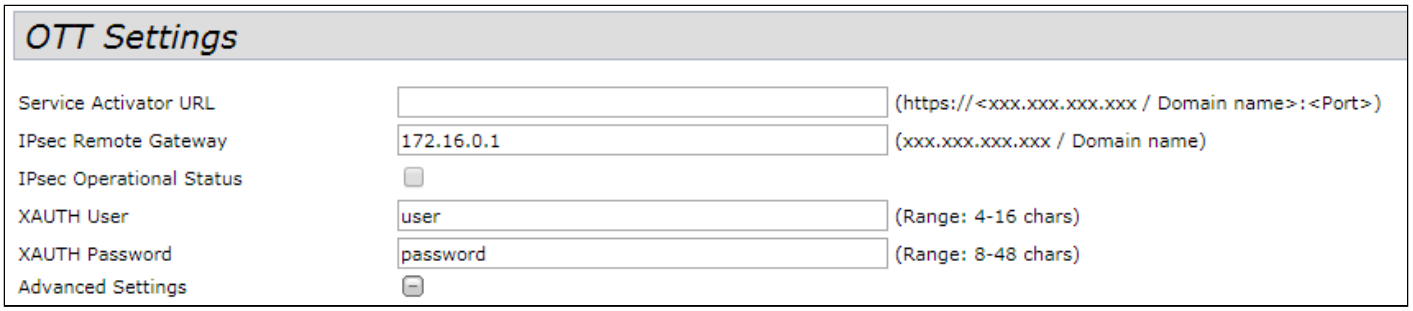


- *Management ACL Mode* – use of device management access lists:
  - *Enabled* – when the flag is set, the functionality is enabled;
  - *Disabled* – when the flag is set, the functionality is disabled.
- *IP Address 1...5* – list of the IPv4 hosts that have access to the device management;
- *IPv6 Address 1...5* – list of the IPv6 hosts that have access to the device management.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

4.5.18 'OTT Settings' submenu

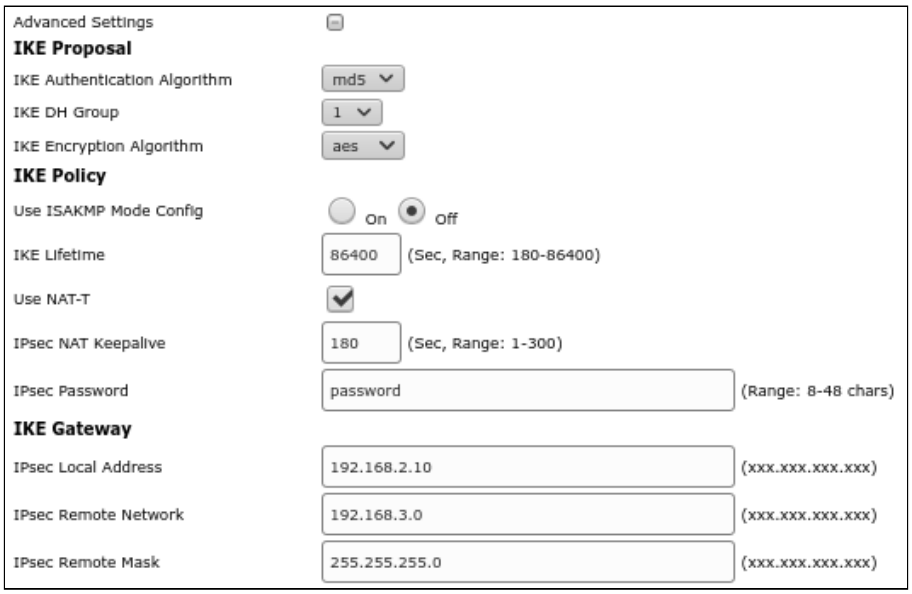
In the **'OTT Settings'** submenu, OTT (Over the Top) parameters are configured to build IPsec or GRE tunnels inside an IPSec connection from an access point.



- *Service Activator URL* – service activator URL, specified in the https://<xxx.xxx.xxx.xxx / Domain name>:<Port>;
- *IPsec Remote Gateway* – gateway for IPsec, specified in the format of IP address or domain name;
- *IPsec Operation Status* – set the flag to enable a configurable IPsec connection;

- *XAUTH User* – user name for extended authorization, necessary for the mode config mechanism to work . The parameter may contain from 4 to 16 characters;
- *XAUTH Password* – username for extended authorization, necessary for the mode config mechanism to work . The parameter may contain from 8 to 48 characters .

To go to the extended list of options, click the button with the '+' symbol next to 'Advanced Settings':



IKE Proposal:

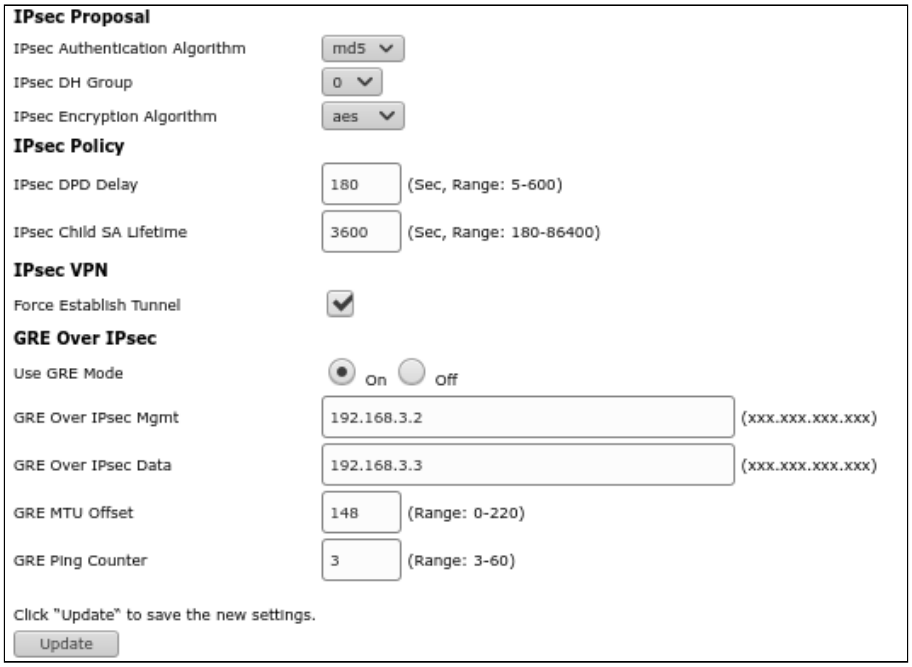
- *IKE Authentication Algorithm* – choice of IKE hashing algorithm, designed to check the integrity of data ;
- *IKE DH Group* – choice of Diffie-Hellman algorithm, used to establish a shared secret in an insecure network ;
- *IKE Encryption Algorithm* – choice of encryption algorithm for phase 1 IPsec connection.

IKE Policy:

- *Use ISAKMP Mode Config* – activate the mode of automatically obtaining a virtual address, a remote subnet, addresses for raising GRE tunnels from ESR, to which connect via IPSec;
- *IKE Lifetime* – IKE lifetime (phase 1), must be identical on both sides of the IKE/IPsec connection . The parameter takes values from 180 to 86400 seconds. By default – 86400 seconds;
- *Use NAT-T* – the flag must be enabled if the access point is behind NAT;
- *IPsec NAT Keepalive* – frequency of sending keepalive packets when working through NAT, so that NAT translation is preserved on upstream routers when the client is not active for a long time . The parameter takes values from 0 to 300 seconds. By default –180 seconds;
- *IPsec Password* – password for IKE/ISPEC connection. The parameter may contain from 8 to 48 characters ;
- *Use XAUTH Password* – if the flag is set, the previously set XAUTH Password will be used for the IKE/ ISPEC connection. If the flag is not set, the password specified in the *IPsec Password* field will be used. The field is available if *Use ISAKMP Mode Config* is enabled.

IKE Gateway – section and all its parameters are available for editing, if *Use ISAKMP Mode Config* is in *off* state*:*

- *IPsec Local Address* – client address that uses local network as IKE with a subnet mask of 255.255.255.255 (/32);
- *IPsec Remote Network* – remote IKE subnetwork;
- *IPsec Remote Mask* – remote IKE network mask.



IPsec Proposal:

- *IPsec Authentication Algorithm* – IPsec hashing algorithm for checking data integrity;
- *IPsec DH Group* – Diffie-Hellman algorithm, used to establish a shared secret in an insecure network;
- *IPsec Encryption Algorithm* – encryption algorithm for phase 1 of IPsec connection.

IPsec Policy:

- IPsec DPD Delay – interval for sending packets to detect a connection break. If there are no responses from the opposite
  side of the IPsec VPN to 5 packets in a row, the access point will consider the VPN to be broken and will restart the IPsec VPN from its side. The parameter may take values from 5 to 600 seconds. By default – 180 seconds;
- *IPsec Child SA Lifetime* – IPsec VPN SA lifetime (phase 2), must be the same on both sides of the IKE/ IPsec tunnel. Must be lower than IKE Lifetime. The parameter may take values from 180 to 86400 seconds. By default – 3600 seconds.

IPsec VPN:

- *Force Establish Tunnel* – enable to establish IPsec VPN connection immediately. Otherwise, the IPsec VPN connection will be established upon request.

GRE Over IPsec:

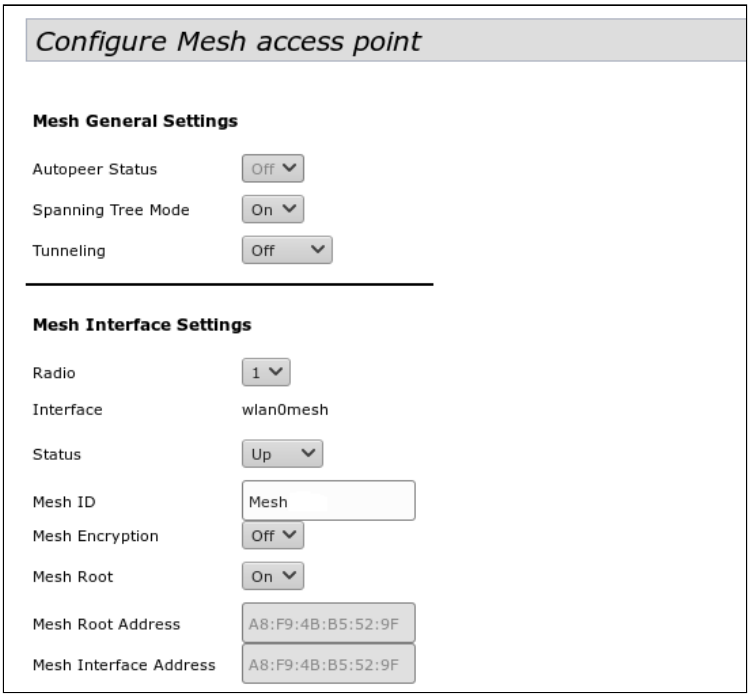
- *Use GRE Mode* – enable or disable GRE over IPsec. When enabled, the following parameters are available for editing:
  - *GRE Over IPsec Mgmt* – GRE IP address for management tunnel;
  - *GRE Over IPsec Data* – GRE IP address for data management tunnel;
  - *GRE MTU Offset* – specifies MTU reduction for GRE tunnels. GRE tunnels will be assigned an MTU based on a calculation of 1500 – *GRE MTU Offset*. The parameter may take values from 0 to 220;
  - *GRE Ping Counter* – check that GRE tunnel is still up by sending ping to GRE IP-management every 10 seconds. This value determines how many ping packets can be lost before the access point restarts the IPsec connection. The parameter takes values from 3 to 60.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

4.5.19 'Mesh'* submenu

In the **'Mesh'** submenu, communication between access points via a wireless Mesh network is configured.

* The submenu is available if the access point has software that supports Mesh (for example, WEP-2ac-1.14.0.X-MESH.tar.gz and later).



Mesh General Settings – in this section, general Mesh parameters are configured.

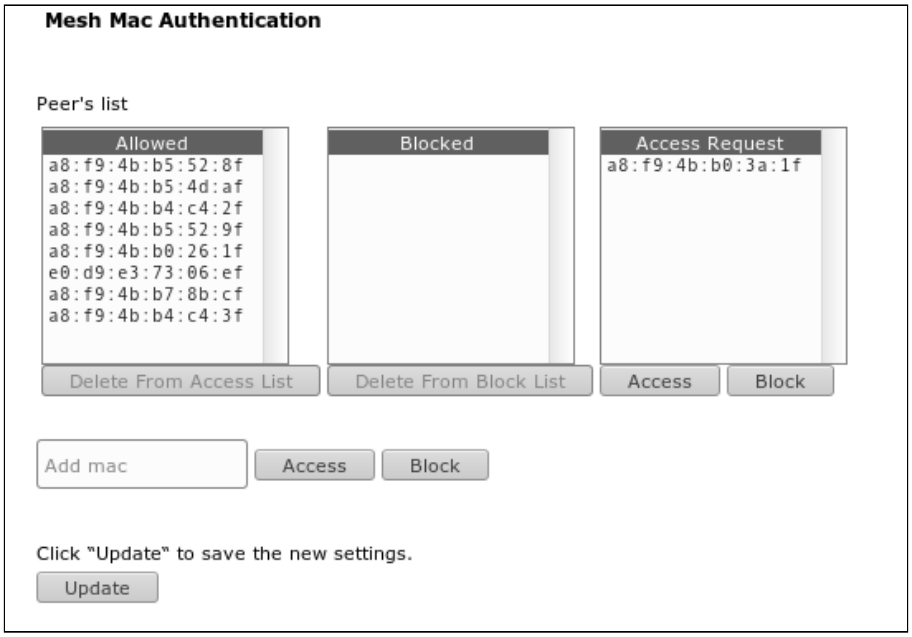
- *Autopeer Status* – autoconfiguration status of the access point. Must be disabled on the wired point (Root) and enabled on the wireless ones.
- *Spanning Tree Mode* – STP protocol operating mode to prevent loops in the network;
- *Tunneling* – available only when using GRE:
  - *Off* – GRE is not used, the Tunneling option is disabled;
  - *Master* – access point is connected to the network via Ethernet interface;
  - *Slave* – access point is connected to the Master point via radio interface.

Mesh Interface Settings – in this section, interface is configured for Mesh organization. The section is available only on the Root point, i.e. when the *Autopeer Status* is *off*.

- *Radio* – selection of the radio interface for organizing Mesh;

On WEP-2ac/WEP-2ac type points, Smart Mesh is only supported on Radio 1 (5 GHz).

- *Interface* – interface used to organize Mesh;
- *Status* – state of the configured Mesh interface;;
- *Mesh ID* – name of the Mesh network;
- *Mesh Encryption* – use Mesh network with encryption (on – enable, off – disable);
- *Mesh Root* – assign an access point as a controller in the Mesh network (must be an entry point/wired);
- *Root Address* – MAC interface address of the access point that is the controller (filled in automatically);
- *Mesh Interface Address* – MAC address of the Mesh interface of the configured access point.



Mesh Mac Authentication – in the section, members of the Mesh network can be added/removed.

- *Allowed* – access points added to the 'Allowed' list are allowed to access the Mesh network:
  - *Delete From Access List* – remove the selected MAC address from the list of allowed addresses.
- *Blocked* – access points added to the 'Blocked' list are denied access to the Mesh network:
  - *Delete From Block List* – remove the selected MAC address from the list of denied addresses.
- *Access Request* – list of access points that sent a request to connect to the Mesh network:
  - *Access* – adding access point to the white list (access is allowed);
  - *Block* – adding access point to the black list (access denied).

To add an access point to the *Allowed/Blocked* list manually, enter the point's MAC address in the *'Add mac'* field and click the corresponding button:

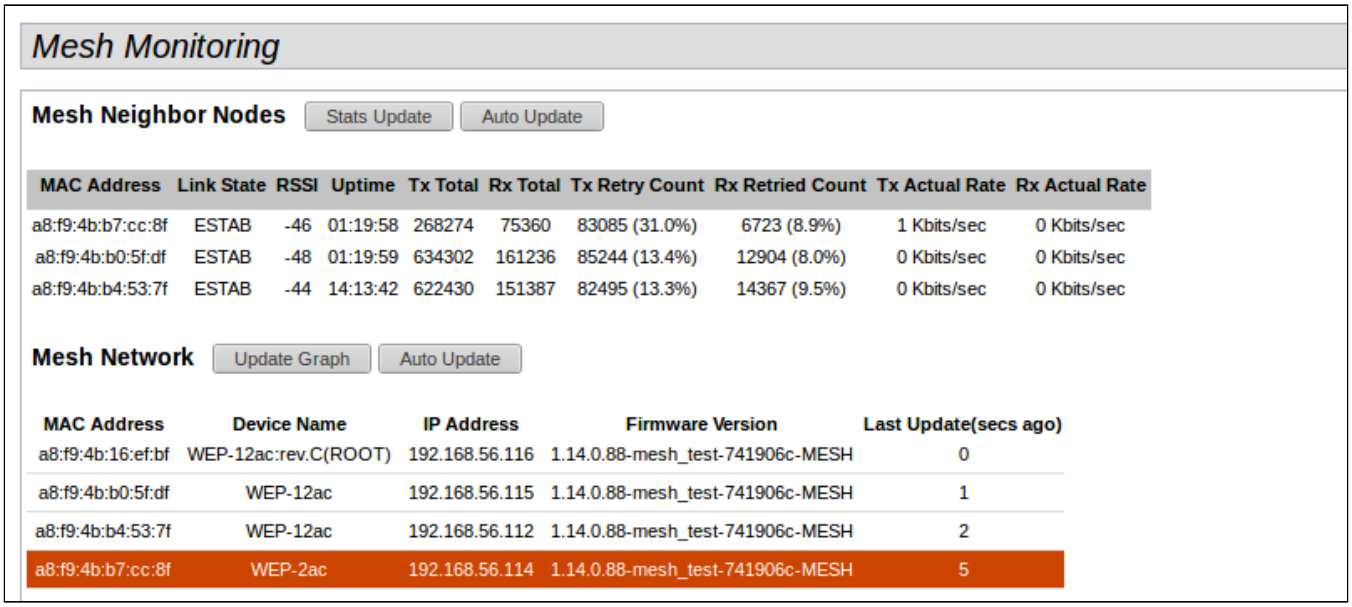
- *Access* – adding access point to the white list;
- *Block* – adding access point to the black list.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

4.5.20 'Mesh Monitoring'* submenu

In the '**Mesh Monitoring**' submenu, statistics and status of connections in the Mesh network are displayed.

* The submenu is available if the access point has software that supports Mesh (for example, WEP-2ac-1.14.0.X-MESH.tar.gz and later).



Mesh Neighbor Nodes – in this section, a table with statistics of connections with neighboring access points is displayed.

Stats Update – when clicking the button, the statistics in the table will be updated;

Auto Update – automatic table update (data is updated once a second);

- *MAC Address* – MAC address of the Mesh interface of the neighboring access point;
- *Link State* – connection state;
- *RSSI* – signal level from a neighboring access point;
- *Uptime* – duration of the connection with the access point;
- *Tx Total* – number of successfully sent packets;
- *Rx Total* – number of successfully received packets;
- *Tx Retry Count* – number of resent packets;
- *Rx Retried Count* – number of received packets resent;
- *Tx Actual Rate* – current data transfer rate, in kbps;
- *Rx Actual Rate* – current data reception rate, in kbps.

Mesh Network – table with information about Mesh network members is displayed.

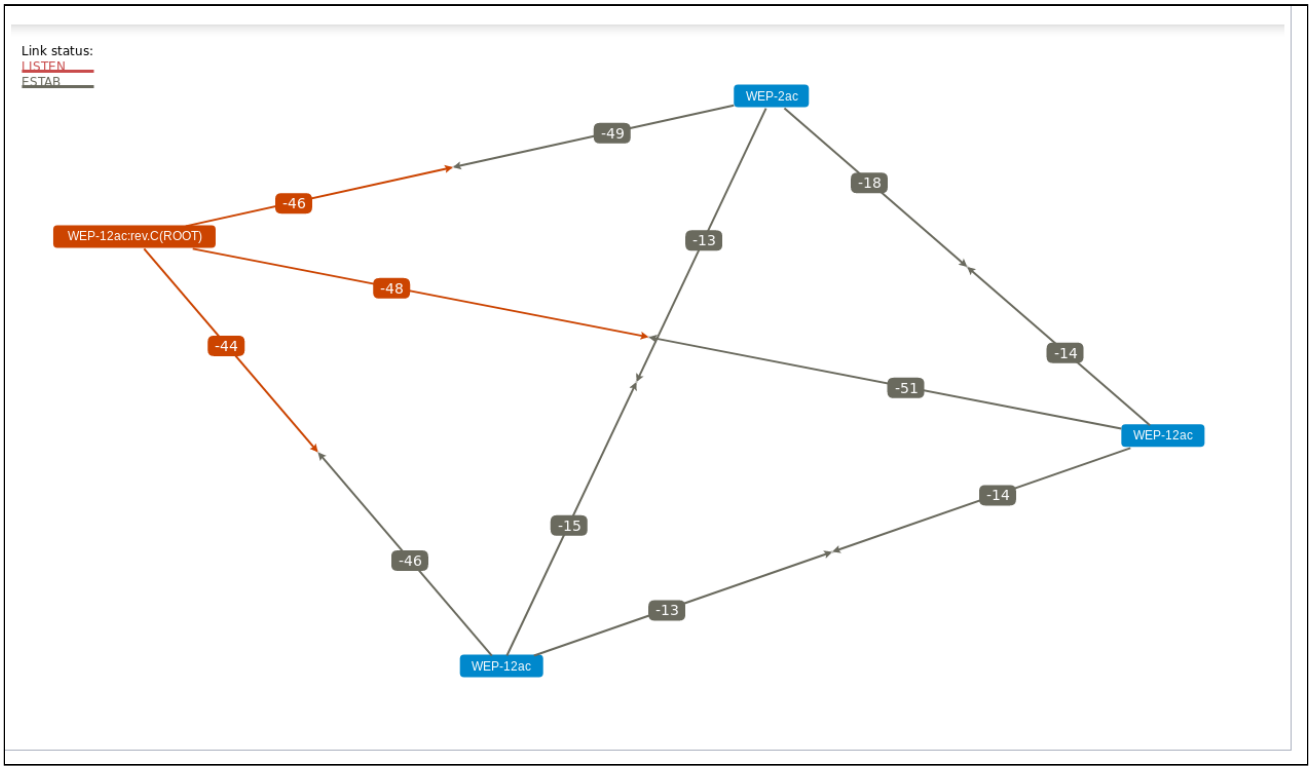
Displayed only on a Mesh Controller (Root AP) device.

Update Graph – when clicking the button, the information in the table and graph will be updated;

Auto update – automatic update of the table and graph (data is updated every 10 seconds);

- *MAC Address* – MAC address of the network member Mesh interface;
- *Device Name* – device system name;
- *IP Address* – device IP address;
- *Firmware Version* – firmware version;
- *Last Update* – time of the last synchronization with the device.

The monitoring section contains a graph with a constructed Mesh network diagram. Based on the table and graph, the network can be analyzed. This will allow assessing the correct location of access points across the coverage area and indicate problem areas, as well as help to monitor the network in real time.

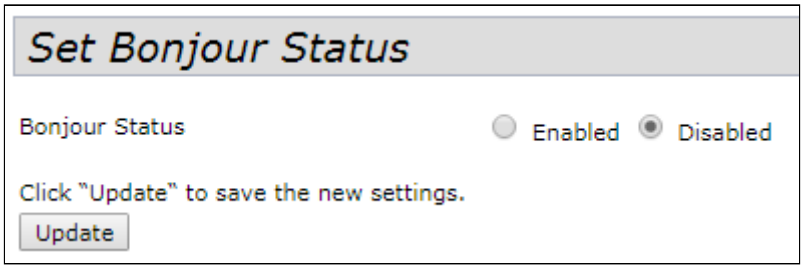


4.6 'Services' menu

In the '**Services**' menu, built-in services of the access point are configured.

4.6.1 'Bonjour' submenu

In the **'Bonjour'** submenu, the Bonjour service is configure. The services allows wireless access points and their services to discover each other within the local network using entries in the multicast Domain Name System (mDNS).

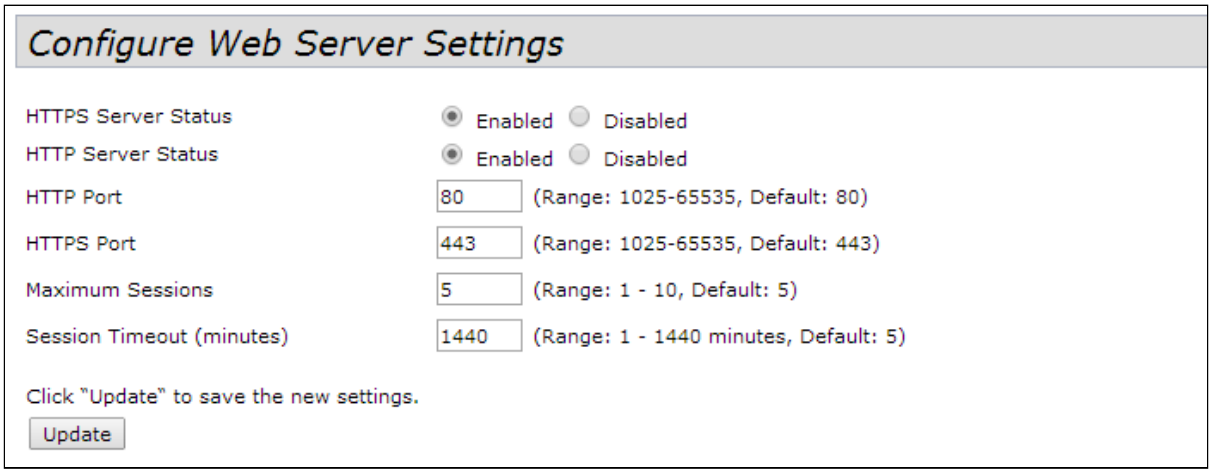


Bonjour Status – Bonjour service status:
- *Enabled* – if the flag is set, the service is active;
- *Disabled* – if the flag is set, the service is disabled.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

4.6.2 'Web Server' submenu

In the '**Web Server**' submenu, access to the access point via web interface is configured.



- *HTTPS Server Status* – HTTPS server status:
  - *Enabled* – if the flag is set, connection to the device web interface will be via secure HTTP protocol (HTTPS);
  - *Disabled* – if the flag is set, connection to the device web interface is not available via HTTPS protocol.
- *HTTP Server Status* – HTTPS server status, this parameter does not depend on the state of the settings of the 'HTTPS Server Status' parameter:
  - *Enabled* – if the flag is set, connection to the device web-interface will be allowed via HTTP protocol;
  - *Disabled* – if the flag is set, connection to the device web-interface is not available via the HTTP protocol.
- *HTTP Port* – port number for HTTP traffic transmission. The parameter takes values from 1025 to 65535. By default – 80;

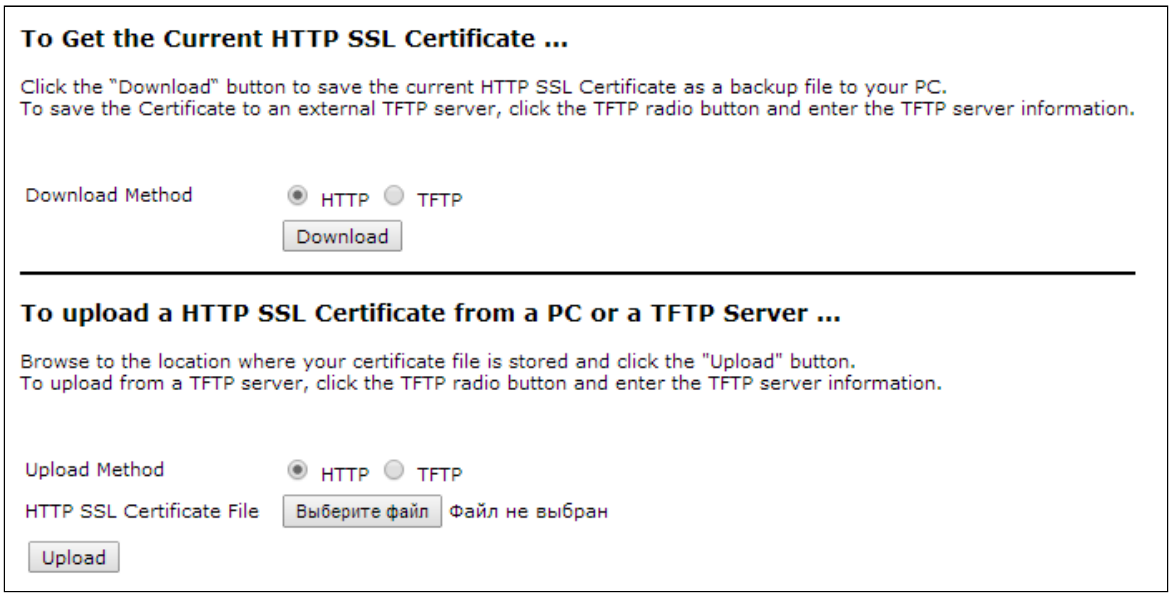
- *HTTPS Port* – port number for HTTPS traffic transmission. The parameter takes values from 1025 to 65535. By default – 443;
- *Maximum Sessions* – number of web sessions, including HTTP and HTTPs, that can be running at the same time. The parameter takes values from 1 to 10 sessions. By default – 5;
- *Session Timeout (minutes)* – period of time after which the system will automatically exit the web interface if the user has not been active. The parameter takes values from 1 to 1440 minutes. By default – 60 minutes.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

Generate HTTP SSL Certificate – in this section, by clicking the 'Update button', a new HTTP SSL certificate is generated for secure access to the web server. This action must be performed when obtaining an IP address so that the name of the certificate matches the IP address of the device. When a new certificate is created, the security web server will be started. The secure connection will not function until the new certificate is applied in the browser.

HTTP SSL Certificate File Status – in this section, information about the HTTP SSL certificate is provided.:

- *Certificate File Present* – indicates if an SSL HTTP certificate is present;
- *Certificate Expiration Date* – date until which the certificate is valid;
- *Certificate Issuer Common Name* – name of the certificate.



To Get the Current HTTP SSL Certificate – in this section, the current HTTP SSL certificate is saved, which can later be used as a backup file:

Download Method – HTTP SSL certificate saving method:

- *HTTP* – file will be saved via HTTP to PC;
- *TFTP* – certificate will be saved on the TFTP server; when specifying this method, the following fields must be filled in:

- *HTTP SSL Certificate File* – certificate file name specified as a string of up to 256 characters;
- *Server IP* – IPv4 or IPv6 address of the TFTP server that will be used to upload the file.

To save the HTTP SSL certificate file, click the 'Download' button.

To upload a HTTP SSL Certificate from a PC or a TFTP Server – in this section, the HTTP SSL Certificate file is uploaded:

Upload Method – method for uploading an HTTP SSL certificate file:

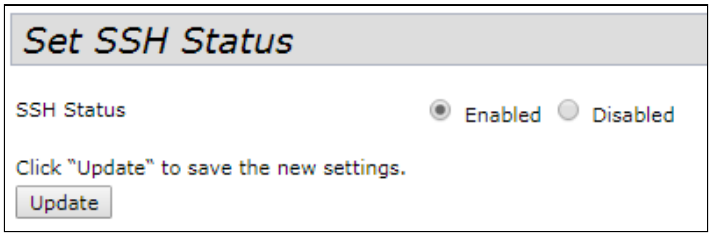
- *HTTP* – via HTTP. When specifying this method, click the 'Select file' button, specify the file to be downloaded to the device;
- *TFTP* – via a TFTP server. When specifying this method, fill in the following fields:
  - *HTTP SSL Certificate File* – certificate file name specified as a string of up to 256 characters;
  - *Server IP* – IPv4 or IPv6 address of the TFTP server that will be used to upload the file.

To upload the file to the device, click the 'Upload' button.

4.6.3 'SSH' submenu

In the '**SSH**' submenu, access to the device via SSH protocol is configured.

SSH is a secure protocol for remote device management. Unlike Telnet, the SSH protocol encrypts all traffic, including transmitted passwords.



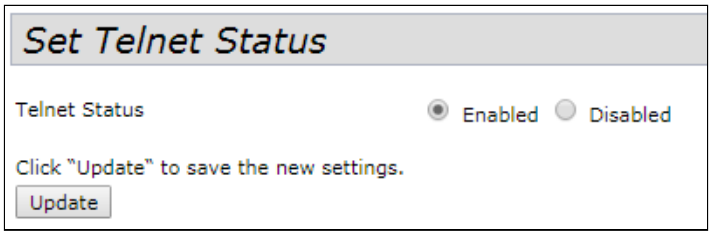
SSH Status – status of access to device via SSH protocol:

- *Enabled* – if the flag is set, access is allowed;
- *Disabled* – if the flag is set, access is denied.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

4.6.4 'Telnet' submenu

In the '**Telnet**' submenu, access to device via Telnet protocol is configured.
Telnet is a protocol for organizing management over a network. Allows remotely connecting to the gateway from a computer for configuration and management.



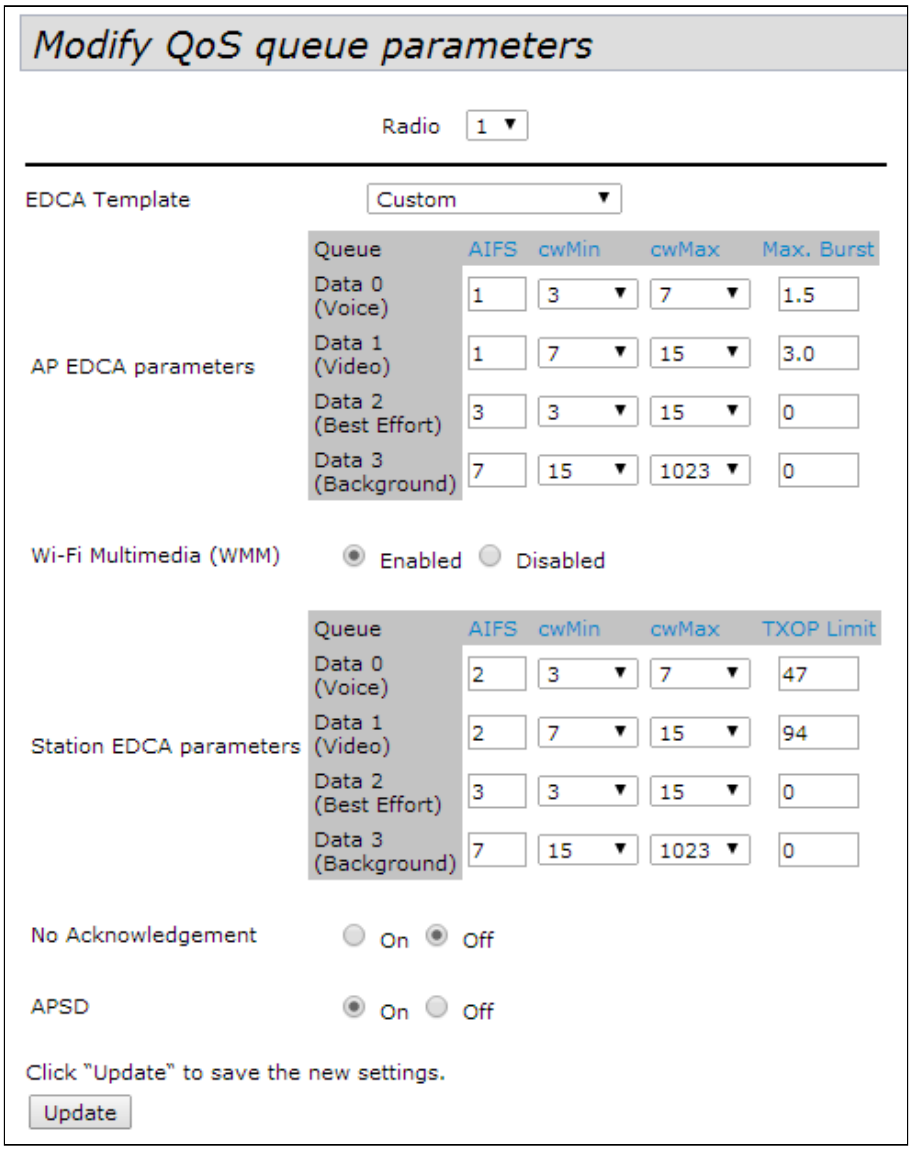
Telnet Status – status of access to device via Telnet protocol:

- *Enabled* – if the flag is set, access is allowed;
- *Disabled* – if the flag is set, access is denied.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

4.6.5 'QoS' submenu

In the '**QoS**' submenu, the Quality of Service functions are configured. QoS is configured for each radio interface.
QQoS is used to ensure minimum latency in the transmission of data for services such as voice over IP (VoIP), real-time video, and other time-sensitive services.



Radio – radio interface for which QoS will be configured;

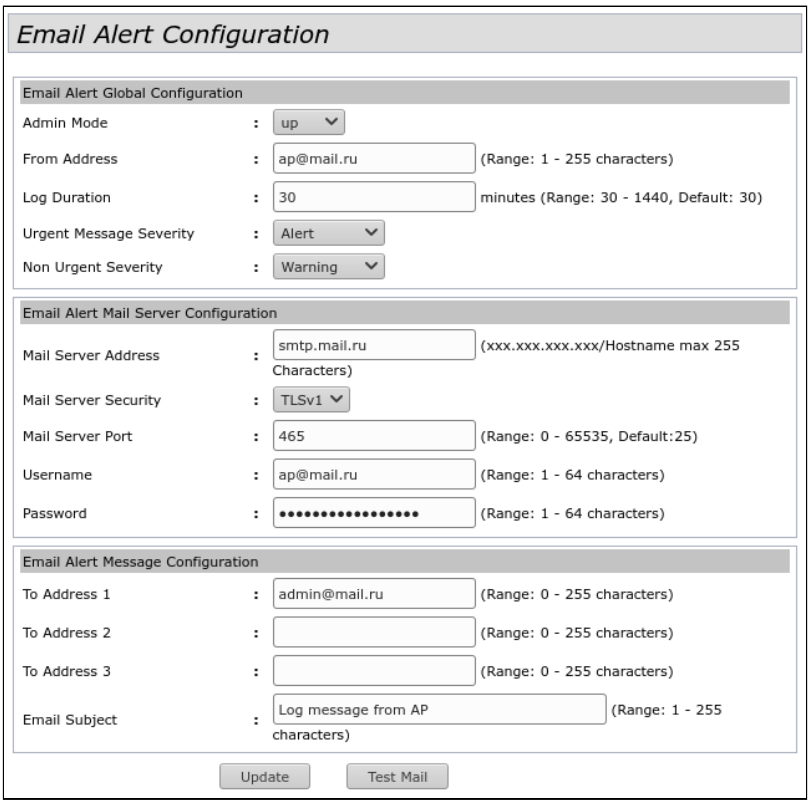
- *EDCA Template* – template with predefined EDCA parameters:
  - *Default* – default settings;
  - *Optimized for Voice* – optimal settings for voice transmission;
  - *Custom* – user settings.
- *AP EDCA Parameters* – table of settings for access point parameters (traffic is transmitted from the access point to the client):
  - *Queue* – predefined queues for various types of traffic:
  - *Data 0 (Voice)* – high priority queue, minimum delays. This queue automatically handles time-sensitive data such as VoIP and streaming video;
  - *Data 1 (Video)* – high priority queue, minimum delays. Time-sensitive video data is automatically processed in this queue;
  - *Data 2 (best effort)* – medium priority queue, average throughput and delay. Most traditional IP data is sent to this queue;

    - *Data 3 (Background)* – low priority queue, high throughput;
    - *AIFS* (Arbitration Inter-Frame Spacing) – defines the waiting time for data frames. The parameter takes values from 1 to 15, and is measured in slots;
    - *cwMin* – initial value of waiting time before resending a frame. The parameter takes values 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023 in milliseconds. The cwMin value cannot exceed the cwMax value;
    - *cwMax* – maximum waiting time before resending a frame. The parameter takes values 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023 in milliseconds. The cwMax value must be greater than the cwMin value;
    - *Max. Burst* – parameter is used only for data transmitted from the access point to the client station. The maximum packet length allowed for wireless queues is 0-999.
- *Wi-Fi MultiMedia (WMM)* – state of the WiFi Multimedia function, which allows optimizing the transmission of multimedia traffic over a wireless environment:
    - *Enable* – function is enabled;
    - *Disable* – function is disabled.
- *Station EDCA Parameters* – table of client station settings (traffic is transmitted from the client station to the access point):
    - Description of the *Queue, AIFS, cwMin, cwMax* parameters is given above;
    - *TXOP Limit* – parameter is used only for data transmitted from the client station to the access point. Transmit capability - time interval in milliseconds, when a client WME station has rights to initiate data transmission over the wireless medium to the access point, the maximum value is 65535 milliseconds.
- *No Acknowledgement* – if the 'On' flag is set, the access point should not recognize QosNoAck frames as a class of service value;
- *APSD* – if the 'On' flag is set, the APSD delivery power saving mode, which is a power management method, will be enabled. This mode is recommended if network access is provided for VoIP phones through an access point.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

4.6.6 'Email Alert' submenu

In the '**Email Alert**' submenu, sending of service information by e-mail can be configured.



In the '**Email Alert Global Configuration**' section, global settings for the function of sending Email messages are set.

- *Admin Mode* – state of the function of sending Email messages on the access point::
  - *Up* – function is enabled;
  - *Down* – function is disabled.
- *From Address* – sender's mailing address specified as a string of up to 255 characters;
- *Log Duration* – time intervals for sending non-critical messages. The parameter takes values from 30 to 1440. By default – 30;
- *Urgent Message Severity* – severity level of messages that will be sent immediately;
- *Non Urgent Severity* – severity level of messages that will be sent within 'Log Duration' intervals.

In the '**Email Alert Mail Server Configuration**' section, mail server and client are configured.

- *Mail Server Address* – mail server address, a string of the XXX.XXX.XXX.XXX format;
- *Mail Server Security* – authentication protocol on the mail server: Open, TLSv1. By default – Open;
- *Mail Server Port* – mail server port number. The parameter takes values from 0 to 65535. By default– 25;
- *Username* – mail client name specified as a string of up to 64 characters;
- Password – mail client password specified as a string of up to 64 characters.

In the '**Email Alert Message Configuration**' parameters of the alarm message are configured:

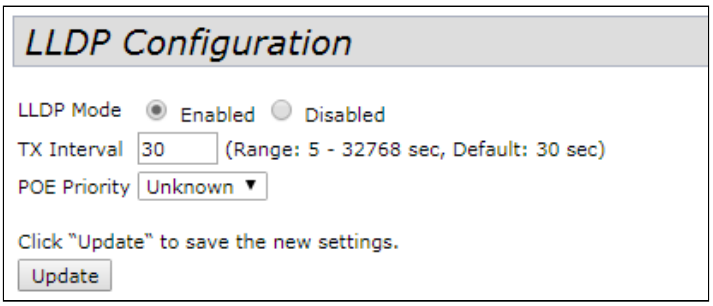
- *To Address 1* – address of the first message recipient;
- *To Address 2* – address of the second message recipient;
- *To Address 3* – address of the third message recipient;
- *Email Subject* – text in the email subject.

To send a test message, click the 'Test Mail' button.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

4.6.7 'LLDP' submenu

In the '**LLDP**' submenu, operation of the LLDP (Link Layer Discovery Protocol) protocol is configured.

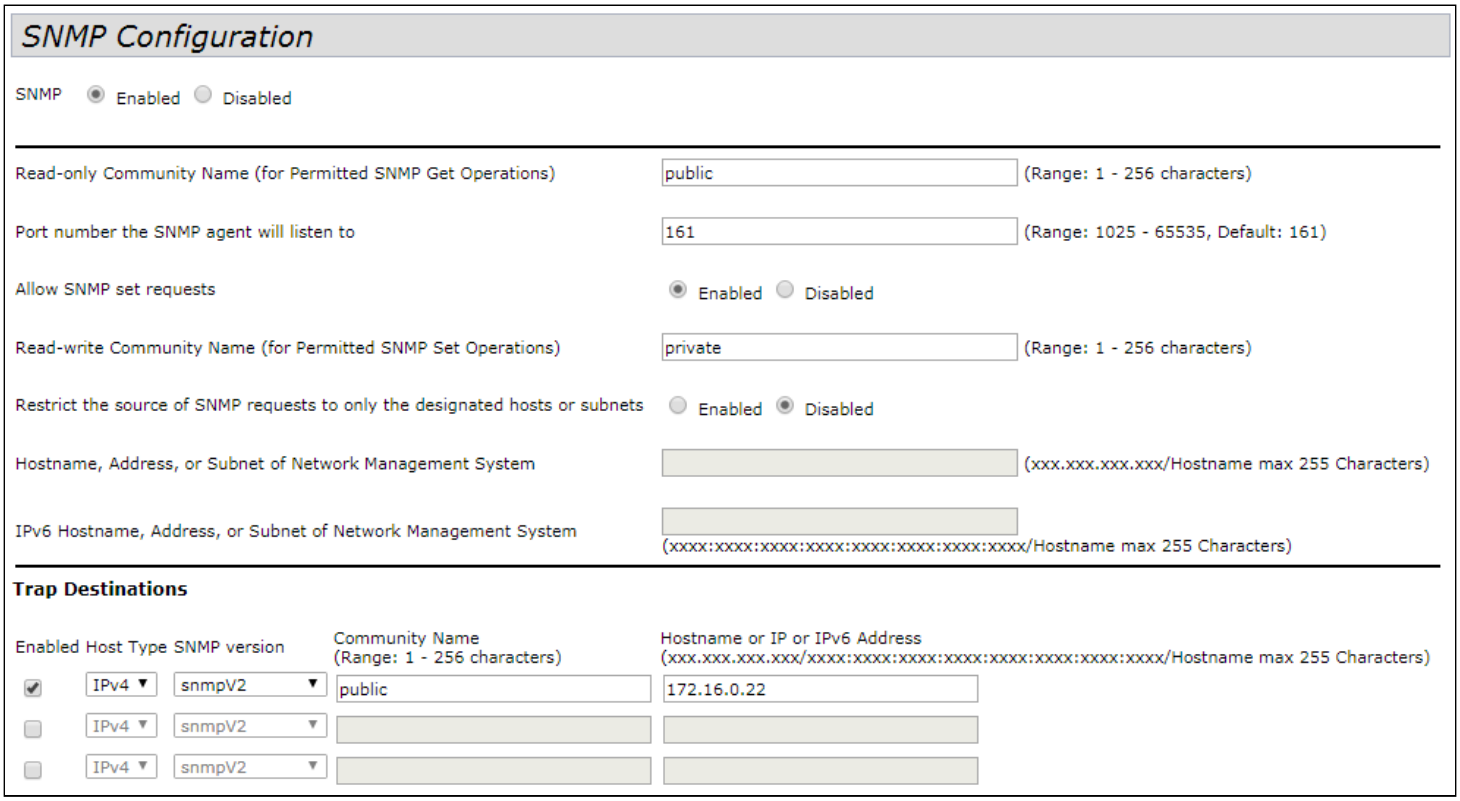


- *LLDP Mode* – state of the LLDP protocol:
  - *Enabled* – when the flag is set, LLDP is active;
  - *Disabled* – when the flag is set, LLDP is disabled.
- *TX Interval* – LLDP message sending interval. The parameter takes values from 5 to 32768 seconds. By default – 30 seconds;
- *POE Priority* – priority sent in the 'Extended Power Information' field.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

4.6.8 'SNMP' submenu

In the '**SNMP**' submenu, device management via SNMP can be configured.



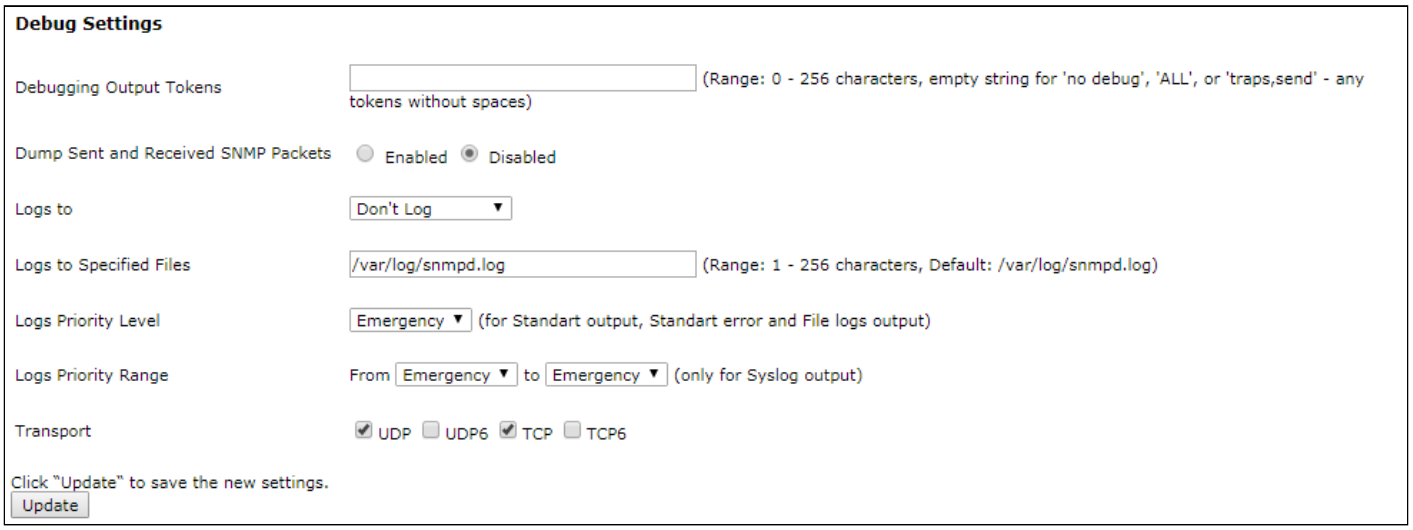
- *SNMP* – enable/disable device management via SNMP:
  - *Enabled* – when the flag is set, SNMP is active;
  - *Disabled* – when the flag is set, SNMP is disabled;
- *Read-only community name* – password for read-only requests, specified as string from 1 to 256 characters long;

- *Port number the SNMP agent will listen to* – port number for receiving/sending SNMP messages. The parameter takes values from 1025 to 65535. By default – 161;
- *Allow SNMP set requests* – enable/disable device configuration via SNMP:
  - *Enabled* – enable device configuration via SNMP:
    - *Read-write community name* – password for read-write requests, specified as string from 1 to 256 characters long;
  - *Disabled* – disable device configuration via SNMP;
- *Restrict the source of SNMP requests to only the designated hosts or subnets* – accept SNMP requests only from the specified addresses. IP address specified as XXX.XXX.XXX.XXX or host name. If enabled, fill in the following parameters:
  - *Hostname, Address, or Subnet of Network Management System* – name, address or IPv4 network from which SNMP requests are allowed to be received;
  - *IPv6 hostname, address, or subnet of Network Management System* – name, address or IPv6 network from which SNMP requests are allowed to be received.

Trap Destinations – configuring the sending of SNMP traps to a remote server:

- *Enabled* – enable trap sending;
- *Host Type* – specify whether the enabled host is an IPv4 host or an IPv6 host.
- *SNMP version* – SNMP protocol version;
- *Community Name* – enter community name specified as string from 1 to 256 characters long;
- *Hostname or IP or IPv6 Address* – enter DNS name or server IP address, to which the access point will send SNMP traps.

In the **'Debug Settings'** section sending of debug messages is configured.

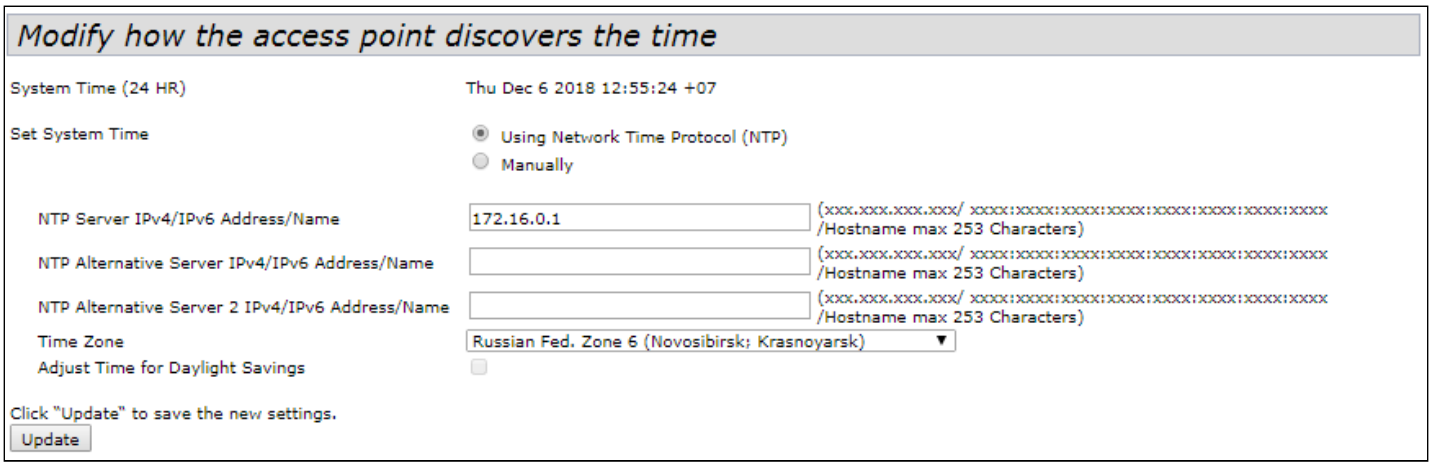


- *Debugging Output Tokens* – identifier of the group of debugging messages;
- *Dump Sent and Received SNMP Packets* – output of the received and transmitted SNMP messages to the log;
- *Logs to* – log output location:
  - *Don't Log* – do not output the log;
  - *Standart Error, Standart Output* – output to the console;
  - *File* – output to the file;
  - *Syslog* – Syslog output;
- *Logs to Specified Files* – specifying a file for log output;
- *Logs Priority Level* – level of output logs specified at log output to the console or file;
- *Logs Priority Range* – specifying the range of log levels for Syslog output;
- *Transport* – transport protocol used to transmit SNMP messages.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

4.6.9 'Time Settings (NTP)' submenu

In the **'Time Settings (NTP)'** submenu local time of the device can be configured.



- *System Time (24 HR)* – current system time;
- *Set System Time* – selection of the time setting method:
  - *Using Network Time Protocol (NTP)* – automatic installation using the NTP protocol;
  - *Manually* – manual time installation.

Automatic installation using NTP protocol (Using Network Time Protocol (NTP) is selected):

- *NTP Server IPv4/IPv6 Address/Name* – IPv4 address, IPv6 address or NTP server host name. If a server is not specified, the name of the server received in the DHCP option will be used;
- *NTP Alternative Server IPv4/IPv6 Address/Name и NTP Alternative Server 2 IPv4/IPv6 Address/Name* – specify IPv4 address, IPv6 address host name of the additional NTP servers. If a server is not specified, the name of the server received in the DHCP option will be used.

Manual time installation (Manually is selected):

- *System Date* – date installation;
- *System Time (24 HR)* – system time installation in 24-hour format.

- *Time Zone* – time zone, Russia (Moscow) is installed by default;
- *Adjust Time for Daylight Savings* – when selected, daylight saving change will be performed automatically. When the flag is set, the fallowing fields are available:
  - *DST Start (24 HR)* – time when daylight saving time is starting;
  - *DST End (24 HR)* – time when daylight saving time is ending;
  - *DST Offset (minutes)* – set time offset (in minutes).

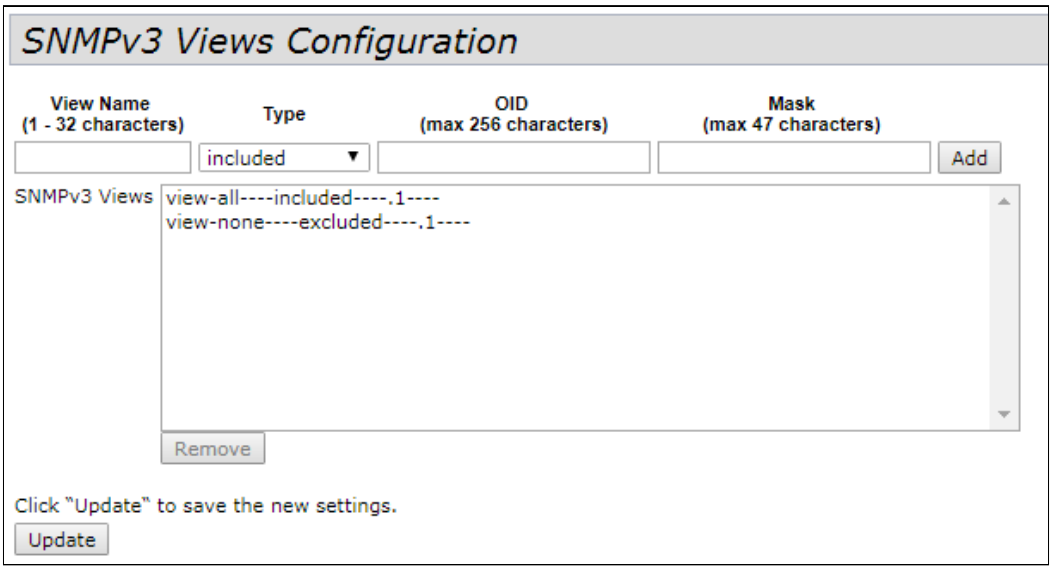
To apply a new configuration and save setting to non-volatile memory, click 'Update'.

4.7 'SNMPv3' menu

In the **'SNMPv3'** menu, SNMP protocol version 3 is being configured**.**

4.7.1 'SNMPv3 Views' submenu

In the **'SNMPv3 Views'** menu, a description of the OID tree or subtree is formed, as well as the inclusion or exclusion of the subtree from the view.



- *View Name* – name of the MIB tree or subtree specified as string of up to 32 characters;
- *Type* – include or exclude the MIB subtree from the view:
  - included – include MIB subtree;
  - excluded – exclude MIB subtree.
- *OID* – OID string describing the subtree to be included or excluded from the view, specified as string of up to 256 characters;
- *Mask* – mask specified in the xx.xx.xx....(.) format not longer than 47 characters, used to form the required subtree within the specified OID;
- *SNMPv3 Views* – list of existing rules.

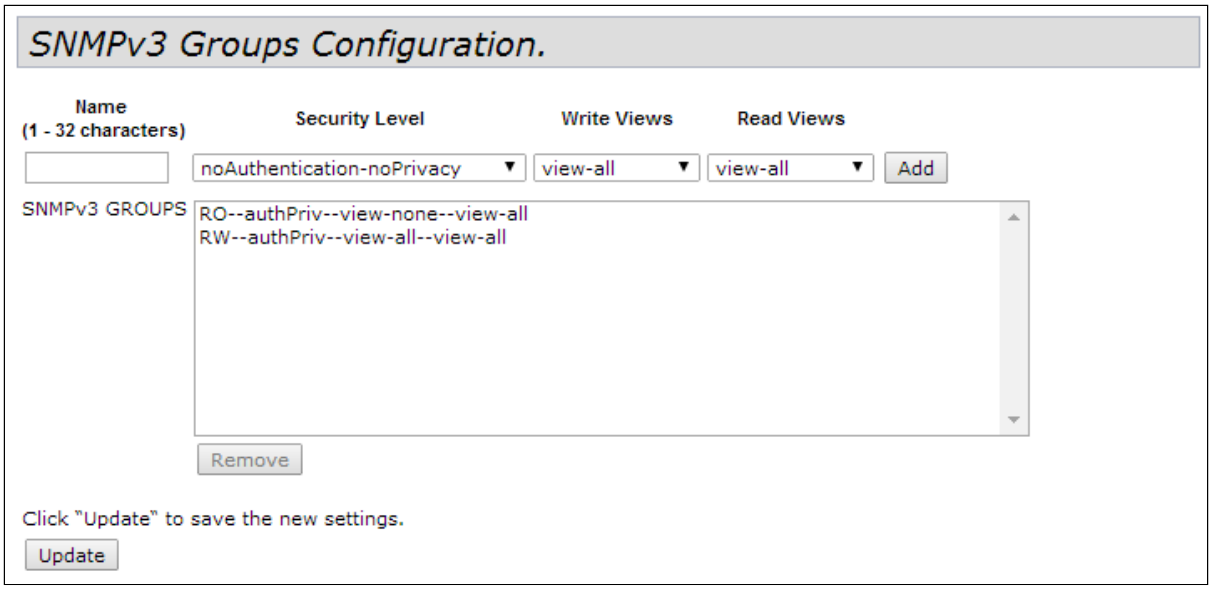
To add a rule, click 'Add'.

To remove rule from the 'SNMPv3 *Views'* field, select entry and click 'Remove'.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

4.7.2 'SNMPv3 Groups' submenu

In the **'SNMPv3 Groups'** submenu groups are formed with different security levels applied to tree and subtree browsing rules.



- *Name* – group name specified as string of up to 32 characters;
- Security Level – security level for the group:
  - *noAuthentication-noPrivacy* – authentication and data encryption are not used;
  - *Authentication-noPrivacy* – authentication is used, but data encryption is not used. When sending SNMP messages, an MD5 key and password are used for authentication;
  - *Authentication-Privacy* – authentication and data encryption are used. When sending SNMP messages, an MD5 key/password is used for authentication, and a DES key/password is used for data encryption.
- *Write Views* – selection of the OID tree/subtree available for writing:
  - *view-all* – group can create, modify and delete MIBs;
  - *view-none* – group is not allowed to create, modify, or delete MIBs.
- *Read Views* – selection of OID tree/subtree available for reading:
  - *view-all* – group is allowed to view and read all MIB files;
  - *view-none* – group is not allowed to view and read MIB files.
- *SNMPv3 GROUPS* – list of existing groups.

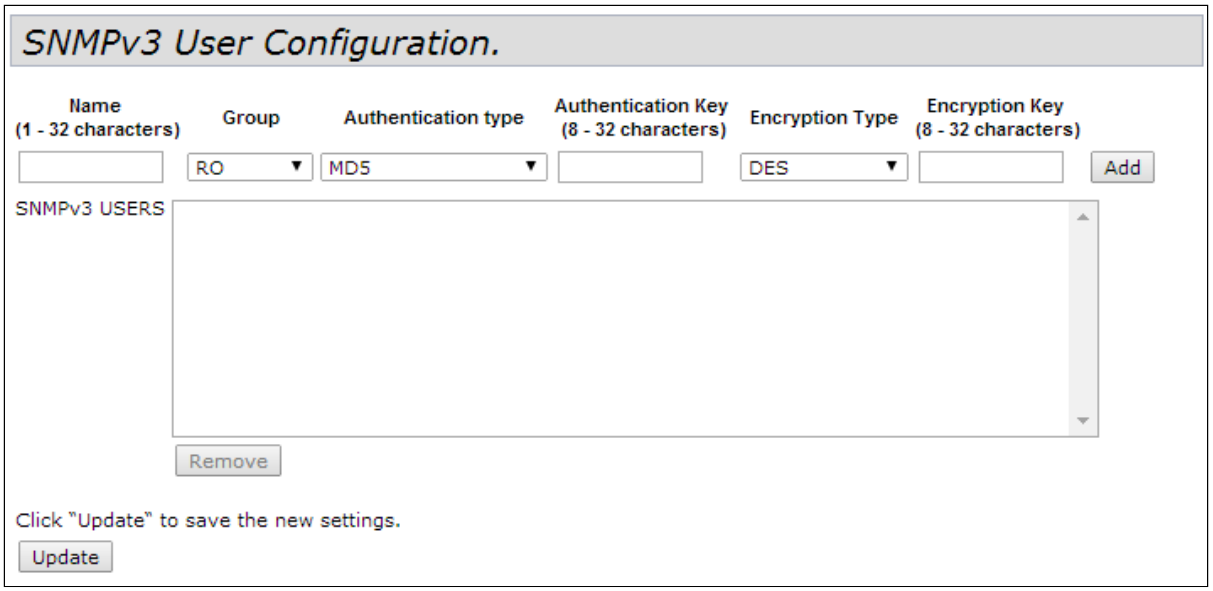
To add a rule, click 'Add'.

To remove group from the 'SNMPv3 GROUPS' field, select entry and click 'Remove'.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

4.7.3 'SNMPv3 Users' submenu

'SNMPv3 Users' submenu is used to create users and their access parameters that work with the device via the SNMPv3 protocol.



- *Name* – user name specified as string of up to 32 characters;
- *Group* – group created in the 'SNMPv3 Groups' submenu;
- *Authentication type* – authentication type for using SNMP request:
  - *MD5* – MD5 authentication is required for SNMPv3 user requests;
  - *None* – no authentication is required when sending SNMPv3 requests from this user.
- *Authentication Key* – authentication key specified as string from 8 to 32 characters. It is used if the 'MD5' value is selected in the 'Authentication type' field;
- *Encryption Type* – encryption type:
  - *DES* – use the DES encryption algorithm for user SNMPv3 requests;
  - *None* – no encryption is required when sending SNMPv3 requests from this user.
- *Encryption Key* – encryption key specified as string from 8 to 32 characters. It is used if the 'DES' value is selected in the 'Encryption Type' field.

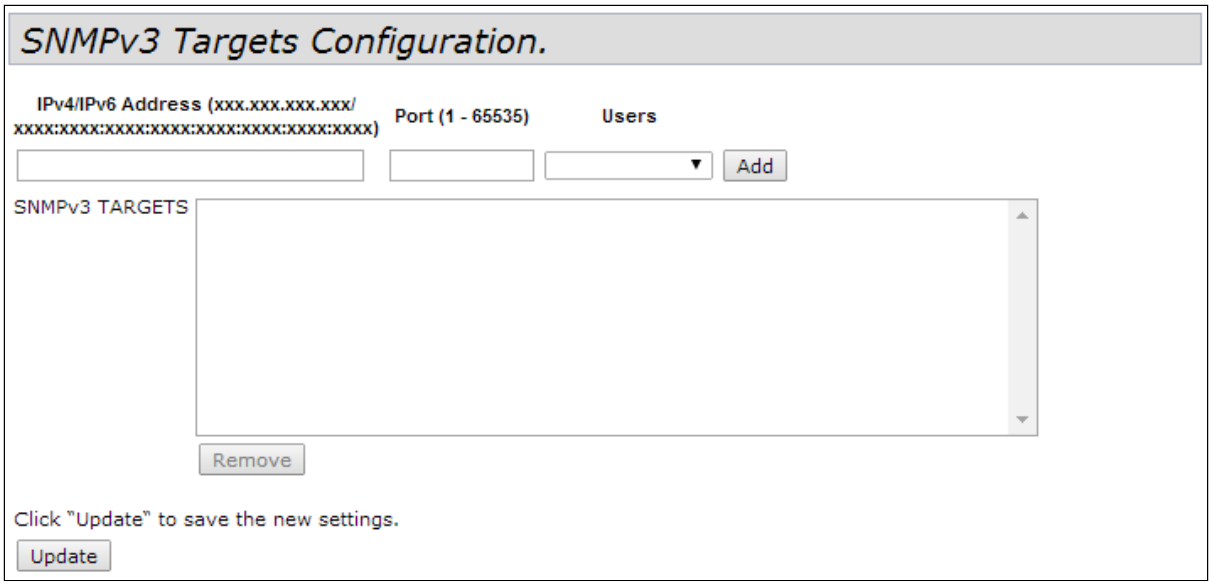
To add a user, click 'Add'.

To remove group from the 'SNMPv3 USERS' field, select entry and click 'Remove'.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

4.7.4 'SNMPv3 Targets' submenu

In the **'SNMPv3 Targets'** to configure sending of traps from the device to a specific IP address, UDP port, and user.



- *IPv4/IPv6 Address* – IPv4 or IPv6 address to which traps will be sent;
- *Port* – UDP port to which the traps will be sent. The parameter takes values from 1 to 65535;
- *Users* – name of the user to which the traps will be sent.

To add rule for trap sending, click 'Add'.

To remove rule for trap sending from the 'SNMPv3 TARGETS' field, select entry and click 'Remove'.

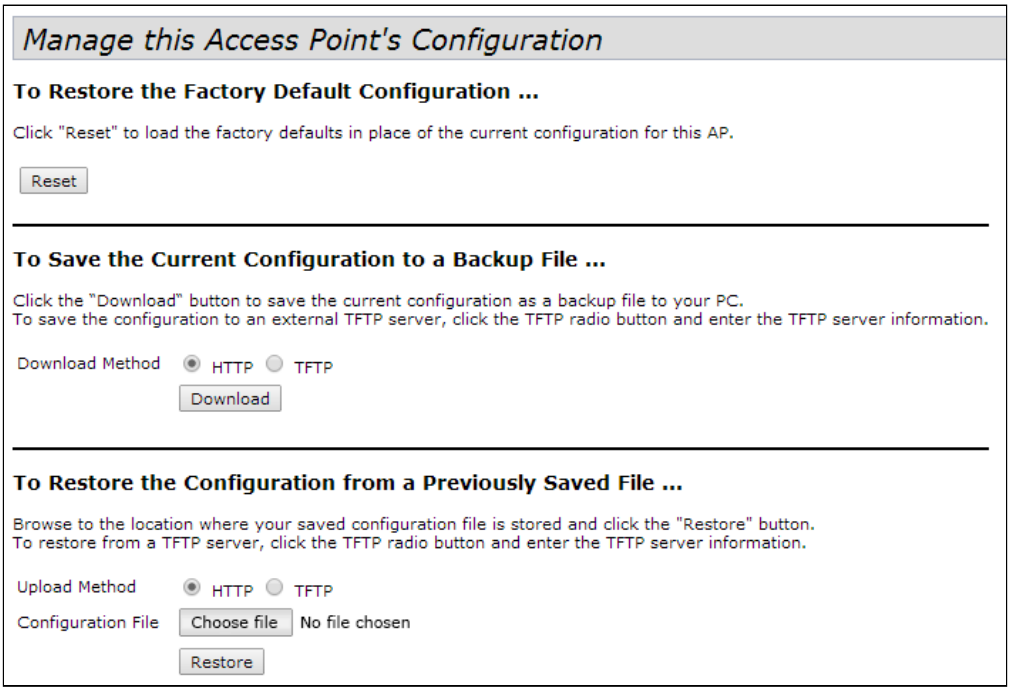
To apply a new configuration and save setting to non-volatile memory, click 'Update'.

4.8 'Maintenance' menu

'Maintenance' menu is intended for general device management: uploading, downloading, setting the default configuration, updating firmware, rebooting the device, as well as for debugging operations: sniffing traffic passing through the access point and uploading diagnostic information on the device.

4.8.1 'Configuration' submenu

The uploading and downloading of the device configuration, resetting of the device to its default configuration, and rebooting of the device can be performed by the **'Configuration'** submenu.



To Restore the Factory Default Configuration – reset device to factory defaults.

To reset the device configuration to factory settings, click the 'Reset' button. After the reset, the device will automatically reboot. The whole process will take a few minutes.

> Resetting to factory settings will delete the entire configuration of the device, including the IP address for accessing the device. After performing this operation, communication with the device may be lost.

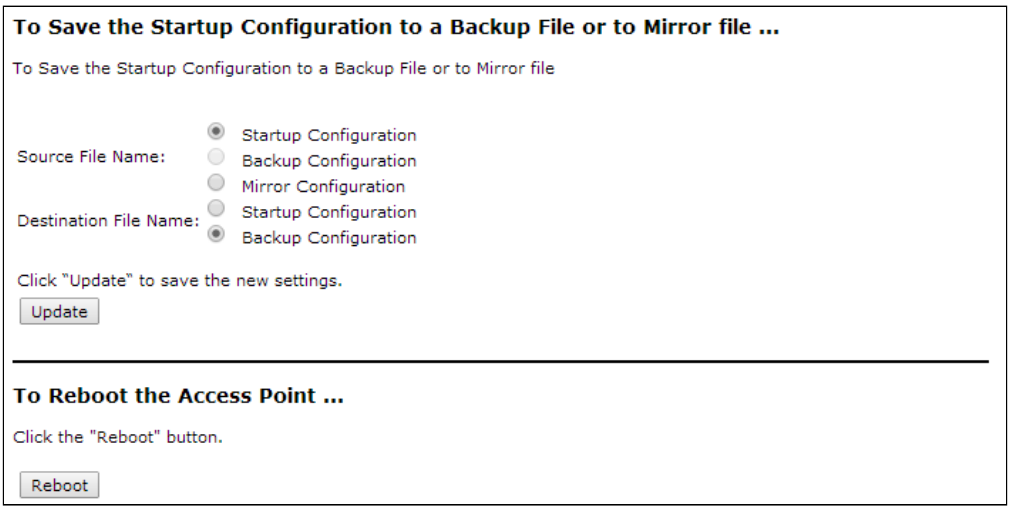
To Save the Current Configuration to a Backup File – downloading the current configuration to a backup file, followed by loading the file to a remote server. Loading the configuration file from the device can be done via HTTP and TFTP protocols.

- **Download via HTTP.** Set the 'Download Method' flag to 'HTTP'. Click the 'Download' button, in the dialog box, select the path to save the file to the PC.
- **Download via TFTP.** Set the 'Download Method' flag to 'TFTP'. In the 'Configuration File' field, specify the file name where the device configuration will be saved. The file name must contain the .xml extension. In the 'Server IP' field, enter the IP address of the TFTP server where the backup file will be saved. Click the 'Download' button to start downloading the file.

To Restore the Configuration from a Previously Saved File – upload previously saved configuration file to the access point. Uploading the configuration to the device can be done via HTTP and TFTP protocols.

When loading a configuration backup file, the device will apply all the settings from the file, including Management VLAN and IP. If the configuration file of another device is loaded, then due to the use of an unauthorized IP address or Management VLAN, communication with the device may be lost.

- **Upload via HTTP.** Set the 'Upload Method' flag to 'HTTP'. Click 'Choose file', and in the dialog box, select the path to the saved backup file on the PC. Click the 'Restore' button to start downloading the configuration file to the device.
- **Upload via TFTP.** Set the 'Upload Method' flag to 'TFTP'. In the 'Filename' field, enter the name of the file that will be downloaded to the device. The file name must contain the .xml extension. In the 'Server IP' field, enter the IP address of the TFTP server where the backup file is saved. Click the 'Restore' button to start downloading the file.



To Save the Startup Configuration to a Backup File or to Mirror file – upload the current configuration to a backup file in the non-volatile memory of the device and load the saved configuration from the non-volatile memory of the device.

- *Source File Name* – configuration source file name (Startup or Backup).
- *Destination File Name* – name of the file where the selected configuration will be written.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

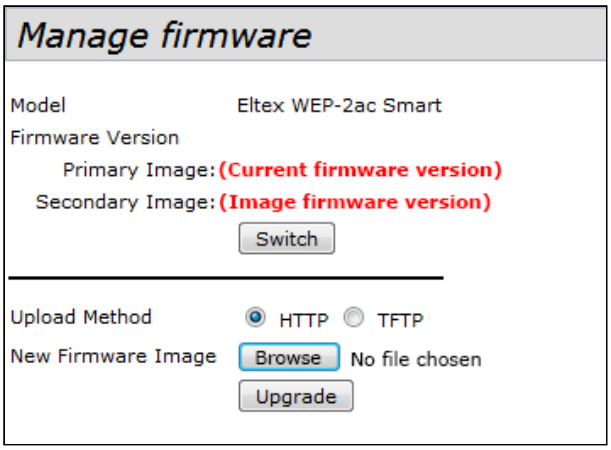
Rebooting the Access Point – software reboot of the device.

To reboot the device, click 'Reboot'.

4.8.2 'Upgrade' submenu

In the **'Upgrade'**, the device firmware is upgraded and changed.

The physical memory of the device contains two firmware images at the same time. If one of the device images fails, then the boot will be performed from another firmware image. Only one image can be active on a device at a time.



- *Model* – device model;
- *Firmware Version* – device firmware version:
  - *Primary Image* – firmware version of the active image (current firmware version);
  - *Secondary Image* – firmware version of the backup image (not in use at the moment).
- *Switch* – load the device firmware from a backup image. When this operation is performed, the active image will go into the standby state, and the standby image will go into the active state. The device will automatically reboot and set the backup firmware as active.

Updating the device firmware. When updating the device firmware, the firmware file is downloaded to the device and becomes active (Primary Image). In this case, the current image is moved to the 'Secondary Image' position. The device automatically reboots and the access point boots with firmware that matches the downloaded image. Downloading the firmware file to the device can be done via HTTP or TFTP protocol. The firmware file can be uploaded to the device using either the HTTP or TFTP protocols.

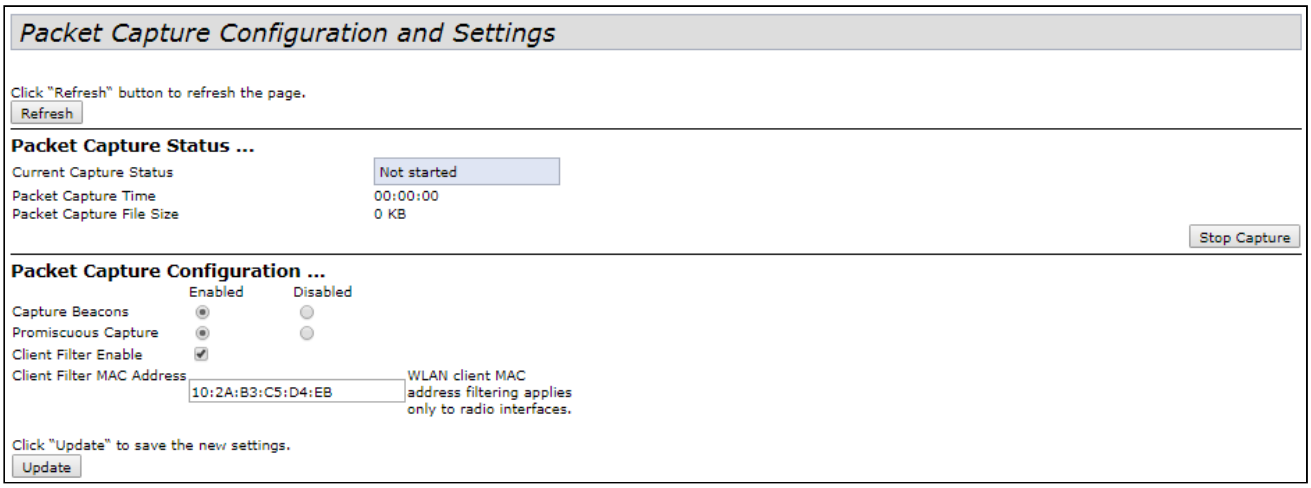
Upload via HTTP. Set the 'Upload Method' flag to 'HTTP'. Click the 'Browse' button. In the dialog box, select the path to the firmware file on the PC. Click the 'Upgrade' button to start uploading the selected firmware file to the device.

Upload via TFTP. Set the 'Upload Method' flag to 'TFTP'. In the 'Image Filename' field, specify the name of the firmware file that will be uploaded to the device. The file name must contain the .tar extension. In the 'Server IP' field, enter the IP address of the TFTP server where the firmware file is saved. Click the 'Upgrade' button to start uploading the file.

While updating the device firmware, do not turn off the power of the device, and do not update or change the current web page with the update progress bar.

4.8.3 'Packet Capture' submenu

The **'Packet Capture'** provides the ability to generate and upload a traffic dump from one of the device's interfaces to a .pcap file. After selecting the parameters for recording a traffic dump, starting recording, stopping recording and uploading a file, the dump can be analyzed with special programs, for example, Wireshark.



To update information on the page, click 'Refresh'.

Packet Capture Status – in this section, information about the status of the traffic dump recording and the capability to stop the process can be viewed.

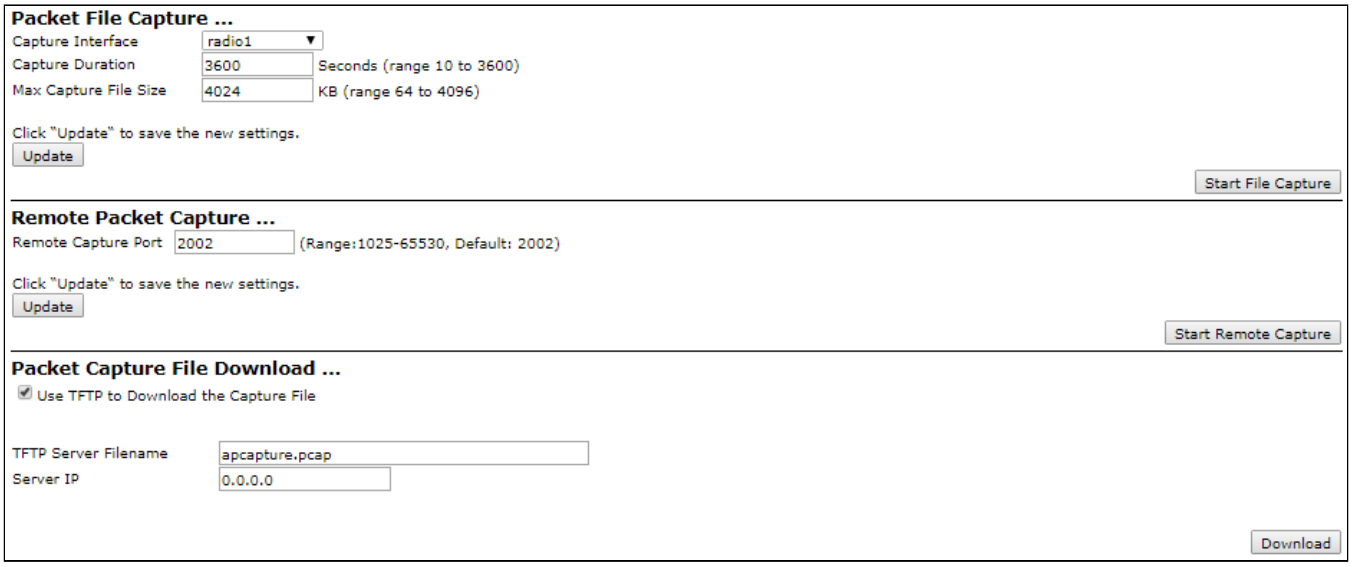
- *Current Capture Status* – current status of traffic dump recording (recording started/stopped);
- *Packet Capture Time* – traffic dump recording time;
- *Packet Capture File Size* – size of the recorded traffic dump.

To stop recording a traffic dump, click 'Stop Capture'.

Packet Capture Configuration – in the section, parameters for recording a traffic dump can be configured:

- *Capture Beacons* – if the flag is set to 'Enabled' – write Beacon packets to the dump, if the flag is set to 'Disabled' – do not write;
- *Promiscuous Capture* – if the flag is set to 'Enabled' – write to the dump all packets received by the radio interface, including packets not intended for this access point;
- *Client Filter Enable* – if the flag is set, only those packets that come from a specific user will be written to the dump. When enabling this feature, the following field must be filled in:
    - *Client Filter MAC Address* – MAC address of the client whose traffic should be filtered into the dump.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.



Packet File Capture – in the section, parameters for recording a traffic dump can be configured:

- *Capture Interface* – name of the interface of the device from which the traffic dump will be recorded (eth0 – GE1, wlan0vap1 – virtual network 1 on wireless interface 0);
- *Capture Duration* – duration of the dump recording. The parameter takes values from 10 to 3600 seconds. The default is 60 seconds;
- *Max Capture File Size* – maximum dump size. The parameter takes values from 64 to 4096 KB. The default is 1024 KB.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

To start writing a traffic dump to a file with the specified parameters, click 'Start File Capture'.

Remote Packet Capture – in the section, a remote recording of a traffic dump is performed:

The device supports the RPCAP protocol, which allows recording a traffic dump from the device interface on a remote machine online.

- *Remote Capture Port* – port number that is used to connect to a remote machine. The parameter takes values from 1025 to 65530. The default is 2002.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

To start the RPCAP server on the device, click 'Start Remote Capture'.

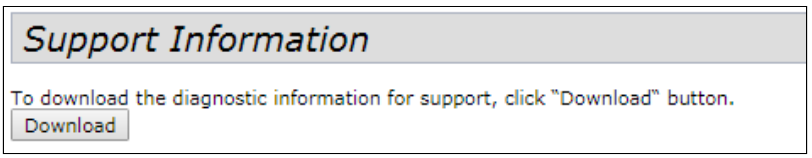
After starting the RPCAP server on the device, connect to the access point on the remote machine. To connect remotely, use the RPCAP protocol, specify the device IP address and the port set in *Remote Capture Port*. For example, this can be done using the Wireshark program. Then, get a list of interfaces for sniffing from the device, select one of them and start dumping from the remote interface.

Packet Capture File Download – in the section, a recorded file with a traffic dump is downloaded. The dump can be downloaded via HTTP or TFTP protocol:

- *Download via HTTP*. The '*Use TFTP to Download the Capture File*' must be unchecked. Click the 'Download' button and in the dialog box select the path to save the dump to PC;
- *Download via TFTP. The ' Use TFTP to Download the Capture File*' flag must be set. In the 'TFTP Server Filename' specify the name of the file in which the traffic dump will be saved on the TFTP server. The file name must contain the .pcap extension. In the 'Server IP' field, enter the IP address of the TFTP server to which the traffic dump will be sent. Click the 'Download' button to start uploading the dump.

4.8.4 'Support Information' submenu

In the **'Support Information'** submenu, the current information about the device (amount of memory, running processes, configuration) is downloaded as a text file. This information can be used to analyze the status of the device, diagnose problems, and identify problems.



Download – downloading a text file in RTF format from the device to PC via HTTP. After clicking this button, a dialog box will appear where the path on the local computer needs to be specified to save the file.

4.9 'Cluster' menu

The **'Cluster'** menu describes the operation and configuration of devices in cluster mode. The cluster mode allows configuring only one access point (master) on the network, the remaining points, when connected to the network, will find the master on the network and copy the configuration from it. Subsequently, when changes are made to the configuration of one of the access points, these changes are applied to all points in the cluster.

Cluster mode is enabled on the device by default.

Only access points from the same group can be combined into a cluster:

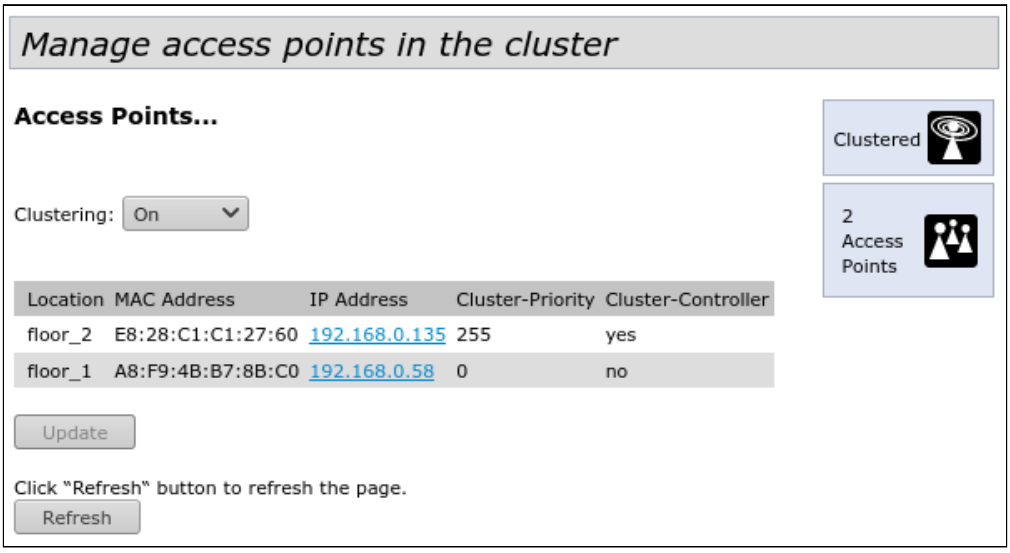
1 group	WEP-12ac	WOP-12ac			
2 group	WEP-2ac	WEP-2ac Smart	WOP-2ac	WOP-2ac SFP	WOP-2ac GPON

The device can work in a cluster only if WDS (Wireless Distribution System) and WGB (Work Group Bridge) are disabled.

To work in a Management cluster, the Ethernet interface of all points must be within the same network.

4.9.1 'Access Points' submenu

In the **'Access Points'** submenu, cluster mode can be enabled/disabled, state of the mode and composition of access points in the cluster can be monitored, and basic parameters of the cluster can be configured.



In the first block of settings, the status of the cluster is viewed and the device is started/stopped in this mode.

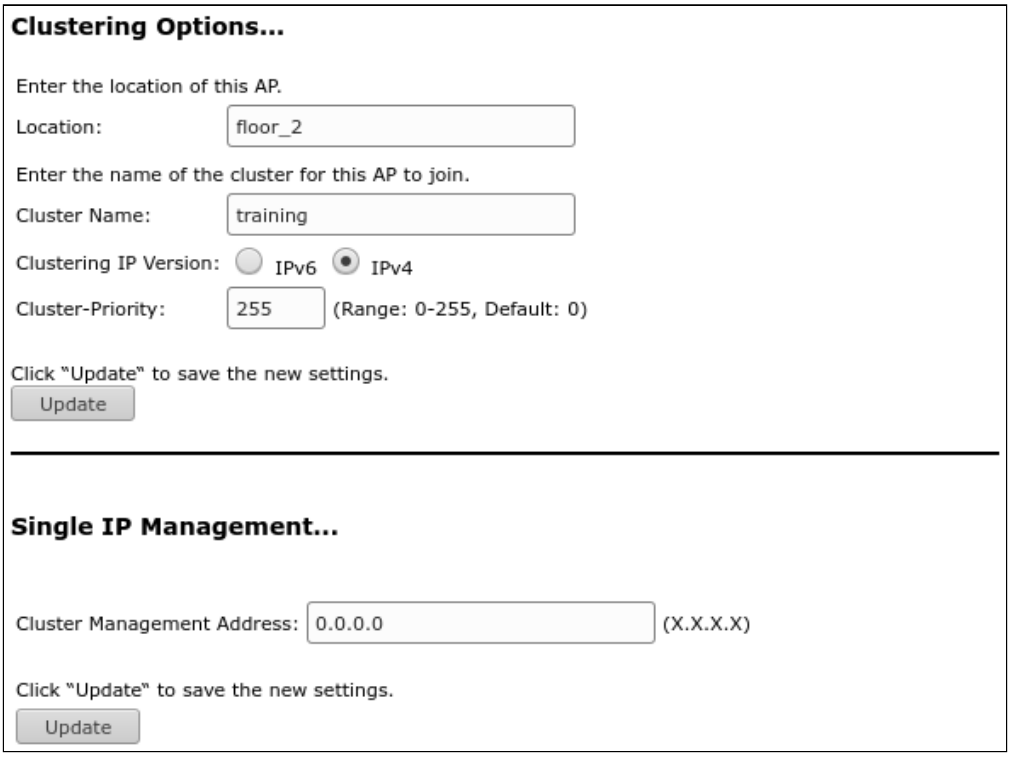
- *Clustering* – cluster operating mode:
  - *Off* – cluster is disabled;
  - *On* – cluster is enabled;
  - *SoftWLC* – cluster is disabled, mode for operation with SoftWLC.

The table lists the access points that are in the same cluster. Based on the information presented in the table, it can be determined:

- *Location* – description of the physical location of the access point. It is filled in on each access point by the administrator in the 'Clustering Options' section;
- *MAC Address* – MAC address of the access point in the cluster;
- *IP Address* – IP address of the access point in the cluster;
- *Cluster-Priority* – priority of the access point in the cluster. The access point with the maximum value of this parameter becomes the Master point. The parameter is set on each access point by the administrator in the 'Clustering Options' section. If the parameter is not set, the access point with the lowest MAC address becomes the master point in the cluster;
- *Cluster-Controller* – parameter indicating which access point is the Master point in this cluster. The parameter can take the following values: yes – the point is a Master point; no – the point is not a Master point.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

To update information on the page, click 'Refresh'.



Clustering Options – in the section, the basic parameters of the cluster are configured.

The section parameters are available for editing if the cluster on the point is disabled, i.e. the 'Clustering' parameter is set to *Off*.

- *Location* – description of the physical location of the access point. Used to display in monitoring tables for easy analysis and network management;
- *Cluster Name* – cluster name. The access point will connect only to the cluster which name is specified in this parameter. By default – default;
- *Clustering IP Version* – version of the IP protocol used to exchange control information between cluster devices;
- *Cluster-Priority* – access point priority in the cluster. The parameter takes values from 0 to 255. The default is 0. Supported only for IPv4 networks. The master in the cluster is the point that has the highest cluster priority. If the parameter is not set, the access point with the lowest MAC address becomes the master point in the cluster.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

Single IP Management – in this section, the additional address of the master in the cluster is set.

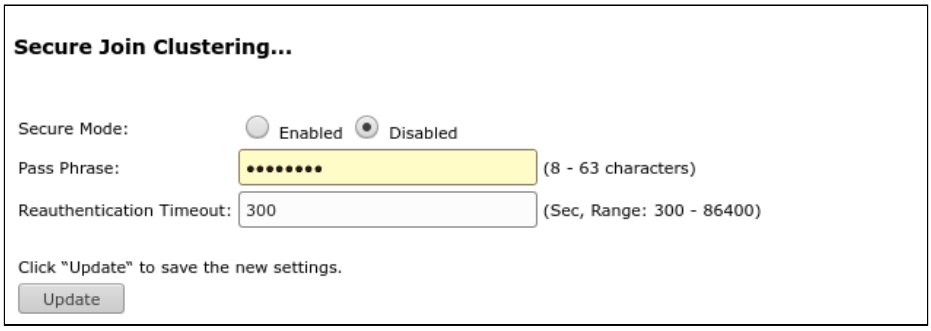
During operation, the master point of the cluster may change due to various situations, for example, the master point has failed or a new access point with a higher priority or a lower MAC address has been added to the network. In order to be able to connect to the Master point, regardless of which point is currently the master, assign a 'Cluster Management Address'.

If a connection is established by the 'Cluster Management Address', the user is guaranteed to connect to the device that is the master in the cluster. In case of a master change in the cluster, the 'Cluster Management Address' also moves to the new access point.

- *Cluster Management Address* – unique IPv4 address, at which the cluster master point will be available. This address must be on the cluster subnet and not be the same as the IP address of other devices on the network.

When this parameter is set on one access point of the cluster, all other points in the cluster will automatically learn about this setting.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.



Secure Join Clustering – in this section, security of the cluster connection is configured.

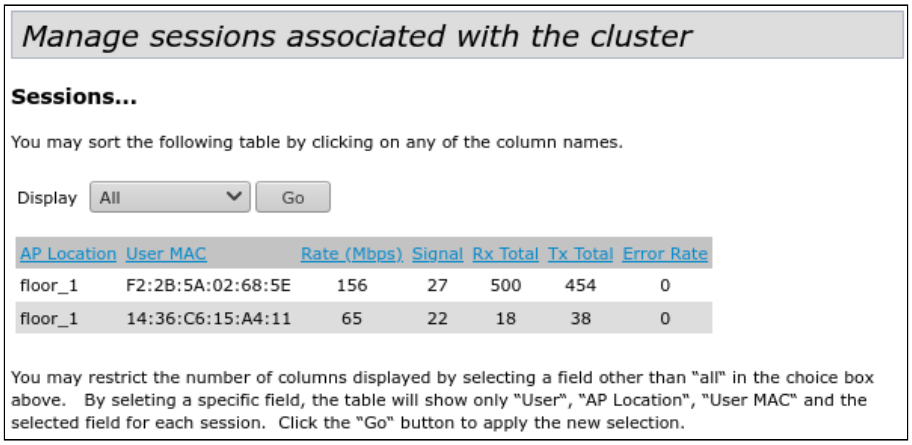
The section parameters are available for editing if the cluster on the point is disabled, i.e. the 'Clustering' parameter is set to *Off*.
The settings are only supported for IPv4 networks.

- *Secure Mode* – enable/disable cluster security. If Enabled, then only those access points that have the same password specified in the 'Pass Phrase' field can join the cluster;
- *Pass Phrase* – cluster security password. The password must contain between 8 and 63 characters. Valid characters: uppercase and lowercase letters, numbers, and special characters such as @ and #;;
- *Reauthentication Timeout* – period of time after which re-authentication will occur. The parameter takes values from 300 to 86400 seconds. The default is 300 seconds.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

4.9.2 'Sessions' submenu

In the **'Sessions'** submenu, the parameters of client sessions connected to access points located in the cluster can be viewed. Each client is identified by the MAC address and access point to which it is currently connected.
A maximum of 20 clients can be listed in the table. All clients connected to this access point can be viewed in the 'Status' → 'Client Associations'.



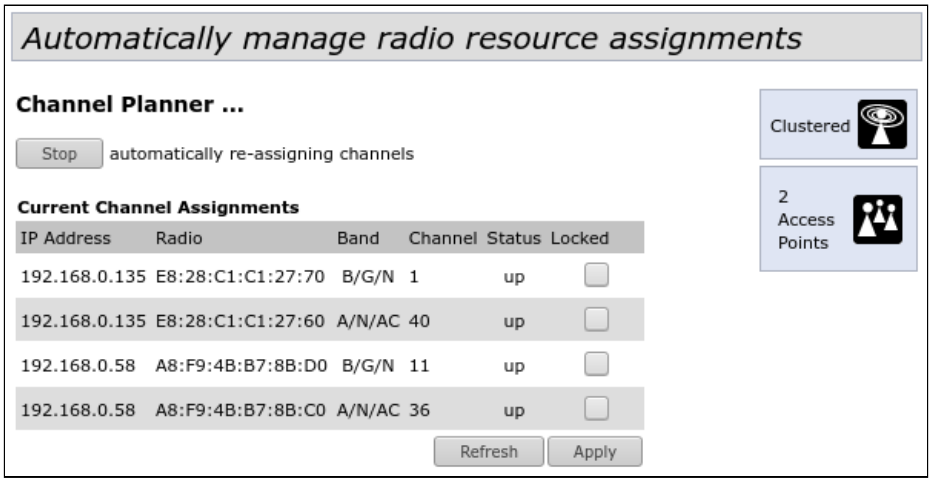
To limit the number of columns displayed in the monitoring table, select an option other than 'All' in the 'Display' field and click the 'Go' button.
When selecting a specific option, the table for each client will display columns: ' AP Location', 'User MAC', and a column with the selected option.

- *AP Location* – description of the physical location of the access point;
- *User MAC* – MAC address of the client's wireless device;
- *Rate* – data transfer rate between the access point and a specific client, Mbps;
- *Signal* – signal level received from the access point;
- *Rx Total* – total number of packets received by the client during this session;
- *Tx Total* – total number of packets transmitted from the client during this session;
- *Error Rate* – percentage of resent packets.

4.9.3 'Radio Resource Management' submenu

In the **'Radio Resource Management'** submenu, automatic selection of access point channels can be managed.

In cluster mode, each access point sets the channel numbers on which nearby access points operate in the same cluster, and also performs a spectral analysis of background noise by third-party access points. At set intervals, access points recalculate the overall spectral structure of the medium and select a channel so that it is the least noisy, and access points which coverage areas overlap are on different channels.



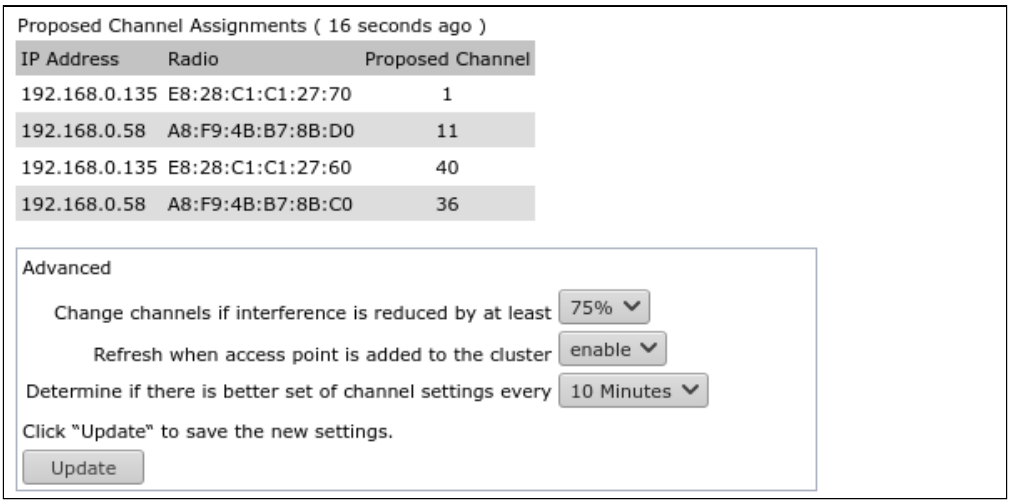
To start the process of spectral analysis of the environment and selection of the optimal channel for each access point in the cluster, click the 'Start' button. To stop the process, click the 'Stop' button.

The **'Current Channel Assignments'** contains the current list of access points in the cluster and their parameters:

- *IP Address* – IP address of the access point in the cluster;
- *Radio* – MAC address of the radio interface of the access point in the cluster;
- *Band* – set of standards currently supported by the radio interface of the access point in the cluster;
- *Channel* – frequency channel in the cluster;
- *Status* – operation status of the radio interface of the access point in the cluster;
- *Locked* – blocking the channel change. If the flag is set, when the optimal channel is selected by all access points, this air interface will use the previous channel for any outcome of the optimal channel selection.

Click 'Apply' to apply the changes.

Click 'Refresh' to refresh data in the 'Current Channel Assignments'.



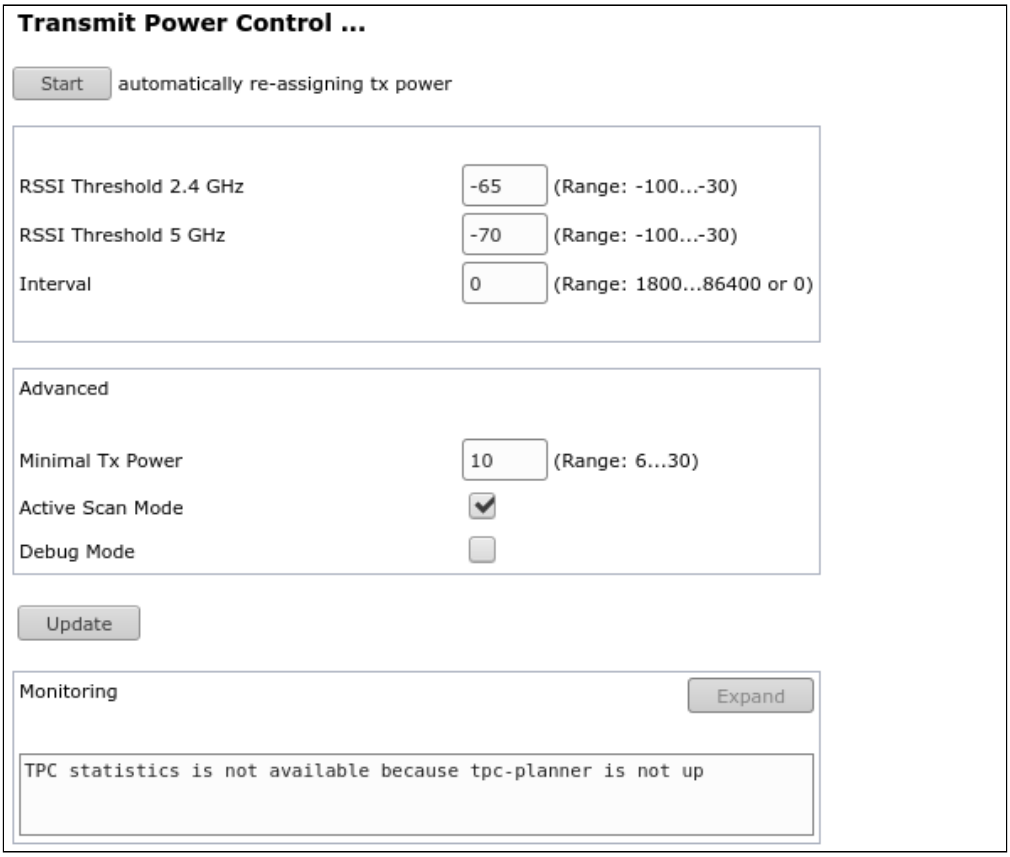
The **'Proposed Channel Assignments'** table provides the information about the possible values of the channel to which the radio interface of the access point will switch in case of starting the recalculation of the optimality of the channel selection:

- *IP Address* – IP address of the access point in the cluster;
- *Radio* – MAC address of the radio interface of the access point in the cluster;
- *Proposed Channel* – channel number to which the radio interface of the access point will switch in case of recalculation of the channel selection optimality.

Advanced – in this section, advanced settings are performed:

- *Change channels if interference is reduced by at least* – percentage gain in reducing the noise level for making a decision to switch to another channel. If, during the analysis of the environment, the access point detects that switching to another channel will result in a noise level decrease greater than the specified amount in this parameter, the decision will be made to switch to another channel. The value setting range for this parameter is between 5% and 75%;
- *Refresh when access point is added to the cluster* – recalculate the overall spectral structure of the environment and select the optimal channel for access points if a new access point joins the cluster;
- *Determine if there is better set of channel settings every* – time interval after which the overall spectral structure of the environment is recalculated and the optimal channel for access points is selected.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.



In the **'Transmit Power Control'** section, access points that are in the same cluster, at set intervals, perform a spectral analysis of the air and recalculate the powers set on access points in the cluster in such a way as to have as little influence as possible on each other. By default, optimization is performed when there is a change in the cluster composition.

To start the auto-tuning process for each access point in the cluster, click the 'Start' button. To stop the process, click the 'Stop' button.

- *RSSI Threshold 2.4 GHz* – RSSI level threshold in the 2.4 GHz band. The parameter takes values from -100 to -30. Default is -65;
- *RSSI Threshold 5 GHz* – RSSI level threshold in the 5 GHz band. The parameter takes values from -100 to -30. Default is -70;
- *Interval* – time interval between optimization cycles. The parameter takes values from 1800 to 86400 seconds. The default value is 0, which means that power optimization is performed once, then only when there is a change in the cluster composition.

Advanced – in this section, advanced settings are performed:

- *Minimal Tx Power* – minimum output power level of the access point. The parameter takes values from 6 to 30. The default is 10;
- *Active Scan Mode* – when the flag is set, the active scanning mode is used, when it is disabled, it is passive;
- *Debug Mode* – when the flag is set, sending debug messages to the access point console is enabled.

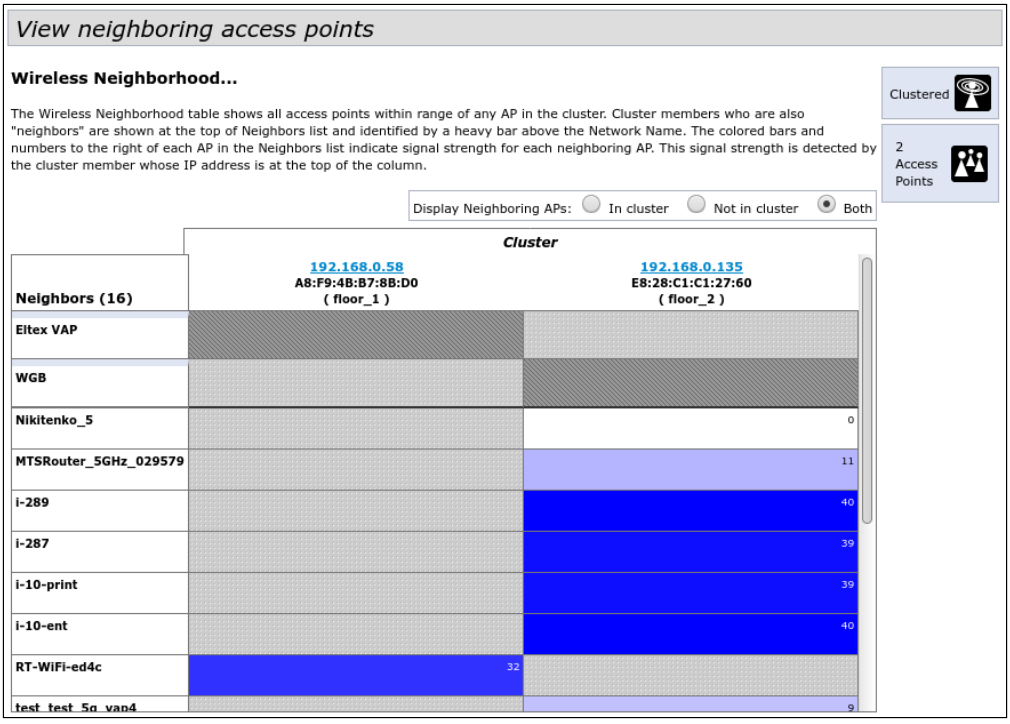
To apply a new configuration and save setting to non-volatile memory, click 'Update'.

After auto-tuning optimization is completed, the results of scanning all access points in the cluster, the level of influence of points on each other, as well as the changed output power of access points can be observed in the 'Monitoring' window.

4.9.4 'Wireless Neighborhood' submenu

The **'Wireless Neighborhood'** submenu contains a table of correspondence between access points located in the cluster and wireless networks detected by these devices. This table shows which wireless networks each access point detects and what signal strength it receives from them.

Based on this table, a spectral analysis of the entire network can be performed, and the impact of interference on each access point can be evaluated. This will enable the assessment of the correct location of access points across the coverage area and identification of problem areas where the level of interference may affect the quality of services.



The top line of the table displays information on each radio interface of access points located in the cluster. The far left column 'Neighbors' contains information on wireless networks that are visible to devices in the cluster.

The signal level from each wireless network is indicated in the upper right corner of the table cell.

The table is formed in such a way that its first rows display wireless networks formed by the cluster itself, followed by the names of third-party networks.

The 'Display Neighboring APs' parameter configures the display of information in the table:

- *In cluster* – when the flag is set, the table will display information only about those wireless networks that are configured on access points located in the cluster;
- *Not in cluster* – when the flag is set, the table will display information only about those wireless networks that are configured on access points that are not in the cluster;
- *Both* – when the flag is set, the table will display information about all networks.

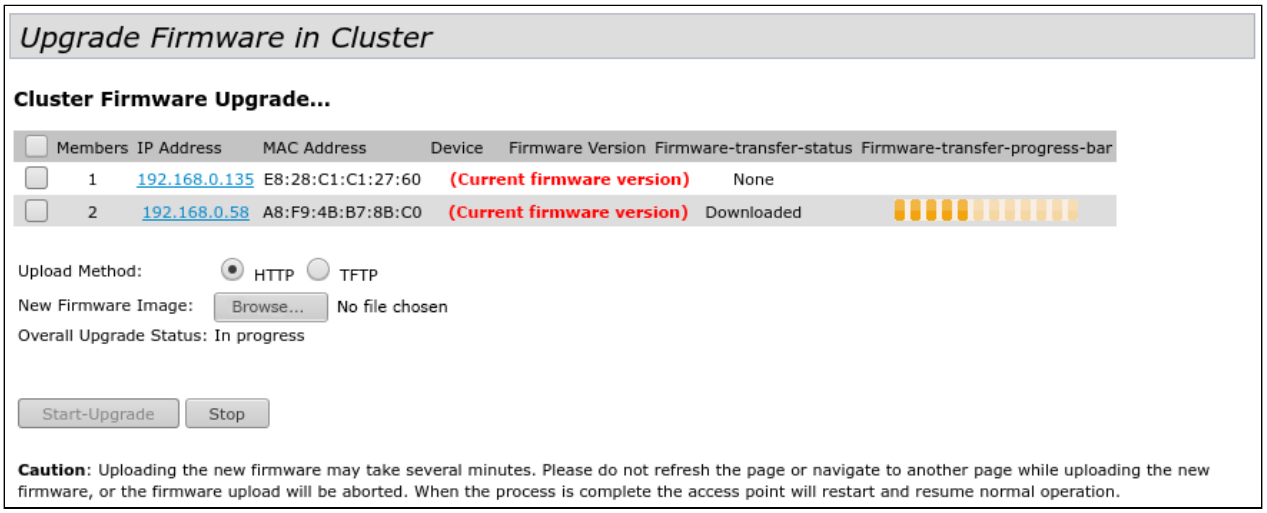
4.9.5 'Cluster Firmware Upgrade' submenu

In the **'Cluster Firmware Upgrade'** submenu, a firmware update can be performed on all devices included in the cluster.

The parameters of this submenu are available for viewing and editing only on the Master point of the cluster.

While updating the device firmware, do not turn off the power of the device, and do not update or change the current web page with the update progress bar.

When updating the firmware of the cluster devices, the firmware file will be downloaded to each device and set to the 'Primary Image' position. The update process automatically reboots devices with firmware that matches the new image. The firmware installed earlier on the cluster devices will be saved and moved to the 'Secondary Image' position (backup version of the firmware).



- *Members* – serial number of the access point in the cluster;
- *IP Address* – IP address of the access point in the cluster;
- *MAC Address* – MAC address of the access point located in the cluster;
- *Device* – access point type;
- *Firmware Version* – current version of the access point firmware;
- *Firmware-transfer-status* – status of the firmware update process on the access point;
- *Firmware-transfer-progress-bar* – status of the firmware upload process to the access point;

Updating the device firmware. The firmware file can be uploaded to the device using either the HTTP or TFTP protocols.

Upload via HTTP. Set the 'Upload Method' flag to 'HTTP'. Click the 'Browse' button. In the dialog box, select the path to the firmware file on the PC. Click the 'Start-Upgrade' button to start uploading the selected firmware file to the device.

Upload via TFTP. Set the 'Upload Method' flag to 'TFTP'. In the 'Image Filename' field, specify the name of the firmware file that will be uploaded to the device. he file name must contain the .tar extension. In the 'Server IP' field, enter the IP address of the TFTP server where the firmware file is saved. Click the 'Start-Upgrade' button to start uploading the file.

Click the 'Stop' button to interrupt the device update process.

In the 'Overall Upgrade Status' field, the generalized status of the firmware upgrade process on the access points is displayed.

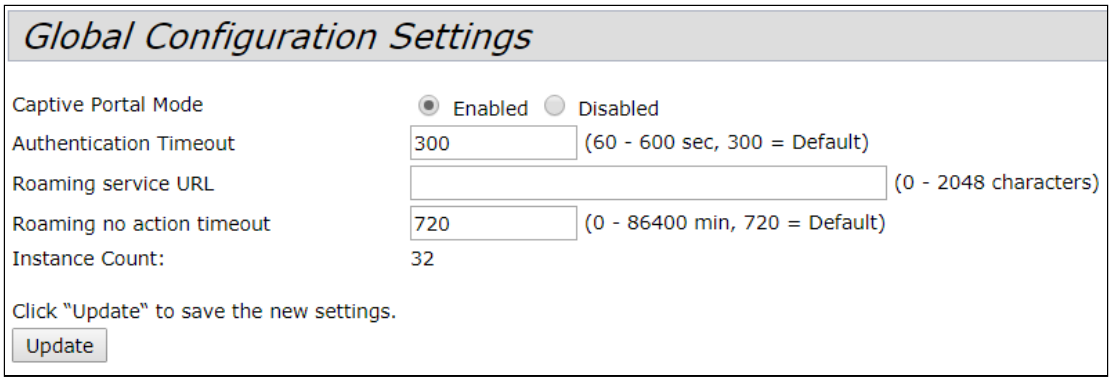
4.10 'Captive Portal' menu

In the **'Captive portal'** menu, the portal to which clients are redirected for authorization when connecting to the Internet can be configured.

Thus, the Wi-Fi network can be switched to open mode by removing encryption, while still restricting access to network resources. Connection to network resources will be implemented through web authorization.

4.10.1 'Global Configuration' submenu

In the **'Global Configuration'**, general parameters of the portal and monitor the current number of created objects can be configured.

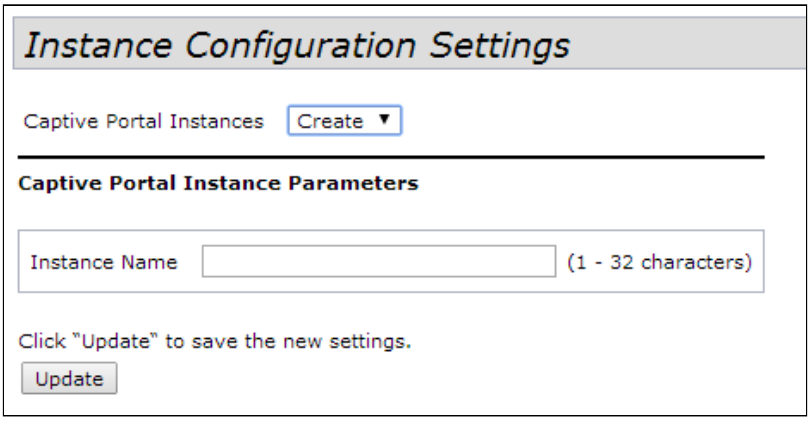


- *Captive Portal Mode* – portal operation status:
  - *Enabled* – when the flag is set, the portal is used;
  - *Disabled* – when the flag is set, the portal is not used.
- *Authentication Timeout* – time period in seconds, during which the client can enter authorization data on the portal page to gain access to the network. If the interval is exceeded, refresh the page or reconnect to the network. The parameter takes values from 60 to 600 seconds. The default is 300 seconds;
- *Roaming Service URL* – APB service address for hotspot roaming support. Specified in the format: 'ws://host:port/path';
- *Roaming No Action Timeout* – time after which the access point will delete outdated/inactive records about clients in roaming. The parameter takes values from 0 to 86400 minutes. The default is 720 minutes;
- *Instance Count* – number of portal instances configured on the access point.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

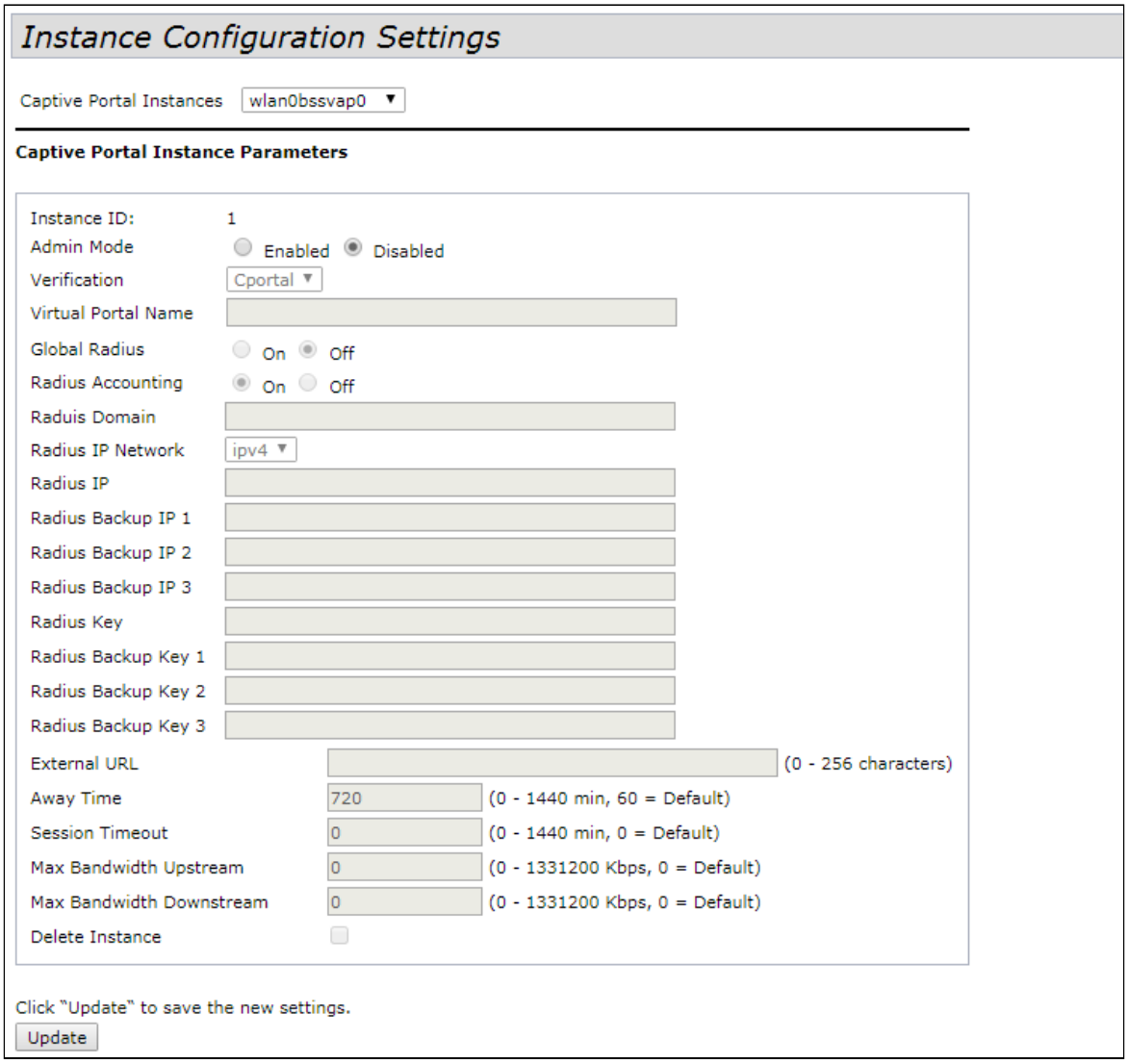
4.10.2 'Instance Configuration' submenu

In the **'Instance Configuration'** submenu, portals are created and configured.



To create new portal in the **'Captive Portal Instances'** field, select **'Create'** and in the **'Instance Name'** field specify the name of the new portal. The portal name can contain from 1 to 32 characters. To create a portal, click the **'Update'** button.

To proceed to work with the portal, select its name in the **'Captive Portal Instances'** field:



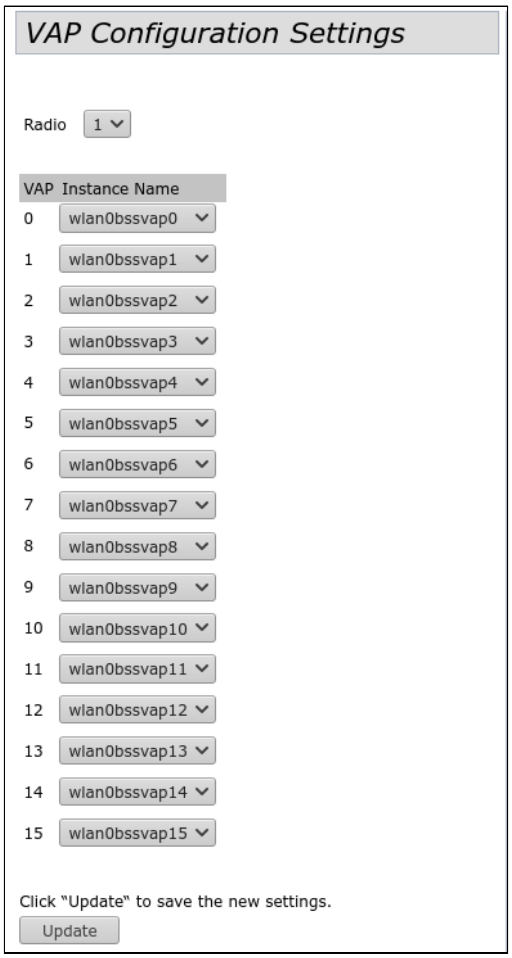
- *Instance ID* – portal number;
- *Admin Mode* – portal operating mode:
  - *Enable* – enabled;
  - *Disabled* – disabled.
- *Verification – user authentication method*:
  - *Cportal* – method in which Captive Portal performs user authentication on the Radius server;
  - *RADIUS* – for authorization, user must be registered on the Radius server;
- *Virtual Portal Name* – virtual portal name;
- *Global Radius* – global authorization settings for the RADIUS protocol:
  - *Off* – disabled;
  - *On* – enabled. Selection of this option allows for the editing of the following fields:
    - *Radius Accounting* – when enabled, 'Accounting' messages will be sent to the RADIUS server:
      - *On* – enabled;
      - *Off* – disabled.
    - *Raduis Domain* – user domain;
    - *Radius IP Network* – select the IPv4 or IPv6 protocol to access the RADIUS server;
    - *Radius IP* – address of the main RADIUS server. If the primary RADIUS server is unavailable, requests will be sent to backup RADIUS servers;
    - *Radius Backup IP 1, 2, 3* – backup RADIUS server address;
    - *Radius Key* – password for authorization on the main RADIUS server;
    - *Radius Backup Key 1, 2, 3* – password for authorization on the backup RADIUS server 1, 2, 3;

- *External URL* – address of the external Captive Portal to which the user will be redirected when connecting to the hotspot network;
- *Away Time* – time during which the user authentication record on the access point is valid after it is dissociated. If the client does not re-authenticate within this time, the entry will be deleted. The parameter takes values from 0 to 1440 minutes. The default is 60 minutes;
- *Session Timeout* – session lifetime timeout. The user is automatically logged out of the portal after a specified period of time. The parameter takes values from 0 to 1440 minutes. Default 0 – no timeout applied;
- *Max Bandwidth Upstream* – maximum traffic transfer rate from the subscriber. The parameter takes values from 0 to 1331200 Kbps. Default 0 – unlimited;
- *Max Bandwidth Downstream* – maximum rate of traffic transfer to the subscriber. The parameter takes values from 0 to 1331200 Kbps. Default 0 – unlimited;
- *Delete Instance* – to delete this portal, set the flag and click the 'Update' button. Default portals cannot be deleted.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

4.10.3 'VAP Configuration' submenu

In the **'VAP Configuration'** submenu, portal can be bound to the virtual Wi-Fi networks of the VAP.



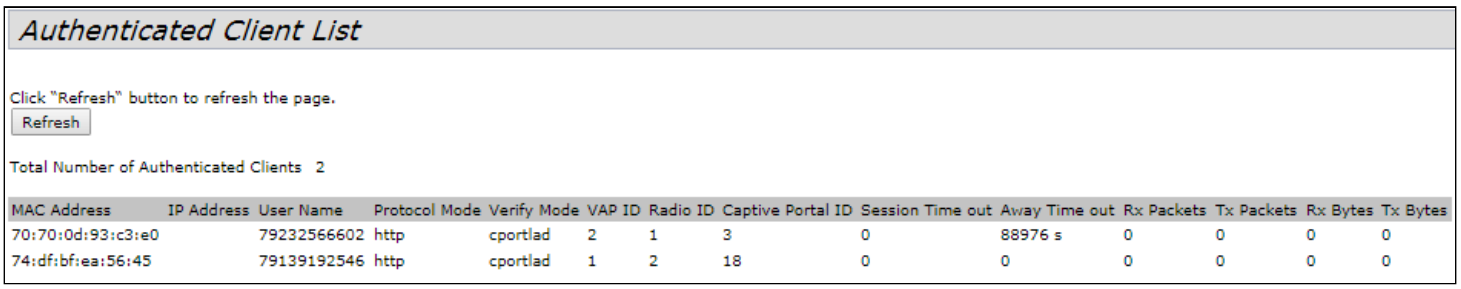
- *Radio* – number the Wi-Fi interface being configured .

The table assigns a portal to each virtual network by its name.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

4.10.4 'Authenticated Clients' submenu

In the **'Authenticated Clients'** submenu, list of clients that have successfully authenticated on the portal is displayed.



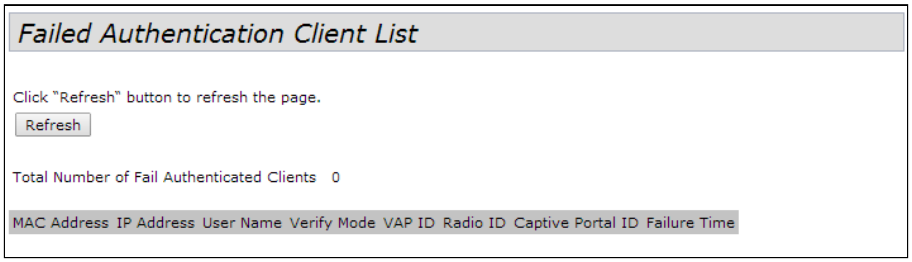
To update information on the page, click 'Refresh'.

- *Total Number of Authenticated Clients* – number of successfully authorized clients at this point in time;
- *MAC Address* – client MAC address;
- *IP Address* – client IP address;

- *User Name* – username with which the client was authenticated on the portal;
- *Protocol Mode* – protocol used for the HTTP/HTTPS connection;
- *Verify Mode* – authorization method on the portal;
- *VAP ID* – virtual network number;
- *Radio ID* – radio interface number;
- *Captive Portal ID* – number of the portal the client is associated with;
- *Session Timeout* – remaining session lifetime;
- *Away Timeout* – remaining lifetime of the client authentication record;
- *Rx Packets* – number of packets received from the client;
- *Tx Packets* – number of packets sent to the client;
- *Rx Bytes* – number of UAP bytes received from the user;
- *Tx Bytes* – number of UAP bytes transmitted by the user.

4.10.5 'Failed Authentication Clients' submenu

The **'Failed Authentication Clients'** contains a list of clients with failed authorization on the portal.



To update information on the page, click 'Refresh'.

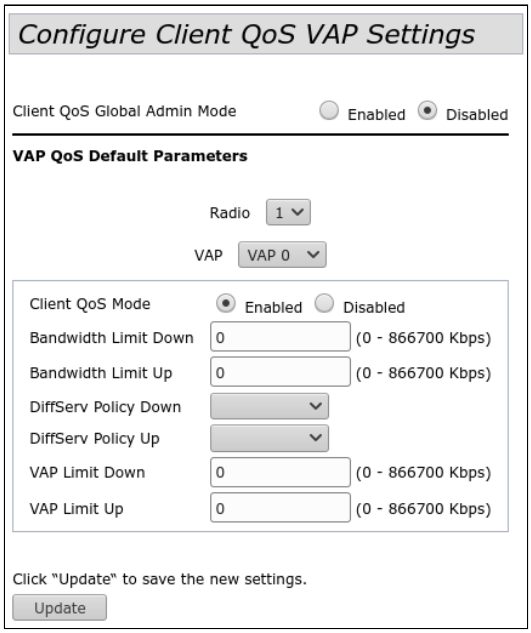
- *MAC Address* – client MAC address;
- *IP Address* – client IP address;
- *User Name* – username with which the client was authenticated on the portal;
- *Verify Mode* – authorization method on the portal;
- *VAP ID* – virtual network number;
- *Radio ID* – radio interface number;
- *Captive Portal ID* – number of the portal the client is associated with;
- *Failure Time* – time the error occurred.

4.11 'Client QoS' menu

The **'Client QoS'** menu is intended for finer tuning of the QoS of client traffic flows. Client QoS allows configuring the prioritization of individual traffic flows, limiting the bandwidth for each client.

4.11.1 'VAP QoS Parameters' submenu

In the **'VAP QoS Parameters'** submenu allows for the global enabling of all Client QoS settings (Class MAP, Policy MAP, Bandwidth Limit) and the assignment of previously generated traffic prioritization rules.

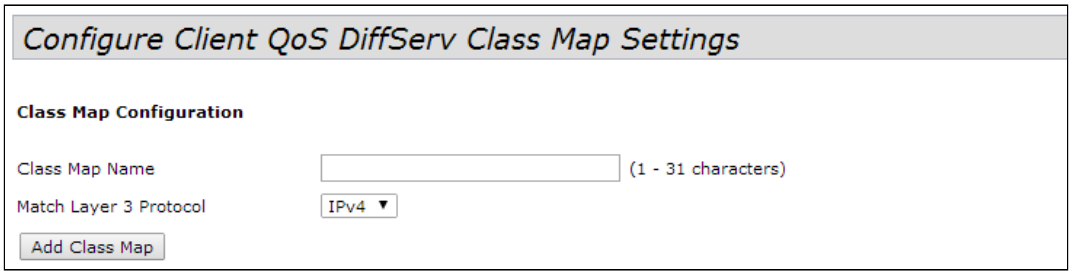


- *Client QoS Global Admin Mode* – use of Client QoS on the entire access point globally:
  - *Enable* – enable;
  - *Disabled* – disable.
- *Radio* – selection of the radio interface on which Client QoS will be configured;
- *VAP* – selection of a virtual access point on which Client QoS will be configured;
- *Client QoS Mode* – use of Client QoS on the selected VAP:
  - *Enable* – enable;
  - *Disabled* – disable.
- *Bandwidth Limit Down* – bandwidth limit from the access point to each client, kbps. The parameter takes values from 0 to 866700 kbps. If 0 is assigned, then the bandwidth limit is not applied. Any non-zero value is rounded up to a multiple of 64 kbps;
- *Bandwidth Limit Up* – bandwidth limit from each client to the access point, kbps. The parameter takes values from 0 to 866700 kbps. If 0 is assigned, then the bandwidth limit is not applied. Any non-zero value is rounded up to a multiple of 64 kbps;
- *DiffServ Policy Down* – name of the Policy profile to be applied to traffic sent in the direction from the access point to the client;
- *DiffServ Policy Up* – name of the Policy profile that should be applied to traffic sent in the direction from the client to the access point;
- *VAP Limit Down* – bandwidth limit from the access point to clients (in total) connected to this VAP, kbps. The parameter takes values from 0 to 866700 kbps. If 0 is assigned, then the restriction is not applied. Any non-zero value is rounded up to a multiple of 64 kbps;
- *VAP Limit Up* – bandwidth limit from the clients (in total) to the access point, kbps. The parameter takes values from 0 to 866700 kbps. If 0 is assigned, then the restriction is not applied. Any non-zero value is rounded up to a multiple of 64 kbps.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

4.11.2 'Class Map' submenu

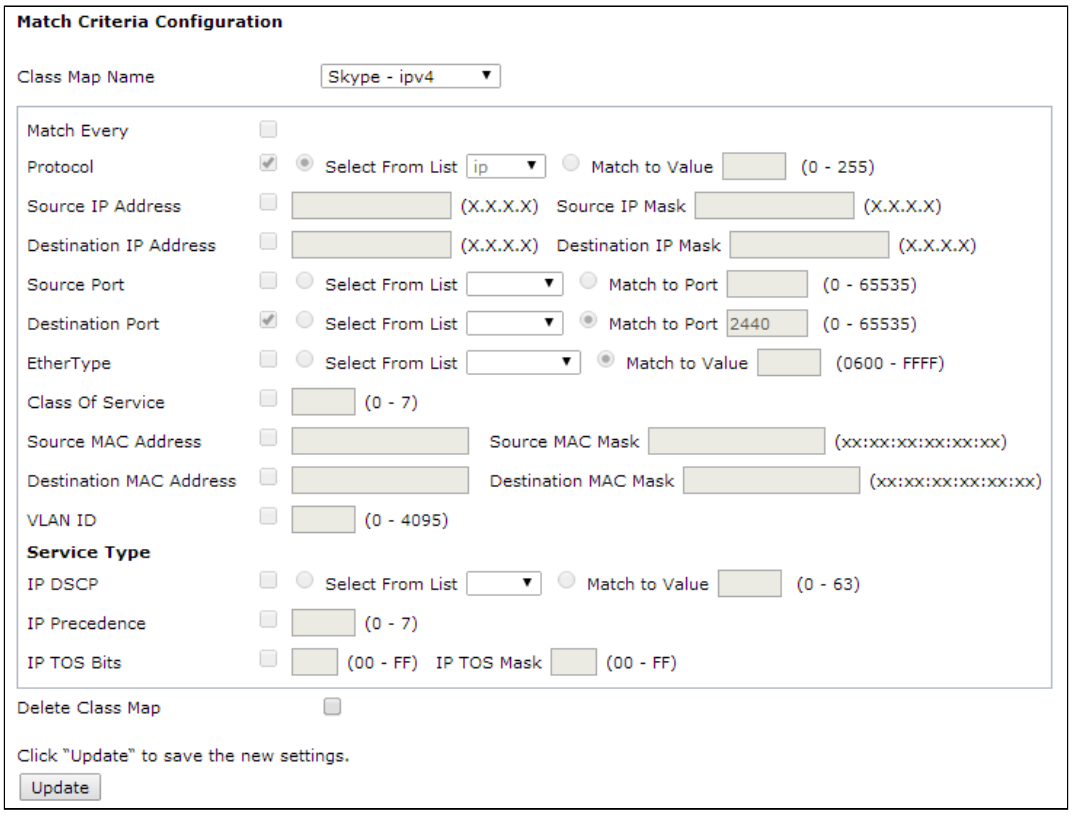
In the **'Class Map'** submenu, traffic classification is configured. Based on the unique features of the packets of a certain traffic flow, the class of belonging of the packets to this flow is formed. In the future, this class will be used for prioritization operations of various flows, united by a common feature.



Class Map Configuration – in the section, a traffic classification profile is created.

- *Class Map Name* – profile name;
- *Match Layer 3 Protocol* – protocol by which the classification will take place (IPv4 or IPv6). Depending on the choice of protocol, a different set of fields will be offered, according to which traffic will be classified.

To create a new traffic class, specify the class name in the 'Class Map Name' field and click the 'Add Class Map' button.



Match Criteria Configuration – in this section, criteria for the traffic class are configured.

- *Class Map Name* – selection of the traffic class for which the attributes of belonging to the class will be configured;
- *Match Every* – if flag is set, the traffic will be assigned to this class, regardless of the contents of the fields in its header. If the flag is not set, then it is required to specify the values of the required traffic fields that must be associated with this class;
- *Protocol* – Protocol field value inIPv4 packet;
- *Source IP Address* – IP address value of the packet sender;
- *Source IP Mask* – mask indicating the significance of the bits in the IP address, based on which the packet is classified;
- *Source IPv6 Prefix Len* – length of the sender IPv6 address prefix;
- *Destination IP Address* – IP address value of the packet recipient;

- *Destination IP Mask* – mask indicating the significance of the bits in the IP address, based on which the packet is classified;
- *Destination IPv6 Prefix Len* – length of the recipient IPv6 address prefix;
- *Source Port* – sender port (Layer 4);
- *Destination Port* – recipient port (Layer 4);
- *EtherType* – EtherType field value, indicating the type of protocol used in the packet;
- *Class Of Service* – CoS field value, indicating the priority of the packet on Layer 2 of the packet;
- *Source MAC Address* – MAC address value of the packet sender;
- *Destination MAC Address* – MAC address value of the packet recipient;
- *VLAN ID* – VLAN field value in the packet;
- *IP DSCP* – DSCP field value in the IP packet header;
- *IP Precedence* – Precedence field value in the IP packet header;
- *IP TOS Bits* – TOS field value in the IP packet header;
- *IP TOS Mask* – mask indicating the significance of the bits in the TOS field, based on which the packet is classified;
- *IPv6 Flow Label* – Flow Label field value.

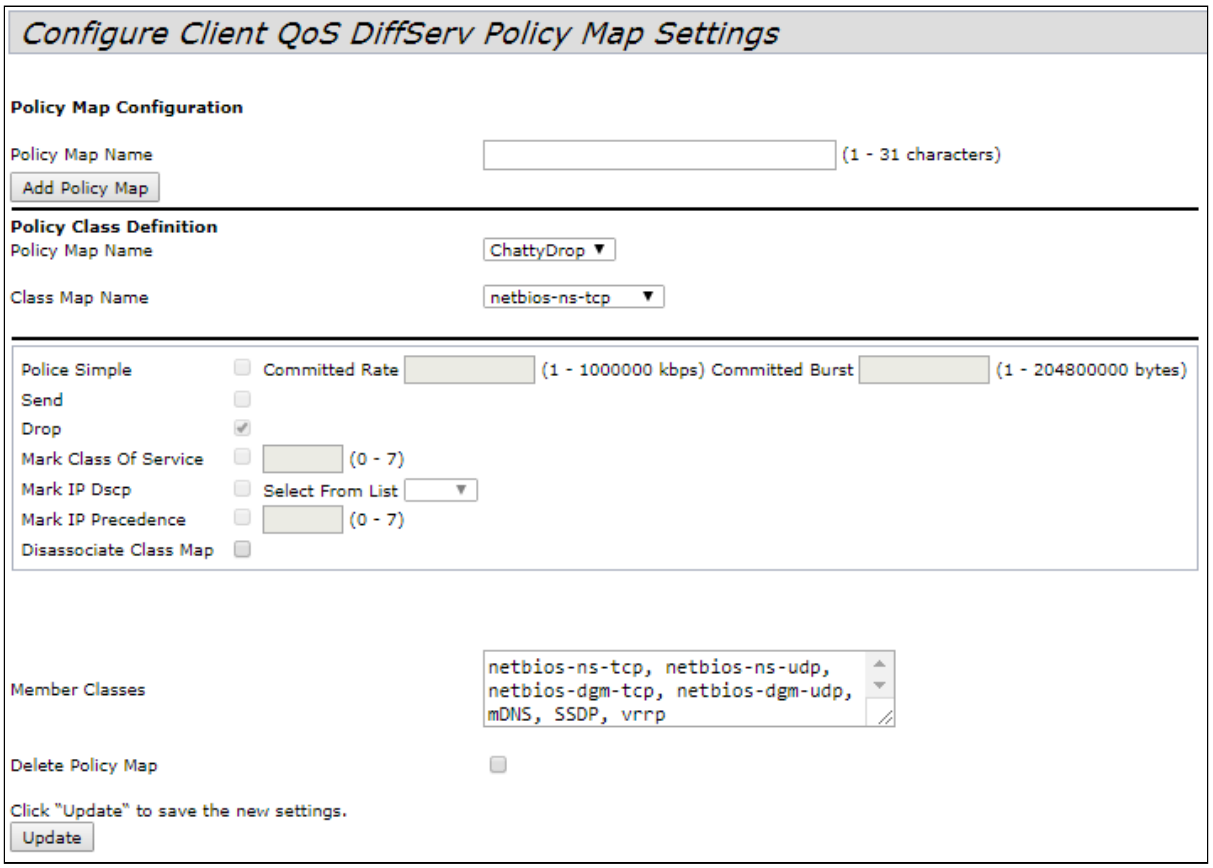
To delete a class, check the box next to 'Delete Class Map' and click the 'Update' button.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

4.11.3 'Policy Map' submenu

The **'Policy Map'** submenu is intended for configuring bandwidth for a traffic stream classified according to a common feature, marking the priority of this traffic class at the Layer 2 and Layer 3 levels (CoS, DSCP, Precedence), as well as for making a decision about passing this traffic or about its blocking.

In this submenu, 'Policy Map' profile is formed, for which the previously created 'Class Map' traffic classifiers are sequentially assigned. For each classifier, the operations to be performed with the given type of traffic are indicated.



Policy Map Configuration – in this section, a new Policy Map profile is being created.

- *Policy Map Name* – Policy Map name profile.

To add a new profile, enter profile name in the 'Police Map Name' field and click the 'Add Policy Map' button.

Policy Class Definition – in this section, traffic classifiers are configured.

- *Policy Map Name* – 'Policy Map' profile name, in which further configuration of operations for traffic classifiers will be performed;
- *Class Map Name* – traffic classifier previously created in the 'Class Map' submenu.

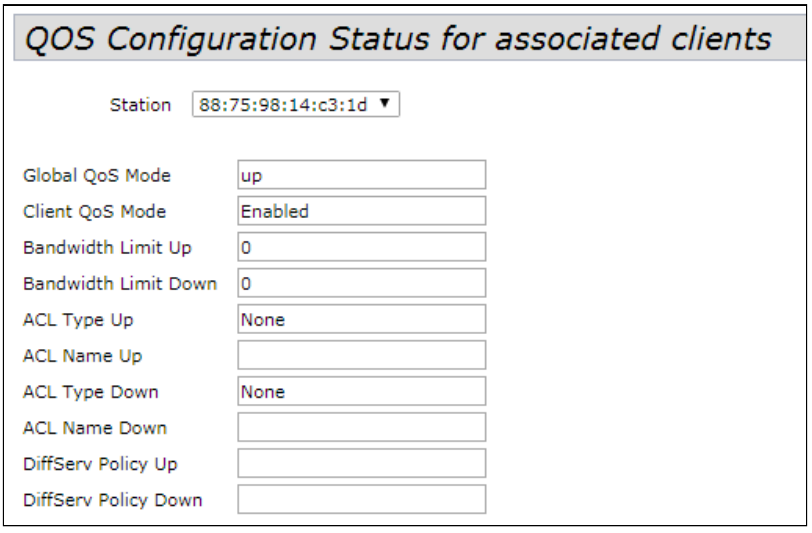
Operations to be performed with this type of traffic:

Police Simple – simplified configuration in which two parameters are set:
  - *Committed Rate* – guaranteed transmission rate for this type of traffic;
  - *Committed Burst* – traffic bursts limitation.
- *Send* – when the flag is set, all packets of the corresponding traffic flow will be sent if the Class Map criteria are met;
- *Drop* – when the flag is set, all packets of the corresponding traffic flow will be dropped if the Class Map criteria are met;
- *Mark Class Of Service* – when the flag is set, all packets of the corresponding traffic flow will be marked with the specified CoS value. The parameter takes a value from 0 to 7;
- *Mark IP Dscp* – when the flag is set, all packets of the corresponding traffic flow will be marked with the specified IP-DSCP value. The value can be selected from the list or specified;
- *Mark IP Precedence* – when the flag is set, all packets of the corresponding traffic flow will be marked with the specified IP Precedence value. The parameter takes a value from 0 to 7;
- *Disassociate Class Map* – set the flag and click the 'Update' button to remove the association of this Class Map and Policy Map;
- *Member Classes* – list of all Class Maps that are associated with the selected Policy Map. If the class is not associated with a policy, this field is empty;
- *Delete Policy Map* – set the flag and click the 'Update' button to delete the Policy Map specified in the Policy Map Name.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

4.11.4 'Client Configuration' submenu

In the **'Client Configuration'** submenu, current QoS configuration in effect for a specific client connected to the access point can be viewed.



- *Station* – select the client connected to the access point;

- *Global QoS Mode* – use of Client QoS on the entire access point globally:
  - *Up* – enabled;
  - *Down* – disabled.
- *Client QoS* Mode – use of Client QoS on the selected VAP:
  - *Enable* – enabled;
  - *Disabled* – disabled.
- *Bandwidth Limit Up* – limiting the traffic bandwidth from each client to the access point, bps;
- *Bandwidth Limit Down* – limiting the traffic bandwidth from the access point to each client, bps;
- *ACL Type Up* – type of traffic from the client to the access point, for which the ACL rules will be applied;
- *ACL Name Up* – name of the ACL profile that should be applied to traffic going from the client to the access point;
- *ACL Type Down* – type of traffic from the access point to the client for which the ACL rules will be applied;
- *ACL Name Down* – name of the ACL profile that should be applied to traffic coming from the access point to the client;
- *DiffServ Policy Up* – name of the Policy profile that should be applied to traffic going from the client to the access point;
- *DiffServ Policy Down* – name of the Policy profile to be applied to traffic going from the access point to the client.

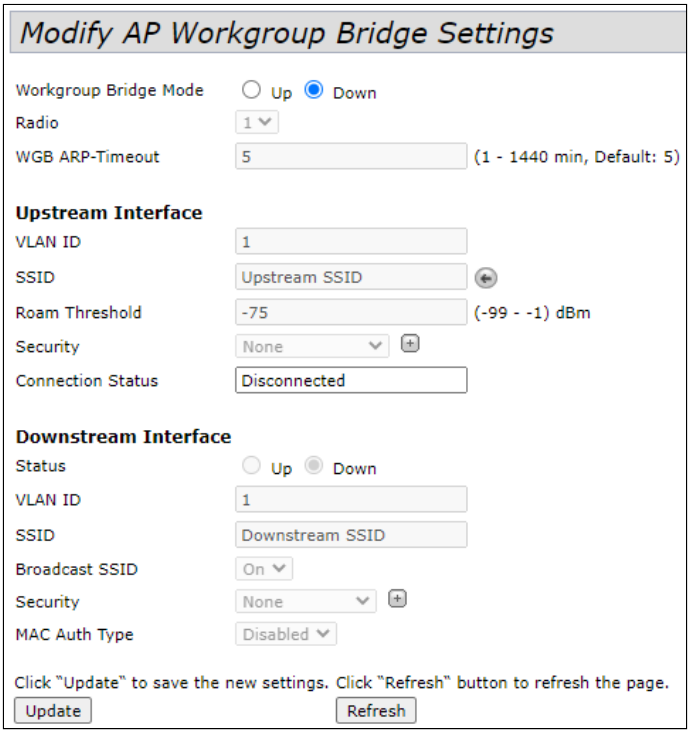
4.12 'Workgroup Bridge' menu

4.12.1 'Workgroup Bridge' submenu

'**Workgroup Bridge**' is intended for configuring the device in the wireless client mode using one of the wireless interfaces.

WGB cannot be configured if WDS is configured on the access point or cluster mode is enabled.

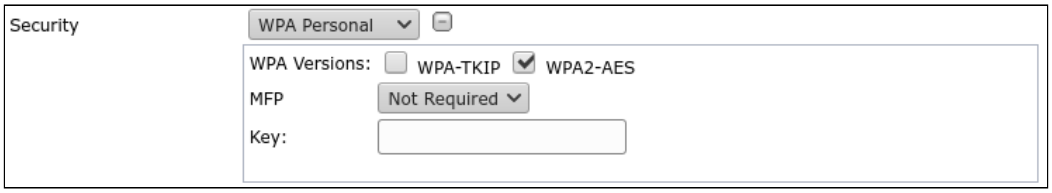
For correct WGB operation, it is necessary that the same firmware version is installed on the access points.



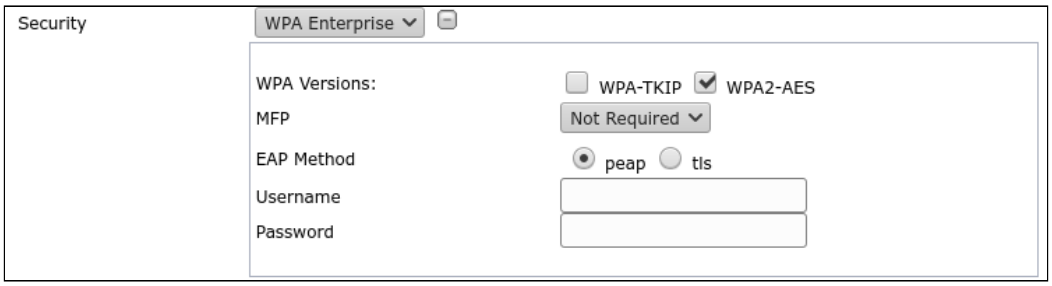
- *Workgroup Bridge Mode* – enable/disable client mode on the interface:
  - *Up* – enabled;
  - *Down* – disabled.
- *Radio* – select wireless interface on which the client mode is enabled. Radio 1 operates on the 5 GHz band, Radio 2 operates on the 2.4 GHz band;
- *WGB ARP-Timeout* – ARP table entry lifetime in WGB mode. The parameter takes a value from 1 to 1440 minutes. The default is 5 minutes.

Upstream Interface – configuring interface that will be a wireless client and connect to a third-party access point.

- *VLAN ID* – VLAN number used on the access point;
- *SSID* – name of the access point to which the connection is made;
- *Roam Threshold* – name of the access point to which the connection is made;
- *Security* – security mode configured on the VAP of the access point to which the connection is made:
  - *None* – do not use encryption for data transfer. The point is open for access by any client;
  - *WPA Personal* – connection mode to an access point using the WPA-TKIP or WPA2-AES security mechanism. When this mode is selected, the following settings will be available for editing:



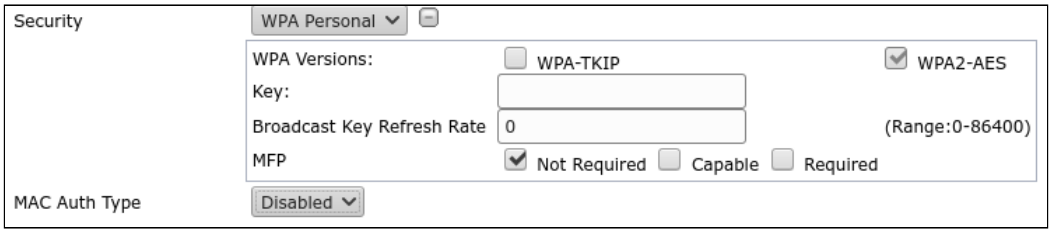
- *WPA Versions* – version of the security protocol used (WPA-TKIP or WPA2-AES);
- *MFP* – configuring client frame protection mode:
  - *Not Required* – do not use protection;
  - *Capable* – use protection when possible;
  - *Required* – use of protection is mandatory, all clients must support CCX5.
- *Key* – key/password required for authorization on the access point;
- *WPA Enterprise* – access point connection mode using authorization and authentication on an upstream RADIUS server. When this mode is selected, the following settings will be available for editing:



- *WPA Versions* – version of the security protocol used (WPA-TKIP or WPA2-AES);
- *MFP* – configuring client frame protection mode:
  - *Not Required* – do not use protection;
  - *Capable* – use protection when possible;
  - *Required* – use of protection is mandatory, all clients must support CCX5.
- *EAP Method* – selection of the authentication protocol (peap or tls);
- *Username* – user name used for authorization on the RADIUS server;
- *Password* – user password used for authorization on the RADIUS server;
- *Connection Status* – connection status to the access point.

Downstream Interface – configuring the interface that acts as an access point.

Status – enable/disable the downstream interface:
  - *Up* – interface is enabled;
  - *Down* – interface is disabled.
- *VLAN ID* – VLAN number in which network traffic for this access point will be transmitted;
- *SSID* – wireless network name;
- *Broadcast SSID* – enable/disable wireless network broadcasting:
  - *On* – broadcasting is enabled;
  - *Off* – broadcasting is disabled.
- *Security* – broadcasting is enabled:
  - *None* – do not use encryption for data transfer. The point is open for access by any client;
  - *WPA Personal* – connection mode to an access point using the WPA-TKIP or WPA2-AES security mechanism. When this mode is selected, the following settings will be available for editing:



- *WPA Versions* – version of the security protocol used (WPA-TKIP or WPA2-AES).

If WPA-TKIP is selected, the following fields will be available for configuration:

- *Key* – key/password required for authorization on the access point;
- *Broadcast Key Refresh Rate* – group key update time interval. The parameter takes values from 0 to 86400.

If WPA2-AES is selected, the following fields will be available for configuration:

- *Key* – key/password required for authorization on the access point;
- *Broadcast Key Refresh Rate* – group key update time interval. The parameter takes values from 0 to 86400;
- *MFP* – configuring client frame protection mode:
  - *Not Required* – do not use protection;
  - *Capable* – use protection when possible;
  - *Required* – use of protection is mandatory, all clients must support CCX5.

MAC Auth Type – user authentication mode based on their MAC address:

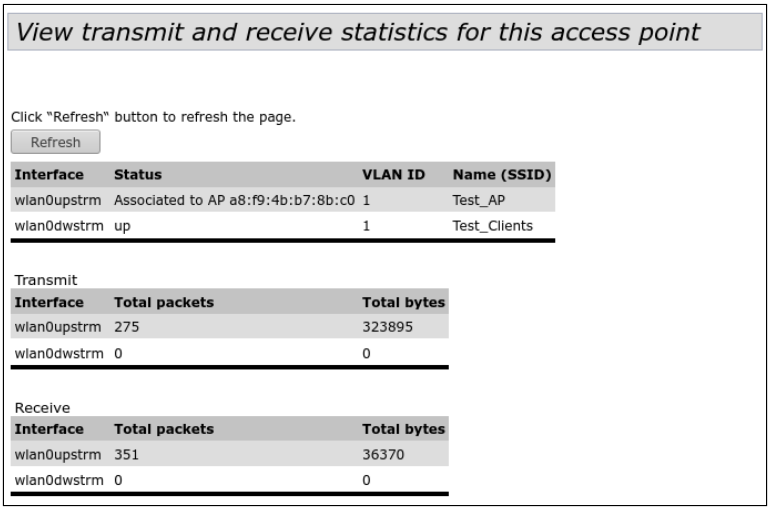
- *Disabled* – do not use user authentication by MAC address;
- *RADIUS* – use user authentication by MAC address using RADIUS server;
- *Local* – use user authentication by MAC address using the local address list generated on this access point.

To apply a new configuration and save setting to non-volatile memory, click 'Update'.

To update information on the page, click 'Refresh'.

4.12.2 'Workgroup Bridge Transmit/Receive' submenu

'**Workgroup Bridge Transmit/Receive**' provides statistics on transmitted/received traffic on interfaces formed in the Work Group Bridge mode.



To update information on the page, click 'Refresh'.

- *Interface* – interface name;
- *Status* – interface operation status;
- *VLAN ID* – VLAN number assigned to the interface;
- *Name (SSID)* – name of the wireless network configured for the interface.

'Transmit' section provides statistics on the transmitted traffic.

'Receive' provides statistics on the received traffic.

- *Interface* – interface name;
- *Total packets* – total number of transmitted/received packets;
- *Total bytes* – total number of bytes sent/received.

5 Managing the device using the command line

This section describes various ways to connect to the command line interface (CLI) of an access point, as well as the basic commands for managing the device through the CLI.

There are three methods available for connecting to an access point.

- Serial port or COM port;
- Telnet, insecure connection;
- SSH, secure connection.

5.1 Connecting to CLI via COM port

To use this type of connection, the personal computer must either have a built-in COM port or must be supplied with a USB-to-COM adapter cable. A terminal program must also be installed on the computer, for example, Hyperterminal, PuTTY, SecureCRT.

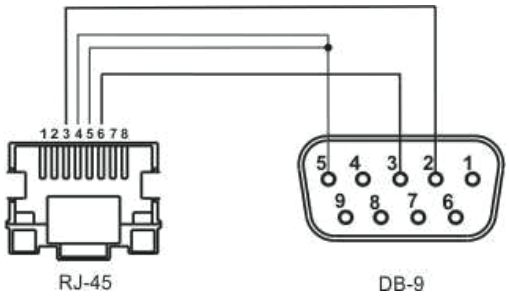
The access point (Console port) connects directly to the computer using a console cable. For access to the device console a terminal program is used.

RJ45-DB9 console cable is required (not supplied with the device) to connect to the access point via COM port.

RJ45-DB9 console cable pinout

Serial Port (RJ-45 Connector) Pin	Adapter (DB-9) Pin
3 (TXD)	2 (RXD)
4 (Signaling Ground)	5 (Signaling Ground)
5 (Signaling Ground)	5 (Signaling Ground)
6 (RXD)	3 (TXD)

The example is shown in the following figure:



Step 1. Using a console cable, connect the **CONSOLE** port of the access point to the computer's COM port. The console cable may require drivers depending on your computer's operating system.

Step 2. Launch terminal program and create new connection. In the **'Connect via'** drop-down list, select the preferred COM port. The COM port (port number) is determined by the device manager, for example, COM4. Set the port parameters according to Table 6. Click the **OK** button.

Table 6 – COM port parameters

Parameters	Value
Baud rate	115200
Data bits	8
Parity	no
Stop bits	1

Parameters	Value
Flow control	no

Step 3. Click the **'Connection'** button. Log in to the device's CLI.

Default login information:

- User name: **admin;**
- Password: **password.**

After successful authorization, *Access point name#* will be displayed, for example, *WEP-2ac#* or *Eltex WLAN AP#* – this means that the access point settings configuration mode is enabled.

By default, the access point's COM port baud rate is 115200 bps. Using the web interface in the 'Serial Settings' section of the 'Status' tab, the baud rate can be changed to 9600, 19200, 38400 and 57600 bps.
The following command is used to change baud rate in CLI: *set serial baud-rate <RATE>* (for example, *set serial baud-rate 115200*). After applying this command, change the baud rate in the connection settings of the terminal program on PC.

5.2 Connecting via Telnet

Telnet connection is more versatile than COM port connection. The disadvantage of such a connection, compared to COM port connection, is that there are no access point initialization messages. Connection to the CLI can be made both directly at the installation site of the device, and from a remote workstation via IP network.
To connect to an access point, a personal computer must have a network card. Additionally, a network cable (Patching Cord RJ-45) is required (not supplied with the device).
To connect via Telnet, programs such as PuTTY, HyperTerminal, SecureCRT can be used.

Step 1. Connect the network cable from the PoE port of the injector to the Ethernet port of the access point (for WEP-2ac, this is **GE (PoE)** port), and the network cable from the Data port of the injector to the network card of the computer.

Step 2. Start, for example, PuTTY. Specify IP address of the access node. Figure 10 shows 192.168.10.10 as an example.

- Access point IP address, by default – **192.168.1.10**;
- Port, by default – **23**;
- Connection type – **Telnet**.

Click the **'Open'** button.

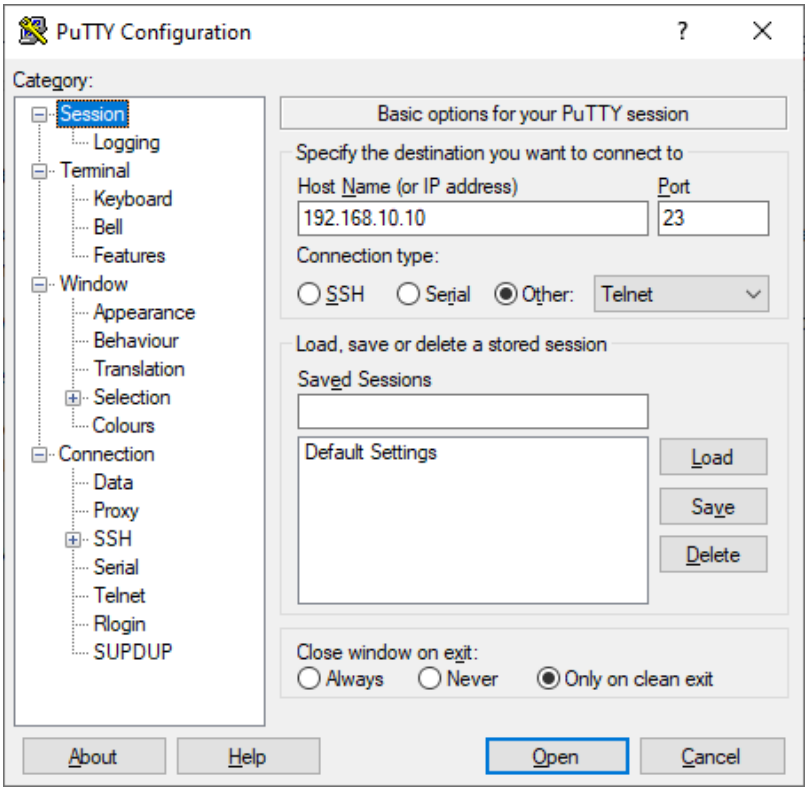


Figure 10 – Telnet client startup

Step 3. Log in to the access point CLI.

Default login information:

- login: **admin;**
- password: **password.**

After successful authorization, *Access point name#* will be displayed, for example, *WEP-2ac#* or *Eltex WLAN AP#* – this means that the access point settings configuration mode is enabled.

5.3 Connecting via Secure Shell

Secure Shell (SSH) connection is similar in functionality to a Telnet connection. Unlike Telnet, Secure Shell encrypts all traffic, including passwords. This ensures secure remote connections over public IP networks. To connect to an access node, a personal computer must have a network card. SSH client program must be installed on the computer, for example, PuTTY , HyperTerminal, SecureCRT. Additionally, a network cable (Patching Cord RJ-45) is required (not supplied with the device).

Step 1. Connect the network cable from the PoE port of the injector to the Ethernet port of the access point (for WEP-2ac, this is **GE (PoE)** port), and the network cable from the Data port of the injector to the network card of the computer.

Step 2. Start, for example, PuTTY. Specify IP address of the access node. Figure 11 shows 192.168.10.10 as an example.

- Access point IP address, by default – **192.168.1.10**;
- Port, by default – **22**;
- Connection type – **SSH**.

Click the **'Open'** button.

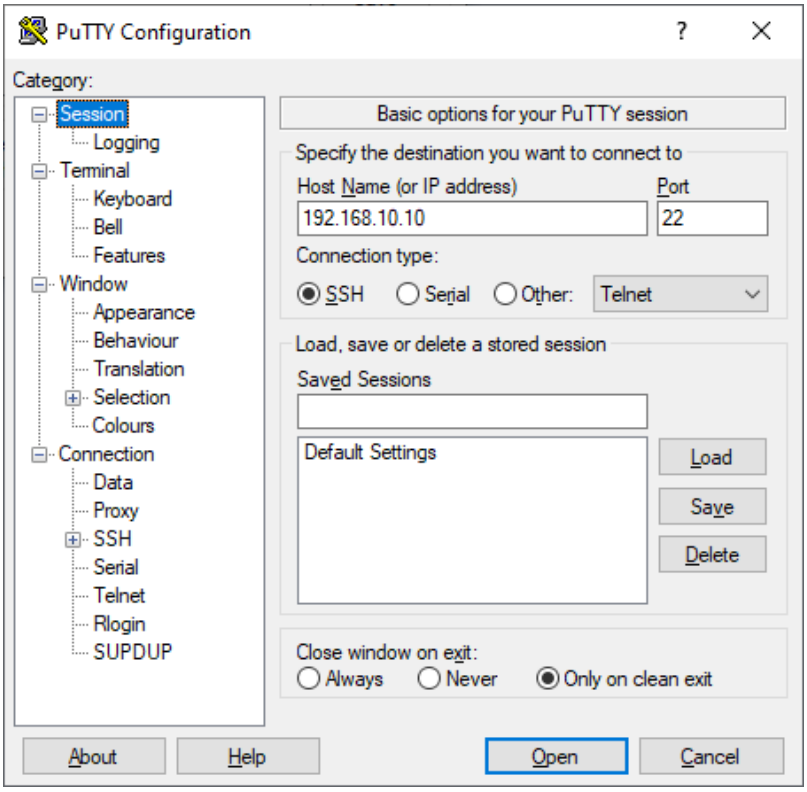


Figure 11 – SSH client startup

Step 3. Log in to the access point CLI.

Default login information:

- login: **admin;**
- password: **password.**

After successful authorization, *Access point name#* will be displayed, for example, *WEP-2ac#* or *Eltex WLAN AP#* – this means that the access point settings configuration mode is enabled.

5.4 Getting started in the access point CLI

In addition to the web configurator, CLI provides an alternative method for specialists to interact with a device. The following section outlines general guidelines for working in the CLI.
The access point configuration is represented by a set of classes (command continuation) and objects (command start). The access point console provides access to the use of such objects:

- get
- set
- add
- remove

The set, add, and remove commands change the current access point configuration, not the boot configuration. To save the current configuration to boot, use the **save-running** command.

5.4.1 Command line rules

To simplify the use of the command line, the interface supports automatic completion of commands. This function is activated when an incomplete command is typed and the <Tab> key is pressed.

Another feature to help using the command line is context help. At any stage of entering a command, a hint about the next elements of the command can be obtained by pressing the <Tab> key twice.

For convenience of using the command line, support for hot keys has been implemented. The list of hot keys is presented in Table 7.

Table 7 – Description of CLI command line hotkeys

Hotkey	Action in CLI
CTRL+a	Moves cursor to the beginning of line
CTRL+e	Moves cursor to the end of line
CTRL+b	Moves cursor to the left
CTRL+f	Moves cursor to the right
CTRL+c	Interrupts command execution
CTRL+h	Deletes one character from the left (backspace)
CTRL+w	Deletes the word to the left of the cursor
CTRL+k	Deletes everything after the cursor
CTRL+u	Deletes everything before the cursor
CTRL+p	Shows the previous command
CTRL+n	Shows the next command
CTRL+d	Exit CLI

5.4.2 Interface notations

This section describes the interface naming used when configuring the device.

To obtain the description in the CLI, execute the **get interface all description** command. For more detailed information about all interfaces, use the **get interface all** command. The interfaces are described in Table 8.

Table 8 – Interface notations

Interface	Description
brtrunk	Bridge - Trunk
brtrunk-user	Bridge - Trunk
eth0	Ethernet
lo	Loopback
isatap0	ISATAP Tunnel
wlan0	Wireless - Virtual Access Point 0
wlan1	Wireless - Virtual Access Point 0 - Radio 2

Interface	Description
wlan0vapX	Wireless - Virtual Access Point X
wlan1vapX	Wireless - Virtual Access Point X - Radio 2
wlan0bssvapX	Virtual Access Point X
wlan1bssvapX	Virtual Access Point X - Radio 2
wlan0wdsX	Wireless Distribution System - Link X

5.4.3 Saving configuration changes

There are several instances of configurations in the system:

– *Factory configuration.* The configuration includes default settings. To return to the factory configuration, use the **factory-reset** command or the 'F' function button on the device case. To do this, hold the 'F' button until the 'Power' indicator starts flashing.

– *Boot configuration*. The boot configuration stores settings that will be used the next time the access point boots (for example, after a reboot). To save the changes made in the CLI to the boot configuration, execute the **save-running** or **set config startup running** command – the current configuration will be copied to the boot configuration;

– *Current configuration.* The access point configuration that is currently applied. When using the **get, set, add, remove** commands, only the current configuration is viewed and changed. If the changes are not saved, they will be lost after rebooting the access point.

5.5 CLI commands description

5.5.1 The *get* command

The ***get*** command allows viewing the set field values in classes. Classes are divided into classes without a name (unnamed-class) and with a name (named-class).

Syntax

```
get unnamed-class <VALUE> |detail
get named-class [<SUBCLASS> |all| [<VALUE> ... | name | detail]]
```

Example

1. An example of using the 'get' command in a class without a name with one set of values:

```
get log
```

The access point has only one set of options for log files, this command displays information about the options of log files.

2. Example of using the 'get' command in a class without a name with multiple values:

```
get log-entry
```

The file stores a continuous sequence of logs without being split into files. The command displays the entire sequence of data contained in the log file.

3. Example of using the 'get' command in a class with a name with multiple values:

```
get bss wlan1bssvap3
```

There is a set of bss class values that are typed in this command. This command displays information about set of basic services called wlan1bssvap3.

4. Example of using the 'get' command in a class with a name to get all values:

```
get interface all mac
get interface all
get radio all detail
```

5.5.2 The *set* command

The ***set*** command sets the values of fields in classes.

Syntax

```
set unnamed-class [<SUBCLASS> <VALUE> ...] <VALUE> ...
set named-class <SUBCLASS> | all |[<SUBCLASS> <VALUE> ...] <VALUE> ...
```

Example

Example of configuring SSID, parameters of Radio interface, and setting a static IP address:

```
set interface wlan0 ssid "Eltex"
set vap vap2 with radio wlan0 to vlan-id 123
set radio all beacon-interval 200
set tx-queue wlan0 with queue data0 to aifs 3
set management static-ip 192.168.10.10
set management static-mask 255.255.255.0
set management dhcp-status down
```

5.5.3 The *add* command

The ***add*** command adds a new subclass or a group of subclasses containing a specific set of values to simplify hardware configuration.

Syntax

```
add unique-named-class <SUBCLASS> [<VALUE> ...]
add group-named-class <SUBCLASS> [<VALUE> ...]
add anonymous-named-class <SUBCLASS> [<VALUE> ...]
```

Example

Example of configuring basic channel rate on Radio interface:

```
add basic-rate wlan1 rate 1
```

5.5.4 The *remove* command

The ***remove*** command removes the created subclasses.

Syntax

```
add unnamed-class [<VALUE> ...]
add named-class <SUBCLASS> | all [<VALUE> ...]
```

Example

Example of deleting basic channel rate settings on Radio interface:

```
remove basic-rate wlan1 rate 1
```

5.5.5 Additional commands

The access point command line interface also includes the following commands, listed in Table 9.

Table 9 – Additional commands

Command	Description
config	Download/Upload access point configuration
copy	Download/Upload/Save access point configuration
delete	Delete configuration files
dot1x-cert	Upload a DOT1X certificate to connect to the access point
factory-reset	Apply factory configuration and reboot
firmware-switch	Change firmware image: current firmware image to alternative image
firmware-upgrade	Firmware update
packet-capture	Generate and upload a traffic dump from an interface
reboot	Reboot the access point
save-running	Saving current configuration to boot
show	Displaying a list of configuration files
wgbridge-cert	Upload a WGB certificate to connect to the access point

5.6 Configuring an access point via the CLI

This section provides an example of configuring the WEP-2ac access point using the command line interface. After connecting to an access point (as described in the Managing the device using the command line section), it is required to configure network parameters if they have not been configured before.

5.6.1 Configuring network parameters

Configuring static network parameters of the access point

WEP-2ac# **set management dhcp-status down** (**down** – disable receiving network parameters via DHCP, use statically configured network parameters. **up** – enable receiving network parameters via DHCP)
WEP-2ac# **set management static-ip 192.168.1.15** (where 192.168.1.15 is device static IP address)
WEP-2ac# **set management static-mask 255.255.255.0** (where 255.255.255.0 is the subnet mask)
WEP-2ac# **set static-ip-route gateway 192.168.1.1** (where 192.168.1.1 is default gateway IP address)

Configuring VLAN for access point management

WEP-2ac# **set management vlan-id 1510** (where 1510 is VLAN number for access point management)

Configuring DNS static IP addresses

WEP-2ac# **set host dns-via-dhcp down** (**down** – use statically set DNS servers. **up** – use DHCP-obtained DNS servers)
WEP-2ac# **set host static-dns-1 8.8.8.8** (where 8.8.8.8 is IP address of DNS server 1)
WEP-2ac# **set host static-dns-2 192.168.1.253** (where192.168.1.253 is IP address of DNS server 2)

5.6.2 Configuring wireless interfaces

By default, radio interfaces use automatic selection of the operating channel. To manually set the channel or change the power, use the following commands:

Configuring radio channel, bandwidth and radio interface power

Configuration for Radio 1 (5 GHz):

WEP-2ac# **set radio wlan0 status up** (**up** – enable Radio 1 radio interface, **down** – disable Radio 1 radio interface)
WEP-2ac# **set radio wlan0 mode a-n-ac** (**a-n-ac** – set Radio 1 radio interface operating mode. The following operating modes are available for Radio 1: **a** – 802.11a, **a-n-ac** – 802.11a/n/ac, **n-ac** – 802.11n/ac)
WEP-2ac# **set radio wlan0 channel-policy static** (**static** – disable automatic channel selection. **best** – enable automatic channel selection)
WEP-2ac# **set radio wlan0 static-channel 36** (**36** – number of static channel on which access point will operate)
WEP-2ac# **set radio wlan0 n-bandwidth 80** (**80** – channel bandwidth. The following bandwidth values are available for Radio 1: **20** – 20 MHz, **40** – 40 MHz, **80** – 80 MHz)
WEP-2ac# **set radio wlan0 tx-power-dbm 19** (**19** – transmitter power value for Radio 1 radio interface. Available values for Radio 1: **from 1 to 21** dBm)

Configuration for Radio 2 (2.4 GHz):

WEP-2ac# **set radio wlan1 status up** (**up** – enable Radio 2 radio interface, **down** – disable Radio 2 radio interface)
WEP-2ac# **set radio wlan1 mode bg-n** (**bg-n** – set Radio 2 radio interface operating mode. The following operating modes are available for Radio 2: **bg** – 802.11b/g, **bg-n** – 802.11b/g/n, **n-only-g** – 2.4 GHz 802.11n)
WEP-2ac# **set radio wlan1 channel-policy static** (**static** – disable automatic channel selection. **best** – enable automatic channel selection)
WEP-2ac# **set radio wlan1 static-channel 6** (**6** – number of static channel on which access point will operate)
WEP-2ac# **set radio wlan1 n-bandwidth 20** (**20** – channel bandwidth. The following bandwidth values are available for Radio 2: **20** – 20 MHz, **40** – 40 MHz)
WEP-2ac# **set radio wlan1 tx-power-dbm 16** (**16** – transmitter power value for Radio 2 radio interface. Available values for Radio 2: **from 5 to 18** dBm)

Lists of available channels

For Radio 1, the following channels are available for selection:

- with 20 MHz channel width: 36, 40, 44, 48, 52, 56, 60, 64, 132, 136, 140, 144, 149, 153, 157, 161, 165.
- with 40 MHz channel width:
  - if 'n-primary-channel' = lower: 36, 44, 52, 60, 132, 140, 149, 157.
  - if 'n-primary-channel' = upper: 40, 48, 56, 64, 136, 144, 153, 161.
- with 80 MHz channel width: 36, 40, 44, 48, 52, 56, 60, 64, 132, 136, 140, 144, 149, 153, 157, 161.

For Radio 2, the following channels are available for selection:

- with 20 MHz channel width: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13.
- with 40 MHz channel width:
  - if 'n-primary-channel' = lower: 1, 2, 3, 4, 5, 6, 7, 8, 9.
  - if 'n-primary-channel' = upper: 5, 6, 7, 8, 9, 10, 11, 12, 13.

5.6.2.1 Additional settings for wireless interfaces

Changing operating mode of the radio interface

Configuration for Radio 1 (5 GHz):

WEP-2ac# **set radio wlan0 mode a-n-ac** (**a-n-ac** – set Radio 1 radio interface operating mode. The following operating modes are available for Radio 1: **a** – 802.11a, **a-n-ac** – 802.11a/n/ac, **n-ac** – 802.11n/ac)

Configuration for Radio 2 (2.4 GHz):

WEP-2ac# **set radio wlan1 mode bg-n** (**bg-n** – set Radio 2 radio interface operating mode. The following operating modes are available for Radio 2: **bg** – 802.11b/g, **bg-n** – 802.11b/g/n, **n-only-g** – 2.4 GHz 802.11n)

Configuring the list of limited channels

Configuration for Radio 1 (5 GHz):

WEP-2ac# **set radio wlan0 limit-channels '36 40 44 48'** (**36 40 44 48** – number of channels that will be used when auto-selecting an operating channel on the access point)

Configuration for Radio 2 (2.4 GHz):

WEP-2ac# **set radio wlan1 limit-channels '1 6 11'** (**1 6 11** – number of channels that will be used when auto-selecting an operating channel on the access point)

Changing primary channel

Configuration for Radio 1 (5 GHz):

WEP-2ac# **set radio wlan0 n-primary-channel upper** (parameter can take the following values: **upper**, **lower**)

Configuration for Radio 2 (2.4 GHz):

WEP-2ac# **set radio wlan1 n-primary-channel upper** (parameter can take the following values: **upper**, **lower**)

Changing VLAN list

Configuration for Radio 1 (5 GHz):

WEP-2ac# **set radio wlan0 vlan-list '10;4033'** (**10** and **4033** – VLAN numbers. Maximum possible number of VLANs in the list: 20)

Configuration for Radio 2 (2.4 GHz):

WEP-2ac# **set radio wlan1 vlan-list '10;4033'** (**10** and **4033** – VLAN numbers. Maximum possible number of VLANs in the list: 20)

Enabling Short Guard interval

Configuration for Radio 1 (5 GHz):

WEP-2ac# **set radio wlan0 short-guard-interval-supported yes** (parameter can take the following values: **yes**, **no**)

Configuration for Radio 2 (2.4 GHz):

WEP-2ac# **set radio wlan1 short-guard-interval-supported yes** (parameter can take the following values: **yes**, **no**)

Enabling STBC

Configuration for Radio 1 (5 GHz):

WEP-2ac# **set radio wlan0 stbc-mode auto** (parameter can take the following values: **auto**, **on**, **off**. Default: **auto**)

Configuration for Radio 2 (2.4 GHz):

WEP-2ac# **set radio wlan1 stbc-mode auto** (parameter can take the following values: **auto**, **on**, **off**. Default: **auto**)

Enabling DFS

Configuration for Radio 1 (5 GHz):

WEP-2ac# **set radio wlan0 dot11h on** (parameter can take the following values: **on**, **off**. Default: **on**)

Enable the automatic channel width change mode

Configuration for Radio 1 (5 GHz):

WEP-2ac# **set radio wlan0 coex-mode on** (parameter can take the following values: **on**, **off**. Default: **on**)

Configuration for Radio 2 (2.4 GHz):

WEP-2ac# **set radio wlan1 coex-mode on** (parameter can take the following values: **on**, **off**. Default: **on**)

Limiting the number of clients connected to the radio interface at the same time

Configuration for Radio 1 (5 GHz):

WEP-2ac# **set radio wlan0 max-stations 150** (**150** – limit on the number of clients. Parameter can take the following values: **from 0 to 200**. Default: **200**)

Configuration for Radio 2 (2.4 GHz):

WEP-2ac# **set radio wlan1 max-stations 150** (**150** – limit on the number of clients. Parameter can take the following values: **from 0 to 200**. Default: **200**)

Configuring DHCP Option 82 processing policy

To configure the 82 DHCP option processing policy on all radio interfaces of the access point at the same time, enter **all** after **radio**. If configuration is required for each radio interface separately, instead of all interfaces, enter the name of the radio interface instead of **all**: **wlan0** – Radio 5 GHz, **wlan1** – Radio 2.4 GHz.

WEP-2ac# **set radio all dhcp-snooping replace** (**replace** – access point substitutes or replaces the option 82 value. The parameter can take the following values: **ignore** – option 82 processing is disabled; **remove** – access point removes option 82 value. By default: **ignore**)

If option 82 processing policy is configured as **replace**, the following parameters become available for configuration:

WEP-2ac# **set radio all dhcp-option-82-CID-format string** (**string** – change CID content to the value specified in **dhcp-option-82-string**. The parameter can take the following values: **APMAC-SSID** – change CID content to <access point MAC address>**;**<SSID name>. **SSID** – change CID content to SSID name, the client is connected to. By default: **APMAC-SSID**)

WEP-2ac# **set radio all dhcp-option-82-string longstring** (**longstring** – value from 1 to 52 characters that will be passed to the CID. Only Latin letters and digits , '.', '-', '_' characters are allowed. If **dhcp-option-82-string** parameter value is not specified, the access point will change the CID to the default value: <access point MAC address>**;**<SSID name>)

WEP-2ac# **set radio all dhcp-option-82-RID-format string2** (**string2** – change RID content to the value specified in **dhcp-option-82-string2**. The parameter can take the following values: **ClientMAC** – change RID content to the MAC address of client device ; **APMAC** – change RID content to the MAC address of access point; **APdomain** – change RID content to the name of the last domain in the tree from the 'AP location' parameter. By default: **ClientMAC**)

WEP-2ac# **set radio all dhcp-option-82-string2 longstring** (**longstring** – value from 1 to 63 characters that will be passed to RID. Only Latin letters and digits, '.', '-', '_' characters are allowed. If **dhcp-option-82-string2** parameter value is not specified, the access point will change the RID to the default value: client device MAC address)

WEP-2ac# **set radio all dhcp-option-82-MAC-format radius** (**radius** – MAC address is sent in RADIUS format; **default** – MAC address is sent in normal format, same as in the 'Client-Ethernet-Address' of DHCP packet)

5.6.3 Virtual Wi-Fi access points (VAP) configuration

5.6.3.1 Configuring VAP without encryption

Configuring VAP0 on Radio 1 (5 GHz):

WEP-2ac# **set bss wlan0bssvap0 status up** (**up** – enable VAP0, **down** – disable VAP0)
WEP-2ac# **set interface wlan0 ssid Test_open_vap0** (**Test_open_vap0** – wireless network name)
WEP-2ac# **set interface wlan0 security plain-text** (**plain-text** – encryption mode – no password)

Configuring VAP1 on Radio 1 (5 GHz):

WEP-2ac# **set bss wlan0bssvap1 status up** (**up** – enable VAP1, **down** – disable VAP1)
WEP-2ac# **set interface wlan0vap1 ssid Test_open_vap1** (**Test_open_vap1** – wireless network name
WEP-2ac# **set interface wlan0vap1 security plain-text** (**plain-text** – encryption mode – no password)

Configuring VAP0 on Radio 2 (2.4 GHz):

WEP-2ac# **set bss wlan1bssvap0 status up** (**up** – enable VAP0, **down** – disable VAP0)
WEP-2ac# **set interface wlan1 ssid Test_open_vap0** (**Test_open_vap0** – wireless network name)
WEP-2ac# **set interface wlan1 security plain-text** (**plain-text** – encryption mode – no password)

Configuring VAP1 on Radio 2 (2.4 GHz):

WEP-2ac# **set bss wlan1bssvap1 status up** (**up** – enable VAP1, **down** – disable VAP1)
WEP-2ac# **set interface wlan1vap1 ssid Test_open_vap1** (**Test_open_vap1** – wireless network name)
WEP-2ac# **set interface wlan1vap1 security plain-text** (**plain-text** – encryption mode – no password)

5.6.3.2 Configuring VAP with WPA-Personal security mode

Configuring VAP0 on Radio 1 (5 GHz):

WEP-2ac# **set bss wlan0bssvap0 status up** (**up** – enable VAP0, **down** – disable VAP0)
WEP-2ac# **set interface wlan0 ssid Test_personal_vap0** (**Test_personal_vap0** – wireless network name)
WEP-2ac# **set interface wlan0 security wpa-personal** (**wpa-personal** – encryption mode)
WEP-2ac# **set interface wlan0 wpa-personal-key 12345678** (**123456789** – password for connection to wireless network. Must contain from 8 to 64 characters)

Configuring VAP1 on Radio 1 (5 GHz):

WEP-2ac# **set bss wlan0bssvap1 status up** (**up** – enable VAP1, **down** – disable VAP1)
WEP-2ac# **set interface wlan0vap1 ssid Test_personal_vap1** (**Test_personal_vap1** – wireless network name)
WEP-2ac# **set interface wlan0vap1 security wpa-personal** (**wpa-personal** – encryption mode)
WEP-2ac# **set interface wlan0vap1 wpa-personal-key 12345678** (**123456789** – password for connection to wireless network. Must contain from 8 to 64 characters)

Configuring VAP0 on Radio 2 (2.4 GHz):

WEP-2ac# **set bss wlan1bssvap0 status up** (**up** – enable VAP0, **down** – disable VAP0)
WEP-2ac# **set interface wlan1 ssid Test_personal_vap0** (**Test_personal_vap0** – wireless network name)
WEP-2ac# **set interface wlan1 security wpa-personal** (**wpa-personal** – encryption mode)
WEP-2ac# **set interface wlan1 wpa-personal-key 12345678** (**123456789** – password for connection to wireless network. Must contain from 8 to 64 characters)

Configuring VAP1 on Radio 2 (2.4 GHz):

WEP-2ac# **set bss wlan1bssvap1 status up** (**up** – enable VAP1, **down** – disable VAP1)
WEP-2ac# **set interface wlan1vap1 ssid Test_personal_vap1** (**Test_personal_vap1** – wireless network name)
WEP-2ac# **set interface wlan1vap1 security wpa-personal** (**wpa-personal** – encryption mode)
WEP-2ac# **set interface wlan1vap1 wpa-personal-key 12345678** (**123456789** – password for connection to wireless network. Must contain from 8 to 64 characters)

5.6.3.3 Configuring VAP with Enterprise authorization

Creating VAP with WPA2-Enterprise security mode

Configuring VAP0 on Radio 1 (5 GHz):

WEP-2ac# **set bss wlan0bssvap0 status up** (**up** – enable VAP0, **down** – disable VAP0)
WEP-2ac# **set interface wlan0 ssid Test_enterprise_vap0** (**Test_enterprise_vap0** – wireless network name)
WEP-2ac# **set interface wlan0 security wpa-enterprise** (**wpa-enterprise** – encryption mode)
WEP-2ac# **set bss wlan0bssvap0 global-radius on** (**on** – use global RADIUS server settings. The parameter can take values: **on**, **off**. By default: **on**)

Configuring VAP1 on Radio 1 (5 GHz):

WEP-2ac# **set bss wlan0bssvap1 status up** (**up** – enable VAP1, **down** – disable VAP1)
WEP-2ac# **set interface wlan0vap1 ssid Test_enterprise_vap1** (**Test_enterprise_vap1** – wireless network name)
WEP-2ac# **set interface wlan0vap1 security wpa-enterprise** (**wpa-enterprise** – encryption mode)
WEP-2ac# **set bss wlan0bssvap1 global-radius on** (**on** – use global RADIUS server settings. The parameter can take values: **on**, **off**. By default: **on**)

Configuring VAP0 on Radio 2 (2.4 GHz):

WEP-2ac# **set bss wlan1bssvap0 status up** (**up** – enable VAP0, **down** – disable VAP0)
WEP-2ac# **set interface wlan1 ssid Test_enterprise_vap0** (**Test_enterprise_vap0** – wireless network name)
WEP-2ac# **set interface wlan1 security wpa-enterprise** (**wpa-enterprise** – encryption mode)
WEP-2ac# **set bss wlan1bssvap0 global-radius on** – use global RADIUS server settings. The parameter can take values: **on**, **off**. By default: **on**)

Configuring VAP1 on Radio 2 (2.4 GHz):

WEP-2ac# **set bss wlan1bssvap1 status up** (**up** – enable VAP1, **down** – disable VAP1)
WEP-2ac# **set interface wlan1vap1 ssid Test_enterprise_vap1** (**Test_enterprise_vap1** – wireless network name)
WEP-2ac# **set interface wlan1vap1 security wpa-enterprise** (**wpa-enterprise** – encryption mode)
WEP-2ac# **set bss wlan1bssvap1 global-radius on** (**on** – use global RADIUS server settings. The parameter can take values: **on**, **off**. By default: **on**)

5.6.3.3.1 Configuring Global RADIUS parameters

WEP-2ac# **set bss wlan0bssvap0 global-radius on** (**on** – use global RADIUS server settings on VAP0 Radio1. The parameter can take values: **on**, **off**. By default: **on**)
WEP-2ac# **set global-radius-server radius-domain enterprise.service.root** (**enterprise.service.root** – user domain)
WEP-2ac# **set global-radius-server radius-ip 192.168.1.100** (**192.168.1.100** – IP address of main RADIUS server)
WEP-2ac# **set global-radius-server radius-backupone-ip 192.168.1.101** (**192.168.1.101** – IP address of backup RADIUS server-1)
WEP-2ac# **set global-radius-server radius-backuptwo-ip 192.168.1.101** (**192.168.1.102** – IP address of backup RADIUS server-2)
WEP-2ac# **set global-radius-server radius-backupthree-ip 192.168.1.101** (**192.168.1.103** – IP address of backup RADIUS server-3)
WEP-2ac# **set global-radius-server radius-key eltex** (**eltex** – key for connection to main RADIUS server)
WEP-2ac# **set global-radius-server radius-backupone-key eltex1** (**eltex1** – key for connection to backup RADIUS server-1)
WEP-2ac# **set global-radius-server radius-backuptwo-key eltex2** (**eltex2** – key for connection to backup RADIUS server-2)
WEP-2ac# **set global-radius-server radius-backupthree-key eltex3** (**eltex3** – key for connection to backup RADIUS server-3)
WEP-2ac# **set global-radius-server radius-current primary** (**primary** – use the main RADIUS server. The parameter can take values: **primary**, **backuptwo**, **backupone**, **backupthree**. By default: **primary**)
WEP-2ac# **set global-radius-server radius-port 1812** (**1812** – RADIUS server port used for authentication and authorization. By default: **1812**)
WEP-2ac# **set global-radius-server radius-accounting-port 1813** (**1813** – RADIUS server port used for user accounting. By default: **1813**)
WEP-2ac# **set global-radius-server radius-accounting on** (**on** – enable sending 'Accounting' messages to the RADIUS server. By default: **off**)

5.6.3.3.2 Configuring RADIUS server for a specific VAP

Example of configuring RADIUS server parameters for VAP0 Radio1 (5 GHz):

```
WEP-2ac# set bss wlan0bssvap0 global-radius off (off – use of global RADIUS server settings is disabled. The parameter can take values: on, off. By default: on)
WEP-2ac# set bss wlan0bssvap0 radius-domain enterprise.service.root (enterprise.service.root – user domain)
WEP-2ac# set bss wlan0bssvap0 radius-ip 192.168.1.100 (192.168.1.100 – IP address of main RADIUS server)
WEP-2ac# set bss wlan0bssvap0 radius-backupone-ip 192.168.1.101 (192.168.1.101 – IP address of backup RADIUS server-1)
WEP-2ac# set bss wlan0bssvap0 radius-backuptwo-ip 192.168.1.101 (192.168.1.102 – IP address of backup RADIUS server-2)
WEP-2ac# set bss wlan0bssvap0 radius-backupthree-ip 192.168.1.101 (192.168.1.103 – IP address of backup RADIUS server-3)
WEP-2ac# set bss wlan0bssvap0 radius-key eltex (eltex – key for connection to main RADIUS server)
WEP-2ac# set bss wlan0bssvap0 radius-backupone-key eltex1 (eltex1 – key for connection to backup RADIUS server-1)
WEP-2ac# set bss wlan0bssvap0 radius-backuptwo-key eltex2 (eltex2 – key for connection to backup RADIUS server-2)
WEP-2ac# set bss wlan0bssvap0 radius-backupthree-key eltex3 (eltex3 – key for connection to backup RADIUS server-3)
WEP-2ac# set bss wlan0bssvap0 radius-current primary (primary – use the main RADIUS server. The parameter can take values: primary, backuptwo, backupone, backupthree. By default: primary)
WEP-2ac# set bss wlan0bssvap0 radius-port 1812 (1812 – RADIUS server port used for authentication and authorization. By default: 1812)
WEP-2ac# set bss wlan0bssvap0 radius-accounting-port 1813 (1813 – RADIUS server port used for user accounting. By default: 1813)
WEP-2ac# set bss wlan0bssvap0 radius-accounting on (on – enable sending 'Accounting' messages to the RADIUS server. By default: off)
```

5.6.3.4 Configuring VAP with portal authorization

To configure VAP with portal authorization:

1. Create VAP without encryption (described in detail in the Configuring VAP without encryption section);
2. Configure portal on the access point;
3. Assign portal to the previously configured VAP.

5.6.3.4.1 Configuring portal

To configure Captive Portal for VAP0 on Radio 1, make changes to the previously created portal template – cp-instance **wlan0bssvap0**. To configure a portal, for example, for VAP12 on Radio 2, edit portal template under the **wlan1bssvap12** name.

Example of configuring portal for VAP0 on Radio 1.

Example of configuring wlan0bssvap0 portal

WEP-2ac# **set captive-portal mode up** (**up** – enable Captive Portal. The parameter can take values: **down**, **up**. By default: **down**)
WEP-2ac# **set cp-instance wlan0bssvap0 global-radius off** (**off** – disable use of Global RADIUS settings for this portal. The parameter can take values: **off**, **on**. By default: **off**)
WEP-2ac# **set cp-instance wlan0bssvap0 radius-ip 192.168.1.100** (**192.168.1.100** – IP address of main RADIUS server)
WEP-2ac# **set cp-instance wlan0bssvap0 radius-key eltex** (**eltex** – key for connection to main RADIUS server)
WEP-2ac# **set cp-instance wlan0bssvap0 radius-domain portal.service.root** (**enterprise.service.root** – user domain)
WEP-2ac# **set cp-instance wlan0bssvap0 radius-accounting on** (**on** – enable sending 'Accounting' messages to the RADIUS server. The parameter can take values: **off**, **on**. By default: **on**)
WEP-2ac# **set cp-instance wlan0bssvap0 external up** (**up** – enable user redirecting to an external virtual portal. The parameter can take values: **up**, **down**. By default: **up**)
WEP-2ac# **set cp-instance wlan0bssvap0 external-url http://192.168.1.100:8080/eltex_portal/** (virtual portal URL that the user will be redirected to when connected to the wireless network)
WEP-2ac# **set cp-instance wlan0bssvap0 admin-mode up** (**up** – enable virtual portal operation. The parameter can take values: **up**, **down**. By default: **down**)

5.6.3.4.2 Binding portal to VAP

By default, a portal with the name of a particular VAP is associated with a given VAP, but it is possible to associate a portal with multiple VAPs. Below is an example of binding a **wlan0bssvap0** portal to VAP3 on Radio 2.

WEP-2ac# **set cp-vap vap3 with radio wlan1 cp-instance-name wlan0bssvap0** (binding portal with a name wlan0bssvap0 to VAP3 on Radio 2)

It is also possible to bind the portal to two VAPs of the same name located on all radio interfaces of the access point.

WEP-2ac# **set cp-vap vap1 cp-instance-name wlan0bssvap0** (simultaneously bind portal with a name wlan0bssvap0 to VAP1 on Radio 1 and VAP1 on Radio 2)

5.6.3.5 Advanced VAP settings

Assigning VLAN ID to VAP

WEP-2ac# **set vap vap0 with radio wlan0 vlan-id 15** (15 – VLAN number assigned to VAP0 Radio1)
WEP-2ac# **set vap vap0 vlan-id 15** (**15** – VLAN number assigned to both VAP0 Radio1 and VAP0 Radio2 at the same time)

Limiting the number of clients connected to VAP at the same time

WEP-2ac# **set bss wlan0bssvap0 max-stations 150** (**150** – limit on the number of clients. The parameter can take values: **from 0 to 200**. By default: **200**)

Enabling Minimal Signal and Roaming Signal

WEP-2ac# **set bss wlan0bssvap0 min-signal-enable on** (**on** – enable minimal signal. To disable enter **off.** By default: **off**)
WEP-2ac# **set bss wlan0bssvap0 min-signal -75** (**-75** – RSSI threshold value, upon reaching which the access point will disconnect the client from the VAP. The parameter can take values **from -100 to -1** dBm)
WEP-2ac# **set bss wlan0bssvap0 check-signal-timeout 10** (**10** – time period in seconds after which a decision is made to disconnect client equipment from the virtual network. By default: **10**)
WEP-2ac# **set bss wlan0bssvap0 roaming-signal-limit -70** (**-70** – RSSI threshold value, upon reaching which the client equipment switches to another access point. The parameter can take values **from -100 to -1** dBm)
Value of the **roaming-signal-limit** parameter must be lower than **min-signal**: if **min-signal** = -75 dB, then **roaming-signal-limit** must be equal to, for example, -70 dBm)

Enabling VLAN Trunk on VAP

WEP-2ac# **set bss wlan0bssvap0 tagged-sta-mode on** (**on** – enable VLAN Trunk on VAP0 Radio 1. To disable, enter **off**)

To allow tagged traffic transmission towards the client, the VLAN numbers that can pass through the radio interface must be designated. VLAN numbers must be specified in **vlan-list** parameters.

Example of **vlan-list** configuration on Radio 1:

WEP-2ac# **set radio wlan0 vlan-list '10;4033'** (**10** and **4033** – VLAN numbers. Maximum possible number of VLAN in the list: 20)

Enabling General VLAN on VAP

WEP-2ac# **set bss wlan0bssvap0 general-vlan-mode on** (**on** – enable General VLAN on VAP0 Radio 1. To disable, enter **off**)
WEP-2ac# **set bss wlan0bssvap0 general-vlan-id 12** (**12** – General VLAN number)

Enabling hidden SSID

WEP-2ac# **set bss wlan0bssvap0 ignore-broadcast-ssid on** (**on** – enable hidden SSID on VAP0 Radio 1. To disable, enter **off**)

Enabling Band Steer

WEP-2ac# **set vap vap0 with radio wlan0 band-steer-mode up** (**up** – enable Band Steer on VAP0 Radio1. To disable, enter **down**)
WEP-2ac# **set vap vap0 band-steer-mode up** (**up** – enable Band Steer simultaneously on VAP0 Radio1 and VAP0 Radio2. To disable, enter **down**)

Enabling client isolation on VAP

WEP-2ac# **set bss wlan0bssvap0 station-isolation on** (**on** – enable client isolation on VAP0 Radio 1. To disable, enter **off**)

Configuring VLAN Priority on VAP

WEP-2ac# **set vap vap0 with radio wlan0 vlan-prio 6** (**6** – DSCP priority assigned to the traffic received by a client connected to VAP0 Radio 1. By default: **0**)
WEP-2ac# **set vap vap0 vlan-prio 6** (**6** – DSCP priority assigned to the traffic received by a client connected to VAP0 Radio 1 or VAP0 Radio 2. By default: **0**)

Configuring DSCP Priority on VAP

WEP-2ac# **set bss wlan0bssvap0 dscp-prio 0** (**0** – priority analysis from the CoS field (802.1p protocol) of tagged packets on VAP0 Radio1. To parse the priority from the DSCP field of the IP packet header, enter **1**)

5.6.4 Configuring Cluster

Configuring Cluster

WEP-2ac# **set cluster cluster-name test** (**test** – cluster name. By default: **default**)
WEP-2ac# **set cluster location floor-2** (**floor-2** – access point physical location. By default: **not set**)
WEP-2ac# **set cluster priority 255** (**255** – access point priority in cluster. If priority of all points in the cluster is the same, then Master point is selected based on the lower MAC address. The parameter can take values: **from 0 to 255**. By default: **0**)
WEP-2ac# **set cluster clustered 1** (**1** – enable Cluster mode. The parameter can take values: **0** – Cluster is disabled; **softwlc** – Cluster is disabled, mode for working with SoftWLC; **1** – Cluster is enabled. By default: **1**)

Configuring Single IP Management

WEP-2ac# **set cluster cluster-ipaddr 192.168.1.222** (**192.168.1.222** – IP address at which the master point of the cluster will be accessible. By default: **0.0.0.0**)

Configuring Cluster security parameters

WEP-2ac# **set cluster cluster secure-mode 1** (**1** – enabling cluster security – only those access points that have the same password specified in the **pass-phrase** parameter can be added to the cluster. To disable, enter **0**. By default: **0**)
WEP-2ac# **set cluster pass-phrase 12345678** (**12345678** – cluster security password. Must contain from 8 to 63 characters)

Updating firmware of the access points included in the cluster

WEP-2ac# **set cluster-firmware-upgrade upgrade-method selective** (**selective** – mode in which only the selected access point will be updated. Enter **all** to update all access points in the cluster)
WEP-2ac# **set cluster-firmware-upgrade upgrade-members 192.168.0.58** (**192.168.0.58** – IP address of the point in the cluster to be updated. If **upgrade-method** = all is selected, there is no need to specify IP address of the access points)
WEP-2ac# **set cluster-firmware-upgrade upgrade-url tftp://<TFTP sever IP address>/<Firmware file name>.tar.gz** (path to the access point firmware file located on the TFTP server. Example: set cluster-firmware-upgrade upgrade-url tftp://192.168.1.7/WEP-2ac-1.22.X.X.tar.gz)
WEP-2ac# **set cluster-firmware-upgrade upgrade start** (**start** – start the firmware update process on the selected access points. To stop the update process, enter **stop**)

5.6.5 Configuring WDS

Example of WDS configuration on Radio 1 (5 GHz).

Before configuring WDS on access points, it is required to turn off the Cluster, configure the radio interface and VAP.

Pre-configuration

WEP-2ac# **set cluster clustered 0** (**0** – disable Cluster mode)
WEP-2ac# **set bss wlan0bssvap0 status up** (**up** – enable VAP0 on Radio1)
WEP-2ac# **set radio wlan0 mode a-n-ac** (**a-n-ac** – set radio interface operation mode, through which the device will connect to the access point in client mode. The operating mode must match the operating mode on the access point))
WEP-2ac# **set radio wlan0 channel-policy static** (**static** – disable channel auto-select)
WEP-2ac# **set radio wlan0 static-channel 144** (**144** – number of static channel on which the access point operates and to which this device will connect in client mode)
WEP-2ac# **set radio wlan0 n-bandwidth 20** (**20** – width of channel on which the access point operates and to which this device will connect in client mode)
WEP-2ac# **set interface wlan0 ssid WDS** (**WDS** – wireless network name on VAP0 Radio 1)
WEP-2ac# **set interface wlan0 security wpa-personal** (**wpa-personal** – encryption mode)
WEP-2ac# **set interface wlan0 wpa-personal-key 12345678** (**123456789** – wireless network password. Must contain from 8 to 64 characters)

8 WDS connections can be configured on the access point in total. WDS interfaces on the point are named as follows: wlan0wdsX, where X is a number from 0 to 7.
Below is an example of configuring WDS without encryption and with the wpa-personal encryption type on the wlan0wds0 interface.

Configuring WDS without encryption

WEP-2ac# **set interface wlan0wds0 radio wlan0** (**wlan0** – select device interface that will be used for WDS configuring. The parameter takes values: **wlan0** (Radio 1 – 5 GHz), **wlan1** (Radio 2 – 2.4 GHz))
WEP-2ac# **set interface wlan0wds0 remote-mac A8:F9:4B:B7:8B:C0** (**A8:F9:4B:B7:8B:C0** – The MAC address of the access point radio interface intended for collaborative work. MAC address of the radio interface is indicated in the output of the *get interface wlanX* command, where X is a wireless interface number: 0 – Radio 1 (5 GHz); 1 – Radio 2 (2.4 GHz))
WEP-2ac# **set interface wlan0wds0 status up** (**up** – enable WDS on the access point. To disable, enter **down**)

Configuring WDS with wpa-personal

WEP-2ac# **set interface wlan0wds0 radio wlan0** (**wlan0** – select device interface that will be used for WDS configuring. The parameter takes values: **wlan0** (Radio 1 – 5 GHz), **wlan1** (Radio 2 – 2.4 GHz))
WEP-2ac# **set interface wlan0wds0 remote-mac A8:F9:4B:B7:8B:C0** (**A8:F9:4B:B7:8B:C0** – MAC address of the access point radio interface intended for collaborative work. MAC address of the radio interface is indicated in the output of the *get interface wlanX* command, where X is a wireless interface number: 0 – Radio 1 (5 GHz); 1 – Radio 2 (2.4 GHz))
WEP-2ac# **set interface wlan0wds0 wds-ssid WDS** (**WDS** – SSID name for configuring encrypted WDS)
WEP-2ac# **set interface wlan0wds0 wds-security-policy wpa-personal** (**wpa-personal** – encryption mode)
WEP-2ac# **set interface wlan0wds0 wds-wpa-psk-key 12345678** (**12345678** – WPA key. The key length is from 8 to 63 characters)
WEP-2ac# **set interface wlan0wds0 status up** (**up** – enable WDS on the access point. To disable, enter **down**)

5.6.6 Configuring WGB

Example of WGB configuration on Radio 1 (5 GHz).

Before configuring WGB on access points, it is required to turn off the Cluster, configure the radio interface and VAP.

Pre-configuration

WEP-2ac# **set cluster clustered 0** (**0** – disable Cluster mode)
WEP-2ac# **set bss wlan0bssvap0 status up** (**up** – enable VAP0 on Radio1)
WEP-2ac# **set radio wlan0 mode a-n-ac** (**a-n-ac**– set radio interface operation mode, through which the device will connect to the access point in client mode. The operating mode must match the operating mode on the access point)
WEP-2ac# **set radio wlan0 channel-policy static** (**static** – disable channel auto-select)
WEP-2ac# **set radio wlan0 static-channel 144** (**144** – number of static channel on which the access point operates and to which this device will connect in client mode)
WEP-2ac# **set radio wlan0 n-bandwidth 20** (**20** – width of channel on which the access point operates and to which this device will connect in client mode)
WEP-2ac# **set interface wlan0 ssid WGB** (**WGB** – wireless network name on VAP0 Radio 1)
WEP-2ac# **set interface wlan0 security wpa-personal** (**wpa-personal** – encryption mode)
WEP-2ac# **set interface wlan0 wpa-personal-key 12345678** (**123456789** – wireless network password. Must contain from 8 to 64 characters)

After preliminary configuration, it is necessary to configure parameters of the 'Upstream Interface' – an interface for connecting to an access point in client mode. Below are examples of the 'Upstream Interface' WGB configuration with different types of encryption.

5.6.6.1 Configuring Upstream Interface

Configuring WGB without encryption

WEP-2ac# **set wgbridge radio wlan0** (**wlan0** – select device interface that will be used for access point connection. The parameter takes values: **wlan0** (Radio 1 – 5 GHz), **wlan1** (Radio 2 – 2.4 GHz))
WEP-2ac# **set wg-bridge-upstrm ssid AP-ssid** (**AP-ssid** – name of the wireless network for device connection in client mode)
WEP-2ac# **set wgbridge wgbridge-mode up** (**up** – enable WGB mode on the access point. To disable, enter **down**)
WEP-2ac# **set wg-bridge-upstrm security plain-text** (**plain-text** – encryption mode. The parameter takes values: **wpa-personal**, **wpa-enterprise**, **plain-text**)
WEP-2ac# **set wg-bridge-upstrm roam-threshold -85** (**-85** – minimum signal level from the access point at which a connection to the point occurs)
WEP-2ac# **set wg-bridge-upstrm vlan-id 15** (**15** – VLAN number used on the access point. By default: **1**)

Configuring WGB with wpa-personal

WEP-2ac# **set wgbridge radio wlan0** (**wlan0** – select device interface that will be used for access point connection. The parameter takes values: **wlan0** (Radio 1 – 5 GHz), **wlan1** (Radio 2 – 2.4 GHz))
WEP-2ac# **set wg-bridge-upstrm ssid AP-ssid** (**AP-ssid** – name of the wireless network for device connection in client mode)
WEP-2ac# **set wgbridge wgbridge-mode up** (**up** – enable WGB mode on the access point. To disable, enter **down**)
WEP-2ac# **set wg-bridge-upstrm wpa-personal-key 12345678** (**12345678** – password required for authorization on the access point. Must contain from 8 to 64 characters)
WEP-2ac# **set wg-bridge-upstrm security wpa-personal** (**wpa-personal** – encryption mode. The parameter takes values: **wpa-personal**, **wpa-enterprise**, **plain-text**)
WEP-2ac# **set wg-bridge-upstrm roam-threshold -85** (**-85** – minimum signal level from the access point at which a connection to the point occurs)
WEP-2ac# **set wg-bridge-upstrm vlan-id 15** (**15** – VLAN number used on the access point. By default: **1**)

Configuring WGB with wpa-enterprise

WEP-2ac# **set wgbridge radio wlan0** (**wlan0** – select device interface that will be used for access point connection. The parameter takes values: **wlan0** (Radio 1 – 5 GHz), **wlan1** (Radio 2 – 2.4 GHz))
WEP-2ac# **set wg-bridge-upstrm ssid AP-ssid** (**AP-ssid** – name of the wireless network for device connection in client mode)
WEP-2ac# **set wgbridge wgbridge-mode up** (**up** – enable WGB mode on the access point. To disable, enter **down**)
WEP-2ac# **set wg-bridge-upstrm security wpa-enterprise** (**wpa-enterprise** – encryption mode. The parameter takes values: **wpa-personal**, **wpa-enterprise**, **plain-text**)
WEP-2ac# **set wg-bridge-upstrm eap-user client** (**client** – user name used for authorization on the RADIUS server;
WEP-2ac# **set wg-bridge-upstrm eap-password clientspassword** (**clientspassword** – user password used for authorization on the RADIUS server;
WEP-2ac# **set wg-bridge-upstrm roam-threshold -85** (**-85** – minimum signal level from the access point at which a connection to the point occurs)
WEP-2ac# **set wg-bridge-upstrm eap-method peap** (**peap** – select authentication protocol. The parameter takes values: **peap**, **tls**)
WEP-2ac# **set wg-bridge-upstrm vlan-id 15** (**15** – VLAN number used on the access point. By default: **1**)

If necessary, the 'Downstream Interface' interface can be configured, which acts as an access point for client devices connection.

5.6.6.2 Configuring Downstream Interface

Configuring 'Downstream Interface' with wpa-personal

WEP-2ac# **set wg-bridge-dwstrm ssid Client-ssid** (**Client-ssid** – name of the wireless network for device connection in client mode)
WEP-2ac# **set wg-bridge-dwstrm wpa-personal-key 12345678** (**12345678** – password for connection to wireless network.
WEP-2ac# **set wg-bridge-dwstrm security wpa-personal** (**wpa-personal** – encryption mode. To create SSID without encryption mode, enter **plain-text**. The parameter takes values: **wpa-personal**, **plain-text**)
WEP-2ac# **set wg-bridge-dwstrm ignore-broadcast-ssid off** (**off** – disable hidden SSID mode. To enable, enter **on**)
WEP-2ac# **set wg-bridge-dwstrm vlan-id 15** (**15** – VLAN number in which network traffic for this access point will be transmitted. By default: **1**)
WEP-2ac# **set wg-bridge-dwstrm status up** (**up** – enable Downstream Interface. To disable, enter **down**)

5.6.6.3 Configuring WGB-ARP-Timeout

Configuring WGB-ARP-Timeout

WOP-2ac# **set wgbridge wgb-arp-timeout 5** (**5** – lifetime of entry in WGB mode ARP table. The parameter takes values from **1** to **1440** minutes. By default: **5** minutes)

5.6.7 System settings

5.6.7.1 Firmware update

Do not turn off the power of the device and do not reboot the device during the firmware update.

To update the firmware via TFTP protocol, upload the WEP-2ac-1.22.XXtar.gz firmware file to the TFTP server and run the following command:

Access point firmware update via TFTP
WEP-2ac# **firmware-upgrade tftp://<TFTP server IP address>/<Firmware file name>** (example: firmware-upgrade tftp://192.168.1.100/WEP-2ac-1.22.X.X.tar.gz

To update the firmware via HTTP, upload the WEP-2ac-1.22.XXtar.gz firmware file to the HTTP server and run the following commands:

Access point firmware update via HTTP
WEP-2ac# **set firmware-upgrade upgrade-url http://<TFTP server IP address>:[port]/<Firmware file name>** (example: set firmware-upgrade upgrade-url http://192.168.1.100:8080/WEP-2ac-1.22.X.X.tar.gz) WEP-2ac# **set firmware-upgrade start yes** (command to start the firmware update)

Switching to a backup version of the access point firmware
WEP-2ac# **firmware-switch**

5.6.7.2 Device configuration management

Resetting the device to factory settings
WEP-2ac# **factory-reset**

Upload the device configuration file to TFTP server
WEP-2ac# **config download tftp://<TFTP server IP address>/<Firmware file name>.xml** (example: config download tftp://192.168.1.100/WEP-2ac.xml)

Download the configuration file to the device from TFTP server
WEP-2ac# **config upload tftp://<TFTP server IP address>/<Firmware file name>.xml** (example: config upload tftp://192.168.1.100/WEP-2ac.xml)

5.6.7.3 Device reboot

Command to reboot the device

WEP-2ac# **reboot**

5.6.7.4 Configuring authentication mode

Configuring authentication via RADIUS

WEP-2ac# **set authentication radius-auth-status on** (on – enable RADIUS authentication. The parameter takes values: **on**, **off**. By default: **off**)

WEP-2ac# **set authentication radius-auth-address <RADIUS server IP address>** (example: set authentication radius-auth-address 192.168.1.1)

WEP-2ac# **set authentication radius-auth-port <RADIUS server port>** (example: set authentication radius-auth-port 1234. By default: **1812**)

WEP-2ac# **set authentication radius-auth-password <RADIUS server key>** (example: set authentication radius-auth-password secret. By default: **password**)

Only user with the name specified in the **`get system username`** can be authenticated (by default: **admin**).
If RADIUS server is unavailable, authentication will be performed using a local account.

5.6.7.5 Configuring date and time

Commands to configure time synchronization with NTP server

WEP-2ac# **set ntp status up** (**up** – enable time synchronization with NTP server. The parameter takes values: **down**, **up**. By default: **up**)
WEP-2ac# **set ntp server 192.168.1.100** (**192.168.1.100** – IP address of the main NTP server)
WEP-2ac# **set ntp alternative-server** ntp1.stratum2.ru (**ntp1.stratum2.ru** – domain name of the backup NTP server-1)
WEP-2ac# **set ntp alternative-server2 192.168.1.102** (**192.168.1.102** – IP address of the backup NTP server-2)
WEP-2ac# **set system time-zone 'Russian Fed. Zone 6 (Novosibirsk; Krasnoyarsk)'** (**Russian Fed. Zone 6 (Novosibirsk; Krasnoyarsk)** – set the time zone. By default: 'Russia (Moscow)')

5.6.7.6 Configuring sending of SNMP traps

WEP-2ac# **set snmp source-status up** (**up** – enable receiving of SNMP requests only from the addresses specified in the **snmp source** parameter. The parameter takes values: **down**, **up**. By default: **down**)
WEP-2ac# **set snmp source 192.168.1.100** (**192.168.1.100** – IP address of the host from which SNMP requests are permitted to be received)
WEP-2ac# **add traphost host 192.168.1.100 community public host-type ipv4 trap_version snmpV2** (configure sending of version **snmpV2** SNMP traps to **ipv4** host with **192.168.1.100** IP address for the **public** group)

5.6.8 Configuring APB

Commands to configure the APB service

WEP-2ac# **set captive-portal mode up** (**up** – enable connection to the APB service. The parameter takes values: **up**, **down**. By default: **up**)
WEP-2ac# **set captive-portal roaming-service-url ws://<APB address>:8090/apb/broadcast** (example: set captive-portal roaming-service-url ws://192.168.1.100:8090/apb/broadcast)
WEP-2ac# **get captive-portal apb-operation-status** (command to display APB service status: **connected**, **not_connected** or **not_running**)

5.6.9 Monitoring

5.6.9.1 Wi-Fi clients

WEP-2ac# **get association detail**

```
Property                Value
------------------------------------------------
interface               wlan0vap1
station                 62:3b:f9:4d:ac:27
authenticated           Yes
associated              Yes
authorized              Yes
ip-address              10.24.80.74
hostname                HUAWEI_P40_Pro-81afe9c34a
fw-version
board-type
rx-packets              318
tx-packets              293
rx-bytes                64360
tx-bytes                158746
tx-rate                 156
rx-rate                 156
tx-actual-rate          0
rx-actual-rate          0
tx-modulation           VHT  LDPC  MCS8  NSS2 20MHz
rx-modulation           VHT  LDPC  MCS8  NSS2 20MHz
listen-interval         10
last-rssi               -48
last-snr                44 dB
noise                   -92 dBm
tx-link-quality         100%
tx-rate-quality         100%
tx-link-capacity        100% (not changed)
tx-drop-bytes           0
rx-drop-bytes           0
tx-drop-packets         0
rx-drop-packets         0
client-qos-enabled      Disabled
bw-limit-up             0
bw-limit-down           0
acl-type-up             None
acl-up
acl-type-down           None
acl-down
policy-up
policy-down
ts-violate-rx-packets
ts-violate-tx-packets
uptime                  00:00:00
identity                tutu
domain                  enterprise.service.root
supported-channels      36-64,132-140,149-165
using-802.11r           No
using-802.11k           No
mode                    802.11ac
```

```
aid                     1
ps-mode                 0
vlan-id                 10
auth-mode               WPA2
encryption              AES-CCMP
eltex-serial-number
assoc-duration          0.001337
auth-duration           2.525727
dhcp-start-duration     0.000000
dhcp-end-duration       0.019971
count-dhcp-dis          0
count-dhcp-off          0
count-dhcp-req          1
count-dhcp-ack          1
```

5.6.9.2 Device information

WEP-2ac# **get system detail**

```
Property                                    Value
-------------------------------------------------------------------
username                                    admin
model                                       Eltex WEP-2ac
version                                     1.22.X.X
altversion                                  1.22.X.X
build-year                                  2021
build-date                                  2021.03.18 13:42 +07
loader-version                              1.22.X.X
platform                                    bcm947452acnrm
uptime                                      0 days, 0 hours, 5 minutes
system-time                                 Tue Apr 27 2021 06:02:52 MST
time-zone                                   Russia (Moscow)
enable-dst                                  off
dst-start                                   March.Second.Sunday/02:00
dst-end                                     November.First.Sunday/02:00
dst-offset                                  60
country                                     RU
country-mode                                on
full-isolation                              on
tunneling-over-wds                          off
force-allow-eth                             off
power-source
nmode-supported                             Y
forty-mhz-supported-g                       Y
forty-mhz-supported-a                       Y
eighty-mhz-supported-a                      Y
base-mac                                    e8:28:c1:c1:27:60
base-mac-status                             on
serial-number                               WP12034181
country-code-is-configurable                on
system-name
system-contact                              admin@example.com
system-location                             Default
band-plan
lastboot                                    success
wpa-personal-key-min-complexity-support     off
wpa-personal-key-min-character-class        3
wpa-personal-key-min-length                 8
wpa-personal-key-max-length                 63
wpa-personal-key-different-from-current     no
password-min-complexity-support             off
password-min-character-class                3
password-min-length                         8
password-max-length                         64
password-aging-support                      off
password-aging-time                         180
password-different-from-current             yes
```

5.6.9.3 Network information

WEP-2ac# **get management detail**

```
Property                    Value
------------------------------------------
vlan-id                     1
mtu                         1500
interface                   brtrunk
tunnel-ip
static-ip                   192.168.1.10
static-mask                 255.255.255.0
ip                          100.110.0.242
mask                        255.255.254.0
mac                         E8:28:C1:C1:27:60
ap-location                 eltex.root
dhcp-status                 up
static-ipv6                 ::
static-ipv6-mask
ipv6
ipv6-mask
sw-ratelimit-enable         up
sw-ratelimit-timer          100
ucast-prom-ratelimit        150000
ucast-sw-ratelimit-mode     auto
ucast-sw-ratelimit          120000
ucast-sw-gre-ratelimit      10500
mcast-sw-ratelimit          10000
bcast-sw-ratelimit          1000
arp-req-sw-ratelimit        500
vlan-lock                   up
ipv6-status                 down
ipv6-autoconfig-status      down
static-ipv6                 ::
static-ipv6-prefix-length   0
static-ipv6-addr-status
dhcp6-status                up
autoconfig-link-local
autoconfig-ipv6-global-all
```

WEP-2ac# **get ip-route**

```
Property     Value
-------------------------
destination  0.0.0.0
mask         0.0.0.0
gateway      100.110.0.1
table        254
```

WEP-2ac# **get ntp detail**

```
Property                Value
-----------------------------------------
status                  up
server                  100.110.1.253
alternative-server      100.110.0.22
alternative-server2     0.ru.pool.ntp.org
```

```
dhcp_server               100.110.1.252
dhcp_alt_server
dhcp_alt_server2
manual-daily-drift-secs   0
```

5.6.9.4 Wireless interfaces

WEP-2ac# **get radio wlan0 detail**

```
Property                          Value
------------------------------------------------------
status                            up
description                       IEEE 802.11a
static-mac
channel-policy                    best
channel-update                    1440
mode                              a-n-ac
tpc                               off
scb-timeout                       120
atf                               on
ampdu_atf_us                      4000
ampdu_atf_min_us                  1000
dot11h                            off
dot11d                            up
static-channel                    36
channel                           56
tx-power-dbm                      19
tx-power-dbm-max                  19
tx-power-dbm-min                  1
tx-power-output                   0.00
tx-chain                          3
beacon-interval                   100
rts-threshold                     2347
fragmentation-threshold           2346
arp-suppression                   on
ap-detection                      on
limit-channels                    36 40 44 48 52 56 60 64
operational-bandwidth             20
n-bandwidth                       20
n-primary-channel                 lower
protection                        auto
edca-template                     custom
short-guard-interval-supported    no
stbc-mode                         auto
ldpc-mode                         auto
dhcp-snooping-mode                ignore
dhcp-option-82-string
coex-mode                         on
vlan-list
wme                               on
wme-noack                         off
wme-apsd                          on
rate-limit-enable                 off
rate-limit                        50
rate-limit-burst                  75
stp-block-enable                  on
wlan-util                         8
num-stations                      0
wds-status                        down
fixed-multicast-rate              auto
fixed-tx-modulation               auto
max-stations                      200
```

```
dtim-period                     2
reinit-period                   0
scheduler-profile-name
operational-mode                up
scheduler-operational-mode
vht-mode                        on
vht-features                    off
rsdb-mode
frame-burst                     off
spectrum-analyser-start
spectrum-analyser-status        Not ready
spectrum-analyser-results       Not ready
rrm-block-tpc
rrm-block-dca
ampdu                           up
amsdu                           up
olpc-cal-period                 300
olpc-channel                    yes
```

WEP-2ac# **get radio wlan1 detail**

```
Property                        Value
------------------------------------------
status                          up
description                     IEEE 802.11g
static-mac
channel-policy                  best
channel-update                  1440
mode                            bg-n
tpc                             off
scb-timeout                     120
atf                             on
ampdu_atf_us                    4000
ampdu_atf_min_us                1000
dot11h                          off
dot11d                          up
static-channel                  6
channel                         11
tx-power-dbm                    16
tx-power-dbm-max                16
tx-power-dbm-min                5
tx-power-output                 15.25
tx-chain                        3
beacon-interval                 100
rts-threshold                   1025
fragmentation-threshold         1024
arp-suppression                 on
ap-detection                    on
limit-channels                  1 6 11
operational-bandwidth           20
n-bandwidth                     20
n-primary-channel               lower
protection                      auto
edca-template                   custom
short-guard-interval-supported  no
stbc-mode                       auto
ldpc-mode                       auto
dhcp-snooping-mode              ignore
dhcp-option-82-string
```

```
coex-mode                       on
vlan-list
wme                             on
wme-noack                       off
wme-apsd                        on
rate-limit-enable               off
rate-limit                      50
rate-limit-burst                75
stp-block-enable                on
wlan-util                       88
num-stations                    0
wds-status                      down
fixed-multicast-rate            auto
fixed-tx-modulation             auto
max-stations                    200
dtim-period                     2
reinit-period                   0
scheduler-profile-name
operational-mode                up
scheduler-operational-mode
vht-mode
vht-features                    off
rsdb-mode
frame-burst                     off
spectrum-analyser-start
spectrum-analyser-status        Not ready
spectrum-analyser-results       Not ready
rrm-block-tpc
rrm-block-dca
ampdu                           up
amsdu                           down
olpc-cal-period                 300
olpc-channel                    no
```

5.6.9.5 WDS

WEP-2ac# **get interface wlan0wds0 detail**

```
Property                Value
------------------------------------------------------------
type                    wds
status                  up
description             Wireless Distribution System - Link 1
mac                     E8:28:C1:C1:27:60
ip
mask
static-ip
static-mask
rx-bytes                8235818
rx-packets              38800
rx-errors               0
tx-bytes                172159433
tx-packets              263429
tx-errors               0
tx-drop-bytes           0
rx-drop-bytes           0
tx-drop-packets         0
rx-drop-packets         0
ts-vo-rx-packets        0
ts-vo-tx-packets        0
ts-vo-rx-bytes          0
ts-vo-tx-bytes          0
ts-vi-rx-packets        0
ts-vi-tx-packets        0
ts-vi-rx-bytes          0
ts-vi-tx-bytes          0
ts-be-rx-packets        0
ts-be-tx-packets        0
ts-be-rx-bytes          0
ts-be-tx-bytes          0
ts-bk-rx-packets        0
ts-bk-tx-packets        0
ts-bk-rx-bytes          0
ts-bk-tx-bytes          0
priority                128
port-isolation
auto-negotiation
speed
duplex
link-status
link-uptime
intf-speed
duplex-mode
green-ethernet-mode
ssid
bss
security
wep-key-ascii           no
wep-key-length          104
wep-default-key
wep-key-mapping-length
```

```
vlan-interface
vlan-id
radio                   wlan0
remote-mac              A8:F9:4B:B7:8B:C0
remote-rssi             -16
wep-key
operational-status      up
wds-link-uptime         00:00:46
wds-ssid                WDS
wds-security-policy     wpa-personal
wds-wpa-psk-key         12345678
```

5.6.9.6 WGB

WEP-2ac# **get wgbridge detail**

```
Property       Value
--------------------
wgbridge-mode  up
radio          wlan0
debug
```

WEP-2ac# **get wg-bridge-upstrm detail**

```
Property           Value
-----------------------------------------------------
ssid               AP-ssid
security           wpa-personal
wep-key-ascii      no
wep-key-length     104
wep-default-key    1
wpa-allowed        off
wpa2-allowed       on
upstream-bssid
vlan-id            1
connection-status  Associated to AP a8:f9:4b:b7:8b:c0
rx-bytes           8337952
rx-packets         50212
rx-errors          0
tx-bytes           306207
tx-packets         913
tx-errors          0
iface              wlan0upstrm
eap-user
eap-method         peap
debug
cert-present       no
cert-exp-date      Not Present
mfp                mfp-not-reqd
roam-threshold     -75
roam-delta         10
```

WEP-2ac# **get wg-bridge-dwstrm detail**

```
Property                     Value
-----------------------------------------
ssid                         Client-ssid
security                     wpa-personal
wep-key-ascii                no
wep-key-length               104
wep-default-key              1
wep-key-mapping-length
status                       up
ignore-broadcast-ssid        off
open-system-authentication   on
shared-key-authentication    off
wpa-cipher-tkip              on
wpa-cipher-ccmp              on
wpa-allowed                  on
```

```
wpa2-allowed                on
broadcast-key-refresh-rate  0
vlan-id                     1
rx-bytes                    6522
rx-packets                  40
rx-errors                   0
tx-bytes                    8439
tx-packets                  34
tx-errors                   0
iface                       wlan0dwstrm
mfp                         mfp-not-reqd
```

5.6.9.7 Cluster

WEP-2ac# **get cluster detail**

```
Property            Value
---------------------------------
clustered           1
location            floor-2
cluster-name        test
ipversion           ipv4
member-count        2
clustering-allowed  true
compat              WEP-2ac
operational-mode    1
cluster-ipaddr      192.168.0.222
priority            255
reauth-timeout      300
secure-mode         1
pass-set            1
secure-mode-status  Enabled
trace-debug         0
```

WEP-2ac# **get cluster-member detail**

```
Property            Value
-------------------------------------
mac                 A8:F9:4B:B7:8B:C0
ip                  192.168.0.58
compat              WEP-2ac
location            floor-1
uptime              120
is-dominant         true
priority            0
firmware-version    1.22.X.X
cluster-controller  no

Property            Value
-------------------------------------
mac                 E8:28:C1:C1:27:60
ip                  192.168.0.135
compat              WEP-2ac
location            floor-2
uptime              124
is-dominant         false
priority            255
firmware-version    1.22.X.X
cluster-controller  yes
```

WEP-2ac# **get cluster-fw-member detail**

```
Property         Value
-----------------------------------------------------------
upgrade
upgrade-url      tftp://192.168.1.7/WEP-2ac-1.22.X.X.tar.gz
upgrade-method   selective
upgrade-status   Completed
```

```
upgrade-members  192.168.0.58
```

WEP-2ac# **get cluster-fw-member**

```
ip             mac                fw-download-status
-----------------------------------------------
192.168.0.58   A8:F9:4B:B7:8B:C0  Success
192.168.0.135  E8:28:C1:C1:27:60  None
```

5.6.9.8 Event log

WEP-2ac# **get log-entry**

```
Property  Value
--------------------------------------------------------------------------
number    1
priority  debug
time      Apr 27 2021 05:32:50
daemon    hostapd[17753]
message   Station 62:3b:f9:4d:ac:27 associated, time = 0.001337

Property  Value
--------------------------------------------------------------------------
number    2
priority  debug
time      Apr 27 2021 05:32:50
daemon    hostapd[17753]
message   station: 62:3b:f9:4d:ac:27 associated rssi -49(-49)

Property  Value
--------------------------------------------------------------------------
number    3
priority  info
time      Apr 27 2021 05:32:50
daemon    hostapd[17753]
message   STA 62:3b:f9:4d:ac:27 associated with BSSID e8:28:c1:c1:27:61

Property  Value
--------------------------------------------------------------------------
number    4
priority  info
time      Apr 27 2021 05:32:50
daemon    hostapd[17753]
message   Assoc request from 62:3b:f9:4d:ac:27 BSSID e8:28:c1:c1:27:61 SSID Test_Enterprise
```

5.6.9.9 Environment scan

Environment scan provides information about all wireless access points that the device detects around itself.

WEP-2ac# **get detected-ap**

```
mac                type  privacy  ssid                channel  signal
-------------------------------------------------------------------
e0:d9:e3:50:71:e0  AP    On       i-OTT-ent-06        56       -61
e0:d9:e3:50:71:e1  AP    Off      i-OTT-06-portal     56       -61
e8:28:c1:d7:3c:24  AP    Off      i-200               11       -45
a8:f9:4b:17:02:20  AP    Off      (Non Broadcasting)  11       -56
e8:28:c1:cf:d9:14  AP    On       RT-WiFi-5278        11       -61
e0:d9:e3:8a:38:50  AP    Off      GPB_Free            11       -53
```

5.6.9.10 Spectrum analyzer

Spectrum analyzer provides information on channel congestion in the 2.4 and 5 GHz bands. Spectrum analyzer scans the channels specified in the **limit-channels** parameter in the radio interface settings. The result is displayed as a percentage.

After starting the scan, wait a few minutes to get the results. During the scan, connected clients will experience service interruptions.

WEP-2ac# **set radio all spectrum-analyser-start yes** (start of spectrum analyzer on all radio interfaces simultaneously. To start spectrum analyzer on a specific interface, instead of **all**, enter the name of the interface: **wlan0** – Radio1, **wlan1** – Radio2)

WEP-2ac# **get radio all spectrum-analyser-results** (output of the result of the spectrum analyzer)

```
Property                   Value
-----------------------------------------------------
name                       wlan0
spectrum-analyser-results
  36:      52  | ***********
  40:      52  | ***********
  44:      15  | ****
  48:      13  | ***
  52:       9  | **
  56:       4  | *
  60:       5  | **
  64:      10  | ***
Optimal 20MHz channel: 56
Optimal 40MHz channel: 52l
Optimal 80MHz channel: 56/80

Property                   Value
-----------------------------------------------------
name                       wlan1
spectrum-analyser-results
   1:      92  | ******************
   6:      84  | ****************
  11:      88  | ******************
Optimal 20MHz channel: 11
```

6 Appendix. List of the main classes and subclasses of the commands

Class	Subclass	Feature	Possible commands	Syntax	Examples
debug Debug commands	level	Debug information level	get, set	get debug level set debug level <value>	WEP-2ac# get debug level 0
	timestamp	Add time stamp to debugging information	get, set	get debug timestamp set debug timestamp <value>	WEP-2ac# get debug timestamp
	klevel	Kernel debug information level	get, set	get debug klevel set debug klevel <value>	WEP-2ac# set debug klevel 1 WEP-2ac# get debug klevel 1
system System settings	password	Password to user web interface and CLI	set	set system password <value>	WEP-2ac# set system password password
	model	Device model	get	get system model	WEP-2ac# get system model Eltex WEP-2ac
	version	Firmware version	get	get system version	WEP-2ac# get system version 1.14.0.89
	platform	Hardware platform	get	get system platform	WEP-2ac# get system platform bcm953012er
	encrypted-password	Encrypted password	get, set	get system encrypted-password set system encrypted-password <value>	WEP-2ac# set system encrypted-password "1G6G6G6G6$Dh39pxWqjp3nBRrBPBL7o1" WEP-2ac# WEP-2ac# get system encrypted-password1G6G6G6G6$Dh39pxWqjp3nBRrBPBL7o1

Class	Subclass	Feature	Possible commands	Syntax	Examples
	uptime	System uptime since boot	get	get system uptime	WEP-2ac# get system uptime 6 days, 17 hours, 25 minutes
	system-time	Current system time	get	get system system-time	WEP-2ac# get system system-time Thu May 31 2018 06:59:46 MST
	time-zone	Time zone	get, set	get system time-zone set system time-zone <value>	WEP-2ac# set system time-zone "Russia (Moscow)" WEP-2ac# get system time-zone Russia (Moscow) WEP-2ac#
	enable-dst	Enable daylight saving time	get, set	get system enable-dst set system enable-dst <value>	WEP-2ac# set system enable-dst on WEP-2ac# get system enable-dst on
	summer-time		get, set	get system summer-time set system summer-time <value>	WEP-2ac# set system summer-time enabled WEP-2ac# get system summer-time enabled
	dst-start	Daylight saving time start	get, set	get system dst-start set system dst-start <value>	WEP-2ac# set system dst-start "March.Second.Sunday/02:00" WEP-2ac# get system dst-start March.Second.Sunday/02:00
	dst-end	Daylight saving time end	get, set	get system dst-end set system dst-end <value>	WEP-2ac# set system dst-start "November.First.Sunday/02:00" WEP-2ac# get system dst-end November.First.Sunday/02:00

Class	Subclass	Feature	Possible commands	Syntax	Examples
	dst-offset		get, set	get system dst-offset set system dst-offset <value>	WEP-2ac# set system dst-offset 60 WEP-2ac# get system dst-offset 60
	reboot	Reboot the access point	set	set system reboot	WEP-2ac# set system reboot
	country	Country	get, set	get system country set system country <value>	WEP-2ac# set system country RU WEP-2ac# get system country RU
	country-mode	Possible values: on, off	get, set	get system country-mode set system country-mode <value>	WEP-2ac# set system country-mode off WEP-2ac# get system country-mode off
	full-isolation	Full isolation. Possible values: on – feature is active, off – feature is inactive	get, set	get system full-isolation set system full-isolation <value>	WEP-2ac# set system full-isolation off WEP-2ac# get system full-isolation off
	nmode-supported	IEEE 802.11n standard support. Possible values: Y – supported, N – not supported	get	get system nmode-supported	WEP-2ac# get system nmode-supported Y
	forty-mhz-supported	40 MHz bandwidth support in 5 GHz band	get	get system forty-mhz-supported	

Class	Subclass	Feature	Possible commands	Syntax	Examples
	base-mac		get, set	get system base-mac set system base-mac <value>	WEP-2ac# set system base-mac "a8:f9:4b:b0:21:60" WEP-2ac# get system base-mac a8:f9:4b:b0:21:60
	serial-number	Device serial number	get, set	get system base-mac set system base-mac <value>	WEP-2ac# set system serial-number WP01000167 WEP-2ac# get system serial-number WP01000167
	country-code-is-configurable	Country code configuration. Possible values: on – feature is active, off – feature is inactive	get, set	get system country-code-is-configurable set system country-code-is-configurable <value>	WEP-2ac# set system country-code-is-configurable on WEP-2ac# get system country-code-is-configurable on
	system-name	System name	get, set	get system system-name set system system-name <value>	WEP-2ac# set system system-name "WEP-2ac" WEP-2ac# get system system-name WEP-2ac
	system-contact	System contacts	get, set	get system system-contact set system system-contact <value>	
	system-location	System location	get, set	get system system-location set system system-location <value>	WEP-2ac# get system system-location Default

Class	Subclass	Feature	Possible commands	Syntax	Examples
host Host settings	id	Host ID	get, set	get host id set host id <value>	WEP-2ac# set host id "WEP-2ac" WEP-2ac# get host id WEP-2ac
	dns-1	DNS server (1) IP address	get	get host dns-1	WEP-2ac# get host dns-1 172.16.0.250
	dns-2	DNS server (2) IP address	get	get host dns-2	WEP-2ac# get host dns-2 172.16.0.100
	domain	Domain name	get	get host domain	WEP-2ac# get host domain eltex.loc
	static-dns-1	DNS server (1) that will be used, if address is not obtained via DHCP	get, set	get host static-dns-1 set host static-dns-1 <value>	WEP-2ac# get host static-dns-1
	static-dns-2	DNS server (2) that will be used, if address is not obtained via DHCP	get, set	get host static-dns-2 set host static-dns-2 <value>	WEP-2ac# get host static-dns-1
	static-domain	Domain name that will be used, if domain name is not obtained via DHCP	get, set	get host static-domain set host static-domain <value>	WEP-2ac# set host static-domain "example.com" WEP-2ac# get host static-domain example.com

Class	Subclass	Feature	Possible commands	Syntax	Examples
	dns-via-dhcp	Receive DNS server parameters via DHCP. Possible values: up – receive via DHCP, down – use static parameters	get, set	get host dns-via-dhcp set host dns-via-dhcp <value>	WEP-2ac# set host dns-via-dhcp up WEP-2ac# get host dns-via-dhcp up
config Configuration settings	startup	Configuration during boot	set	set config startup <value>	
	version	Configuration file version	get	get config version	WEP-2ac# get config version 1.02
	backup-file-format	Configuration file format. Possible values: plain – unencrypted, encrypted – encrypted	get, set	get config backup-file-format set config backup-file-format <value>	WEP-2ac# set config backup-file-format plain WEP-2ac# get config backup-file-format plain
interface Network interface settings	type	Network interface type	add, get	add interface <interface_name> type <value> get interface <interface_name> type	WEP-2ac# add interface wlan1vap1 type service-set WEP-2ac# get interface wlan1vap1 type service-set

Class	Subclass	Feature	Possible commands	Syntax	Examples
	status	Interface status	add, get, set	add interface <interface_name> status <value> get interface <interface_name> status set interface <interface_name> status <value>	WEP-2ac# add interface wlan1vap1 status up WEP-2ac# set interface wlan1vap1 status up WEP-2ac# get interface wlan1vap1 status up
	description	Interface description	get, set	get interface <interface_name> description set interface <interface_name> description <value>	WEP-2ac# get interface wlan1vap1 description "Wireless - Virtual Access Point 1 - Radio 2" WEP-2ac# get interface wlan1vap1 description Wireless - Virtual Access Point 1 - Radio 2
	ip	Interface IP address	add, get	add interface <interface_name> ip <value> get interface <interface_name> ip	WEP-2ac# get interface wlan1vap1 ip
	mask	Network mask	add, get, set	add interface <interface_name> mask <value> get interface <interface_name> mask set interface <interface_name> mask <value>	WEP-2ac# get interface wlan1vap1 mask

Class	Subclass	Feature	Possible commands	Syntax	Examples
	static-ip	Static IP address used when DHCP server is inactive	add, get, set	add interface <interface_name> static-ip get interface <interface_name> static-ip set interface <interface_name> static-ip <value>	WEP-2ac# get interface wlan1vap1 static-ip
	static-mask	Network mask used when DHCP server is inactive	add, get, set	add interface <interface_name> static-mask get interface <interface_name> static-mask set interface <interface_name> static-mask <value>	WEP-2ac# get interface wlan1vap1 static-mask
	rx-bytes	Number of received bytes	get	get interface <interface_name> rx-bytes	WEP-2ac# get interface wlan1vap1 rx-bytes 0
	rx-packets	Number of received packets	get	get interface <interface_name> rx-packets	WEP-2ac# get interface wlan1vap1 rx-packets 0
	rx-errors	Number of packets received with errors	get	get interface <interface_name> rx-errors	WEP-2ac# get interface wlan1vap1 rx-errors 0
	rx-drop	Number of received packets that were dropped	get	get interface <interface_name> rx-drop	

Class	Subclass	Feature	Possible commands	Syntax	Examples
	rx-fifo	Number of packets received on buffer overflow	get	get interface <interface_name> rx-fifo	WEP-2ac# get interface wlan1vap1 rx-fifo 0
	rx-frame	Number of packets received with frame error	get	get interface <interface_name> rx-frame	WEP-2ac# get interface wlan1vap1 rx-frame 0
	rx-compressed	Number of received compressed packets	get	get interface <interface_name> rx-compressed	WEP-2ac# get interface wlan1vap1 rx-compressed 0
	rx-multicast	Number of received multicast packets	get	get interface <interface_name> rx-multicast	WEP-2ac# get interface wlan1vap1 rx-multicast 0
	tx-bytes	Number of bytes sent	get	get interface <interface_name> tx-bytes	WEP-2ac# get interface wlan1vap1 tx-bytes 0
	tx-packets	Number of packets sent	get	get interface <interface_name> tx-packets	WEP-2ac# get interface wlan1vap1 tx-packets 0
	tx-errors	Number of packets sent with errors	get	get interface <interface_name> tx-errors	WEP-2ac# get interface wlan1vap1 tx-errors 0
	tx-fifo	Number of packets sent on buffer overflow	get	get interface <interface_name> tx-fifo	WEP-2ac# get interface wlan1vap1 tx-fifo 0
	tx-colls	Number of packets sent with collisions	get	get interface <interface_name> tx-colls	WEP-2ac# get interface wlan1vap1 tx-colls

Class	Subclass	Feature	Possible commands	Syntax	Examples
	tx-carrier	Number of packets sent with carrier errors	get	get interface <interface_name> tx-carrier	WEP-2ac# get interface wlan1vap1 tx-carrier
	tx-compressed	Number of compressed packets sent	get	get interface <interface_name> tx-compressed	WEP-2ac# get interface wlan1vap1 tx-compressed
	tx-drop-bytes	Number of dropped Tx bytes	get	get interface <interface_name> tx-drop-bytes	WEP-2ac# get interface wlan1vap1 tx-drop-bytes
	rx-drop-bytes	Number of dropped Rx bytes	get	get interface <interface_name> rx-drop-bytes	WEP-2ac# get interface wlan1vap1 rx-drop-bytes
	tx-drop-packets	Number of dropped Tx packets	get	get interface <interface_name> tx-drop-packets	WEP-2ac# get interface wlan1vap1 tx-drop-packets
	rx-drop-packets	Number of dropped Rx packets	get	get interface <interface_name> rx-drop-packets	WEP-2ac# get interface wlan1vap1 rx-drop-packets
	stp	Spanning Tree Protocol	add, get, set	add interface <interface_name> stp <value> get interface <interface_name> stp set interface <interface_name> stp <value>	

Class	Subclass	Feature	Possible commands	Syntax	Examples
	fd	Sending delay	add, get, set	add interface <interface_name> fd <value> get interface <interface_name> fd set interface <interface_name> fd <value>	
	hello	Hello interval	add, get, set	add interface <interface_name> hello <value> get interface <interface_name> hello set interface <interface_name> hello <value>	
	priority	Bridge priority	add, get, set	add interface <interface_name> priority <value> get interface <interface_name> priority set interface <interface_name> priority <value>	

Class	Subclass	Feature	Possible commands	Syntax	Examples
	port-isolation	Wireless ports isolation from each other	add, get, set	add interface <interface_name> port-isolation <value> get interface <interface_name> port-isolation set interface <interface_name> port-isolation <value>	
	ssid	Network name	add, get, set	add interface <interface_name> ssid <value> get interface <interface_name> ssid set interface <interface_name> ssid <value>	WEP-2ac# get interface wlan0vap1 ssid ___wep12_15-105
	bss	BSS to which interface belongs	add, get, set	add interface <interface_name> bss <value> get interface <interface_name> bss set interface <interface_name> bss <value>	WEP-2ac# get interface wlan1vap1 bss wlan1bssvap1

Class	Subclass	Feature	Possible commands	Syntax	Examples
	security	Security mode	add, get, set	add interface <interface_name> security <value> get interface <interface_name> security set interface <interface_name> security <value>	WEP-2ac# get interface wlan1vap1 security plain-text
	wpa-personal-key	Personal WPA key (shared use)	add, set	add interface <interface_name> wpa-personal-key <value> get interface <interface_name> wpa-personal-key set interface <interface_name> wpa-personal-key <value>	
	wep-key-ascii	WEP key format: ascii or hex	add, get, set	add interface <interface_name> wep-key-ascii <value> get interface <interface_name> wep-key-ascii set interface <interface_name> wep-key-ascii <value>	WEP-2ac# get interface wlan1vap1 wep-key-ascii no

Class	Subclass	Feature	Possible commands	Syntax	Examples
	wep-key-length	WEP key length	add, get, set	add interface <interface_name> wep-key-length <value> get interface <interface_name> wep-key-length set interface <interface_name> wep-key-length <value>	WEP-2ac# get interface wlan1vap1 wep-key-length 104
	wep-default-key	WEP key used for transmission	add, get, set	add interface <interface_name> wep-key-length <value> get interface <interface_name> wep-key-length set interface <interface_name> wep-key-length <value>	WEP-2ac# get interface wlan1vap1 wep-default-key 1
	wep-key-1	WEP key (1)	add, set	add interface <interface_name> wep-key-1 <value> get interface <interface_name> wep-key-1 set interface <interface_name> wep-key-1 <value>	

Class	Subclass	Feature	Possible commands	Syntax	Examples
	wep-key-2	WEP key (2)	add, get, set	add interface <interface_name> wep-key-2 <value> get interface <interface_name> wep-key-2 set interface <interface_name> wep-key-2 <value>	
	wep-key-3	WEP key (3)	add, get, set	add interface <interface_name> wep-key-3 <value> get interface <interface_name> wep-key-3 set interface <interface_name> wep-key-3 <value>	
	wep-key-4	WEP key (4)	add, get, set	add interface <interface_name> wep-key-4 <value> get interface <interface_name> wep-key-4 set interface <interface_name> wep-key-4 <value>	
	wep-key-mapping-length		get	get interface <interface_name> wep-key-mapping-length	WEP-2ac# get interface wlan1vap1 wep-key-mapping-length 400

Class	Subclass	Feature	Possible commands	Syntax	Examples
	multicast-received-frame-count	Number of received multicast frames	get	get interface <interface_name> multicast-received-frame-count	WEP-2ac# get interface wlan1vap1 multicast-received-frame-count
	vlan-id	ID used in tags	add, get	add interface <interface_name> vlan-id <value> get interface <interface_name> vlan-id	WEP-2ac# get interface wlan1vap1 vlan-id
	radio	Radio interface for WDS	add, get, set	add interface <interface_name> radio <value> get interface <interface_name> radio set interface <interface_name> radio <value>	WEP-2ac# get interface wlan1vap1 radio
	remote-mac	Endpoint MAC address of the WDS connection	add, get, set	add interface <interface_name> remote-mac <value> get interface <interface_name> remote-mac set interface <interface_name> remote-mac <value>	WEP-2ac# get interface wlan1vap1 remote-mac

Class	Subclass	Feature	Possible commands	Syntax	Examples
	wep-key	WEP key for WDS connection	add, get, set	add interface <interface_name> wep-key <value> get interface <interface_name> wep-key set interface <interface_name> wep-key <value>	WEP-2ac# get interface wlan1vap1 wep-key
	wds-ssid	WDS connection SSID	add, get, set	add interface <interface_name> wds-ssid <value> get interface <interface_name> wds-ssid set interface <interface_name> wds-ssid <value>	WEP-2ac# get interface wlan1vap1 wds-ssid
	wds-security-policy	WDS connection security policy	add, get, set	add interface <interface_name> wds-security-policy <value> get interface <interface_name> wds-security-policy set interface <interface_name> wds-security-policy <value>	WEP-2ac# get interface wlan1vap1 wds-security-policy

Class	Subclass	Feature	Possible commands	Syntax	Examples
	wds-wpa-psk-key	WPA PSK key for WDS connection	add, get, set	add interface <interface_name> wds-wpa-psk-key <value> get interface <interface_name> wds-wpa-psk-key set interface <interface_name> wds-wpa-psk-key <value>	WEP-2ac# get interface wlan1vap1 wds-wpa-psk-key
	interface	Management interface	get	get management interface	WEP-2ac# get management interface brtrunk
	static-ip	Management interface static IP address	get, set	get management static-ip set management static-ip <value>	WEP-2ac# set management static-ip "192.168.1.10" WEP-2ac# get management static-ip 192.168.1.10
	static-mask	Management interface static mask	get, set	get management static-mask set management static-mask <value>	WEP-2ac# set management static-mask "255.255.255.0" WEP-2ac# get management static-mask 255.255.255.0
	ip	Management interface IP address	get	get management ip	WEP-2ac# get management ip 192.168.15.105
	mask	Management interface IP address mask	get	get management mask	WEP-2ac# get management mask 255.255.255.0

Class	Subclass	Feature	Possible commands	Syntax	Examples
	mac	Management interface MAC address	get	get management mac	WEP-2ac# get management mac A8:F9:4B:B0:21:60
	dhcp-status	If DHCP on management interface is enabled or not	get	get management dhcp-status	WEP-2ac# get management dhcp-status up
vap Virtual access points settings	radio	Wireless access point radio interface	get, set	get vap <vap> radio set vap <vap> radio <value>	WEP-2ac# get vap vap1 radio radio ----- wlan0 wlan1
	status	Status	get, set	get vap <vap> status set vap <vap> status <value>	WEP-2ac# get vap vap1 status status ------ down down
	vlan-id	VLAN ID	add, get, set	add vap <vap> vlan-id <value> get vap <vap> vlan-id set vap <vap> vlan-id <value>	WEP-2ac# get vap vap1 vlan-id vlan-id ------- 1 1
	global-radius	Use of RADIUS global settings	get, set	get vap <vap> global radius set vap <vap> global radius <value>	
	description	Virtual access point description	get, set	get vap <vap> description set vap <vap> description <value>	WEP-2ac# get vap vap1 description description -------------------------------- Virtual Access Point 1 Virtual Access Point 1 - Radio 2

Class	Subclass	Feature	Possible commands	Syntax	Examples
	qos-mode	QoS administration mode	get, set	get vap <vap> qos-mode set vap <vap> qos-mode <value>	WEP-2ac# get vap vap1 qos-mode qos-mode -------- up up
	def-bwmax-up	Maximum upstream bandwidth by default (0-4294967295)	get, set	get vap <vap> def-bwmax-up set vap <vap> def-bwmax-up <value>	WEP-2ac# get vap vap1 def-bwmax-up def-bwmax-up ------------ 0 0
	def-bwmax-down	Maximum downstream bandwidth by default (0-4294967295)	get, set	get vap <vap> def-bwmax-down set vap <vap> def-bwmax-down <value>	WEP-2ac# get vap vap1 def-bwmax-down def-bwmax-down -------------- 0 0
	def-acltype-up	ACL type for outgoing connections by default (none/ipv4, Currently Unsupported:ipv6/mac)	get, set	get vap <vap> def-acltype-up set vap <vap> def-acltype-up <value>	
	def-acltype-down	ACL type for incoming connections by default (none/ipv4, Currently Unsupported:ipv6/mac)	get, set	get vap <vap> def-acltype-down set vap <vap> def-acltype-down <value>	WEP-2ac# get vap vap1 def-acltype-up def-acltype-up -------------- none none
	def-acl-up	ACL for outgoing connections by default	get, set	get vap <vap> def-acl-up set vap <vap> def-acl-up <value>	

Class	Subclass	Feature	Possible commands	Syntax	Examples
	def-acl-down	ACL for incoming connections by default	get, set	get vap <vap> def-acl-down set vap <vap> def-acl-down <value>	
	def-policy-up	Default Policy Up	get, set	get vap <vap> def-policy-up set vap <vap> def-policy-up <value>	
	def-policy-down	Default Policy Down	get, set	get vap <vap> def-policy-down set vap <vap> def-policy-down <value>	
global-radius-server RADUIS server global settings	radius-accounting	RADIUS Accounting activation	get, set	get global-radius-server radius-accounting set global-radius-server radius-accounting <value>	WEP-2ac# set global-radius-server radius-accounting off WEP-2ac# get global-radius-server radius-accounting off
	radius-ip	RADIUS server IP address	get, set	get global-radius-server radius-ip set global-radius-server radius-ip <value>	WEP-2ac# set global-radius-server radius-ip "192.168.1.1" WEP-2ac# get global-radius-server radius-ip 192.168.1.1

Class	Subclass	Feature	Possible commands	Syntax	Examples
	radius-ip-network	RADIUS server IP network	get, set	get global-radius-server radius-ip-network set global-radius-server radius-ip-network <value>	WEP-2ac# set global-radius-server radius-ip-network ipv4 WEP-2ac# get global-radius-server radius-ip-network ipv4
	radius-key	RADIUS server connection key	set	get global-radius-server radius-key set global-radius-server radius-key <value>	
	radius-nas-identifier	Optional NAS identifier for RADIUS client	get, set	get global-radius-server radius-nas-identifier set global-radius-server radius-nas-identifier <value>	
	description	Description	get, set	get global-radius-server description set global-radius-server description <value>	WEP-2ac# set global-radius-server description "Global radius server settings" WEP-2ac# get global-radius-server description Global radius server settings
dot11 IEEE 802.11 standards support	status	Status	get, set	get dot11 status set dot11 status <value>	WEP-2ac# set dot11 status up WEP-2ac# get dot11 status up

Class	Subclass	Feature	Possible commands	Syntax	Examples
radio Radio interfaces settings	status	Status	get, set	get radio <radio_interface_name> status set radio <radio_interface_name> status <value>	WEP-2ac# set radio wlan0 status up WEP-2ac# get radio wlan0 status up
	description	Description	get	get radio <radio_interface_name> description	WEP-2ac# get radio wlan0 description IEEE 802.11g
	mac	Radio interface MAC address (initial)	get	get radio <radio_interface_name> mac	WEP-2ac# get radio wlan1 mac A8:F9:4B:B0:21:70
	static-mac	Radio interface static MAC address (initial)	get	get radio <radio_interface_name> static-mac	WEP-2ac# get radio wlan0 static-mac
	max-bss	BSS/MAC addresses maximum number	get	get radio <radio_interface_name> max-bss	WEP-2ac# set radio wlan0 max-bss 16 WEP-2ac# get radio wlan0 max-bss 16
	channel-policy	Channel selection policy	get, set	get radio <radio_interface_name> channel-policy set radio <radio_interface_name> channel-policy <value>	WEP-2ac# set radio wlan0 channel-policy best WEP-2ac# get radio wlan0 channel-policy best

Class	Subclass	Feature	Possible commands	Syntax	Examples
	mode	Wireless interface mode	get, set	get radio <radio_interface_name> mode set radio <radio_interface_name> mode <value>	WEP-2ac# set radio wlan1 mode "a-n-ac" WEP-2ac# get radio wlan1 mode a-n-ac
	dot11h	IEEE 802.11h standard support	get, set	get radio <radio_interface_name> dot11h set radio <radio_interface_name> dot11h <value>	WEP-2ac# set radio wlan0 dot11h off WEP-2ac# get radio wlan0 dot11h off
	dot11d	IEEE 802.11d standard support	get, set	get radio <radio_interface_name> dot11d set radio <radio_interface_name> dot11d <value>	WEP-2ac# set radio wlan0 dot11d off WEP-2ac# get radio wlan0 dot11d off
	block-time	Time during which the channel will be blocked after detection by radar	get, set	get radio <radio_interface_name> block-time set radio <radio_interface_name> block-time <value>	WEP-2ac# set radio wlan1 block-time 31 WEP-2ac# get radio wlan1 block-time 31

Class	Subclass	Feature	Possible commands	Syntax	Examples
	quiet-duration	Quiet interval duration in TU	get, set	get radio <radio_interface_name> quiet-duration set radio <radio_interface_name> quiet-duration <value>	WEP-2ac# set radio wlan0 quiet-duration 0 WEP-2ac# get radio wlan0 quiet-duration 0
	quiet-period	Beacon interval between regular quiet intervals	get, set	get radio <radio_interface_name> quiet-period set radio <radio_interface_name> quiet-period <value>	WEP-2ac# set radio wlan1 quiet-period 0 WEP-2ac# get radio wlan1 quiet-period 0
	tx-mitigation	Transmit Power mitigation for stations	get, set	get radio <radio_interface_name> tx-mitigation set radio <radio_interface_name> tx-mitigation <value>	WEP-2ac# set radio wlan0 tx-mitigation 3 WEP-2ac# get radio wlan0 tx-mitigation 3
	static-channel	Channel to be used for a static channel policy (channel policy)	get, set	get radio <radio_interface_name> static-channel set radio <radio_interface_name> static-channel <value>	WEP-2ac# set radio wlan0 static-channel 1 WEP-2ac# get radio wlan0 static-channel 1

Class	Subclass	Feature	Possible commands	Syntax	Examples
	channel	Channel in use	get	get radio <radio_interface_name> channel	WEP-2ac# get radio wlan0 channel 11
	tx-power-dbm	Transmission power	get, set	get radio <radio_interface_name> tx-power-dbm set radio <radio_interface_name> tx-power-dbm <value>	WEP-2ac# set radio wlan0 tx-power-dbm 5 WEP-2ac# get radio wlan0 tx-power-dbm 5
	tx-power-dbm-max	Maximum transmission power	get	get radio <radio_interface_name> tx-power-dbm-max	WEP-2ac# get radio wlan0 tx-power-dbm-max 19
	tx-power-output	Last set power (Last est. power from wl_curpower)	get	get radio <radio_interface_name> tx-power-output	WEP-2ac# get radio wlan0 tx-power-output 5.00
	tpc	IEEE 802.11h TPC	get, set	get radio <radio_interface_name> tpc set radio <radio_interface_name> tpc <value>	WEP-2ac# set radio wlan0 tpc off WEP-2ac# get radio wlan0 tpc off
	atf	Airtime Fairness	get, set	get radio <radio_interface_name> atf set radio <radio_interface_name> atf <value>	WEP-2ac# set radio wlan1 atf on WEP-2ac# get radio wlan1 atf on

Class	Subclass	Feature	Possible commands	Syntax	Examples
	ampdu_atf_us	ampdu_atf_us	get, set	get radio <radio_interface_name> ampdu_atf_us set radio <radio_interface_name> ampdu_atf_us <value>	WEP-2ac# set radio wlan1 ampdu_atf_us 4000 WEP-2ac# get radio wlan1 ampdu_atf_us 4000
	ampdu_atf_min_us	ampdu_atf_min_us	get, set	get radio <radio_interface_name> ampdu_atf_min_us set radio <radio_interface_name> ampdu_atf_min_us <value>	WEP-2ac# set radio wlan1 ampdu_atf_min_us 1000 WEP-2ac# get radio wlan1 ampdu_atf_min_us 1000
	tx-chain	Antenna configuration	get, set	get radio <radio_interface_name> tx-chain set radio <radio_interface_name> tx-chain <value>	WEP-2ac# set radio wlan1 tx-chain 7 WEP-2ac# get radio wlan1 tx-chain 7
	antenna	Use antenna	get, set	get radio <radio_interface_name> antenna set radio <radio_interface_name> antenna <value>	

Class	Subclass	Feature	Possible commands	Syntax	Examples
	tx-rx-status	Receive and transmit status on the radio interface	get, set	get radio <radio_interface_name> tx-rx-status set radio <radio_interface_name> tx-rx-status <value>	WEP-2ac# set radio wlan0 tx-rx-status up WEP-2ac# get radio wlan0 tx-rx-status up
	beacon-interval	Beacon interval	get, set	get radio <radio_interface_name> beacon-interval set radio <radio_interface_name> beacon-interval <value>	WEP-2ac# set radio wlan0 beacon-interval 100 WEP-2ac# get radio wlan0 beacon-interval 100
	rts-threshold	Minimum packet size at which Request-To-Send will be used	get, set	get radio <radio_interface_name> rts-threshold set radio <radio_interface_name> rts-threshold <value>	WEP-2ac# set radio wlan0 rts-threshold 2347 WEP-2ac# get radio wlan0 rts-threshold 2347
	fragmentation-threshold	Minimum packet size at which frag mentation will be used	get, set	get radio <radio_interface_name> fragmentation-threshold set radio <radio_interface_name> fragmentation-threshold <value>	WEP-2ac# set radio wlan0 fragmentation-threshold 2346 WEP-2ac# get radio wlan0 fragmentation-threshold 2346

Class	Subclass	Feature	Possible commands	Syntax	Examples
	load-balance-no-association-utilization	Utilization required to prevent new associations	get, set	get radio <radio_interface_name> load-balance-no-association-utilization set radio <radio_interface_name> load-balance-no-association-utilization <value>	WEP-2ac# set radio wlan0 load-balance-no-association-utilization 0 WEP-2ac# get radio wlan0 load-balance-no-association-utilization 0
	ap-detection	Enable access points detection	get, set	get radio <radio_interface_name> ap-detection set radio <radio_interface_name> ap-detection <value>	WEP-2ac# set radio wlan0 ap-detection on WEP-2ac# get radio wlan0 ap-detection on
	sentry-mode	Enable sentry mode	get, set	get radio <radio_interface_name> sentry-mode set radio <radio_interface_name> sentry-mode <value>	WEP-2ac# set radio wlan0 sentry-mode off WEP-2ac# get radio wlan0 sentry-mode off
	dedicated-spectrum-mode	Enable Dedicated Spectrum mode	get, set	get radio <radio_interface_name> dedicated-spectrum-mode set radio <radio_interface_name> dedicated-spectrum-mode <value>	

Class	Subclass	Feature	Possible commands	Syntax	Examples
	channel-hopping	Channel hopping	get, set	get radio <radio_interface_name> channel-hopping set radio <radio_interface_name> channel-hopping <value>	WEP-2ac# set radio wlan0 channel-hopping on WEP-2ac# get radio wlan0 channel-hopping on
	passive-scan-mode	Scanning in one band or in both bands sentry mode	get, set	get radio <radio_interface_name> passive-scan-mode set radio <radio_interface_name> passive-scan-mode <value>	WEP-2ac# get radio wlan0 passive-scan-mode
	scan-leave-time	Scan intervals	get, set	get radio <radio_interface_name> scan-leave-time set radio <radio_interface_name> scan-leave-time <value>	WEP-2ac# get radio wlan0 scan-leave-time
	scan-duration	Duration of radio frequency scanning in the channel, in ms	get, set	get radio <radio_interface_name> scan-duration set radio <radio_interface_name> scan-duration <value>	WEP-2ac# get radio wlan0 scan-duration

Class	Subclass	Feature	Possible commands	Syntax	Examples
	limit-channel-selection	802.11a channel limit	get, set	get radio <radio_interface_name> limit-channel-selection set radio <radio_interface_name> limit-channel-selection <value>	WEP-2ac# get radio wlan0 limit-channel-selection
	data-snooping	Enable snooping	get, set	get radio <radio_interface_name> data-snooping set radio <radio_interface_name> data-snooping <value>	WEP-2ac# set radio wlan0 data-snooping off WEP-2ac# get radio wlan0 data-snooping off
	n-bandwidth	802.11n (20/40) channels bandwidth	get, set	get radio <radio_interface_name> n-bandwidth set radio <radio_interface_name> n-bandwidth <value>	WEP-2ac# set radio wlan0 n-bandwidth 20 WEP-2ac# get radio wlan0 n-bandwidth 20
	n-primary-channel	802.11n (lower/ upper) primary channel location	get, set	get radio <radio_interface_name> n-primary-channel set radio <radio_interface_name> n-primary-channel <value>	WEP-2ac# set radio wlan0 n-primary-channel lower WEP-2ac# get radio wlan0 n-primary-channel lower

Class	Subclass	Feature	Possible commands	Syntax	Examples
	protection	Protection mode for 802.11g and 802.11n (auto/off)	get, set	get radio <radio_interface_name> protection set radio <radio_interface_name> protection <value>	WEP-2ac# set radio wlan0 protection auto WEP-2ac# get radio wlan0 protection auto
	frequency	Frequency in use in MHz	get	get radio <radio_interface_name> frequency	WEP-2ac# get radio wlan0 frequency 2462
	wme	Enable WME	get, set	get radio <radio_interface_name> wme set radio <radio_interface_name> wme <value>	WEP-2ac# set radio wlan0 wme on WEP-2ac# get radio wlan0 wme on
	wme-noack	Enable WME 'No Acknowledgement'	get, set	get radio <radio_interface_name> wme-noack set radio <radio_interface_name> wme-noack <value>	WEP-2ac# set radio wlan0 wme-noack off WEP-2ac# get radio wlan0 wme-noack off
	wme-apsd	Enable WME APSD	get, set	get radio <radio_interface_name> wme-apsd set radio <radio_interface_name> wme-apsd <value>	WEP-2ac# set radio wlan0 wme-apsd on WEP-2ac# get radio wlan0 wme-apsd on

Class	Subclass	Feature	Possible commands	Syntax	Examples
	rate-limit-enable	Enable broadcast/multicast traffic limit	get, set	get radio <radio_interface_name> rate-limit-enable set radio <radio_interface_name> rate-limit-enable <value>	WEP-2ac# set radio wlan0 rate-limit-enable off WEP-2ac# get radio wlan0 rate-limit-enable off
	rate-limit	Broadcast/multicast traffic limit (packets per second)	get, set	get radio <radio_interface_name> rate-limit set radio <radio_interface_name> rate-limit <value>	WEP-2ac# set radio wlan0 rate-limit 50 WEP-2ac# get radio wlan0 rate-limit 50
	rate-limit-burst	Burst value for broadcast/multicast traffic (packets per second)	get, set	get radio <radio_interface_name> rate-limit-burst set radio <radio_interface_name> rate-limit-burst <value>	WEP-2ac# set radio wlan0 rate-limit-burst 75 WEP-2ac# get radio wlan0 rate-limit-burst 75
	stp-block-enable	Block all STP packets on radio interface	get, set	get radio <radio_interface_name> stp-block-enable set radio <radio_interface_name> stp-block-enable <value>	WEP-2ac# set radio wlan0 stp-block-enable on WEP-2ac# get radio wlan0 stp-block-enable on

Class	Subclass	Feature	Possible commands	Syntax	Examples
	wlan-util	Use wireless LAN	get	get radio <radio_interface_name> wlan-util	WEP-2ac# get radio wlan0 wlan-util 74
	fixed-multicast-rate	Fixed rate for Multicast traffic band	get, set	get radio <radio_interface_name> fixed-multicast-rate set radio <radio_interface_name> fixed-multicast-rate <value>	WEP-2ac# set radio wlan0 fixed-multicast-rate auto WEP-2ac# get radio wlan0 fixed-multicast-rate auto
	fixed-tx-modulation	Fixed modulation for band	get, set	get radio <radio_interface_name> fixed-tx-modulation set radio <radio_interface_name> fixed-tx-modulation <value>	WEP-2ac# set radio wlan0 fixed-tx-modulation auto WEP-2ac# get radio wlan0 fixed-tx-modulation auto
	antenna-diversity	Antenna diversity	get, set	get radio <radio_interface_name> antenna-diversity set radio <radio_interface_name> antenna-diversity <value>	

Class	Subclass	Feature	Possible commands	Syntax	Examples
	antenna-selection	Number of antenna in use	get, set	get radio <radio_interface_name> antenna-selection set radio <radio_interface_name> antenna-selection <value>	
bss Basic Service Set (BSS)	status	Status	add, get, set	add bss <bss_id> status <value> get bss <bss_id> status set bss <bss_id> status <value>	WEP-2ac# set bss wlan0bssvap1 status up WEP-2ac# get bss wlan0bssvap1 status up
	description	Description	get, set	get bss <bss_id> description set bss <bss_id> description <value>	WEP-2ac# set bss wlan0bssvap1 description Virtual Access Point 1 WEP-2ac# get bss wlan0bssvap1 description Virtual Access Point 1
	radio	Radio interface of this BSS	add, get, set	add bss <bss_id> radio <value> get bss <bss_id> radio set bss <bss_id> radio <value>	WEP-2ac# set bss wlan0bssvap1 radio wlan0 WEP-2ac# get bss wlan0bssvap1 radio wlan0

Class	Subclass	Feature	Possible commands	Syntax	Examples
	beacon-interface	BSS interface used for beacon	add, get, set	add bss <bss_id> beacon-interface <value> get bss <bss_id> beacon-interface set bss <bss_id> beacon-interface <value>	WEP-2ac# set bss wlan0bssvap1 beacon-interface wlan0vap1 WEP-2ac# get bss wlan0bssvap1 beacon-interface wlan0vap1
	mac	MAC address	add, get	add bss <bss_id> mac <value> get bss <bss_id> mac	WEP-2ac# get bss wlan0bssvap1 mac A8:F9:4B:B0:21:61
	dtim-period	DTIM interval	add, get, set	add bss <bss_id> dtim-period <value> get bss <bss_id> dtim-period set bss <bss_id> dtim-period <value>	
	max-stations	Maximum stations number	add, get, set	add bss <bss_id> max-stations <value> get bss <bss_id> max-stations set bss <bss_id> max-stations <value>	

Class	Subclass	Feature	Possible commands	Syntax	Examples
	ignore-broadcast-ssid	Do not send SSID to beacon and ignore test requests	add, get, set	add bss <bss_id> max-stations <value> get bss <bss_id> max-stations set bss <bss_id> max-stations <value>	WEP-2ac# set bss wlan0bssvap1 ignore-broadcast-ssid off WEP-2ac# get bss wlan0bssvap1 ignore-broadcast-ssid off
	station-isolation	Station isolation	add, get, set	add bss <bss_id> max-stations <value> get bss <bss_id> max-stations set bss <bss_id> max-stations <value>	WEP-2ac# set bss wlan0bssvap1 station-isolation off WEP-2ac# get bss wlan0bssvap1 station-isolation off
	tagged-sta-mode	Enable/ disable traffic tagging from/to STA	add, get, set	add bss <bss_id> tagged-sta-mode <value> get bss <bss_id> tagged-sta-mode set bss <bss_id> tagged-sta-mode <value>	WEP-2ac# set bss wlan0bssvap1 tagged-sta-mode off WEP-2ac# get bss wlan0bssvap1 tagged-sta-mode off

Class	Subclass	Feature	Possible commands	Syntax	Examples
	mac-acl-mode	MAC addresses list	add, get, set	add bss <bss_id> mac-acl-mode <value> get bss <bss_id> mac-acl-mode set bss <bss_id> mac-acl-mode <value>	WEP-2ac# set bss wlan0bssvap1 mac-acl-mode deny-list WEP-2ac# get bss wlan0bssvap1 mac-acl-mode deny-list
	mac-acl-name	MAC addresses list name	add, get, set	add bss <bss_id> mac-acl-name <value> get bss <bss_id> mac-acl-name set bss <bss_id> mac-acl-name <value>	WEP-2ac# set bss wlan0bssvap1 mac-acl-name default WEP-2ac# get bss wlan0bssvap1 mac-acl-name default
	mac-acl-auth-type	MAC addresses authentication type	add, get, set	add bss <bss_id> mac-acl-auth-type <value> get bss <bss_id> mac-acl-auth-type set bss <bss_id> mac-acl-auth-type <value>	WEP-2ac# set bss wlan0bssvap1 mac-acl-auth-type disable WEP-2ac# get bss wlan0bssvap1 mac-acl-auth-type disable

Class	Subclass	Feature	Possible commands	Syntax	Examples
	radius-accounting	Authorization on RADIUS servre	add, get, set	add bss <bss_id> radius-accounting <value> get bss <bss_id> radius-accounting set bss <bss_id> radius-accounting <value>	WEP-2ac# set bss wlan0bssvap1 radius-accounting on WEP-2ac# get bss wlan0bssvap1 radius-accounting on
	radius-ip	RADIUS server IP address	add, get, set	add bss <bss_id> radius-ip <value> get bss <bss_id> radius-ip set bss <bss_id> radius-ip <value>	WEP-2ac# set bss wlan0bssvap1 radius-ip "192.168.42.220" WEP-2ac# get bss wlan0bssvap1 radius-ip 192.168.42.220
	radius-ip-network	RADIUS server IP network	add, get, set	add bss <bss_id> radius-ip-network <value> get bss <bss_id> radius-ip-network set bss <bss_id> radius-ip-network <value>	WEP-2ac# set bss wlan0bssvap1 radius-ip-network ipv4 WEP-2ac# get bss wlan0bssvap1 radius-ip-network ipv4

Class	Subclass	Feature	Possible commands	Syntax	Examples
	radius-key	Key for connection with RADIUS server	add, set	add bss <bss_id> radius-key <value> get bss <bss_id> radius-key set bss <bss_id> radius-key <value>	
	radius-port	Port for authentication on RADIUS server	add, get, set	add bss <bss_id> radius-port <value> get bss <bss_id> radius-port set bss <bss_id> radius-port <value>	WEP-2ac# set bss wlan0bssvap1 radius-port 1812port WEP-2ac# get bss wlan0bssvap1 radius-port 1812port
	radius-accounting-port	Port for accounting on RADIUS server	add, get, set	add bss <bss_id> radius-accounting-port <value> get bss <bss_id> radius-accounting-port set bss <bss_id> radius-accounting-port <value>	WEP-2ac# set bss wlan0bssvap1 radius-accounting-port 1813 WEP-2ac# get bss wlan0bssvap1 radius-accounting-port 1813

Class	Subclass	Feature	Possible commands	Syntax	Examples
	vlan-tagged-interface	Add dynamic VLAN to interface	add, get, set	add bss <bss_id> vlan-tagged-interface <value> get bss <bss_id> vlan-tagged-interface set bss <bss_id> vlan-tagged-interface <value>	WEP-2ac# set bss wlan0bssvap1 vlan-tagged-interface brtrunk WEP-2ac# get bss wlan0bssvap1 vlan-tagged-interface brtrunk
	open-system-authentication	If Open System authentication is allowed	add, get, set	add bss <bss_id> open-system-authentication <value> get bss <bss_id> open-system-authentication set bss <bss_id> open-system-authentication <value>	WEP-2ac# set bss wlan0bssvap1 open-system-authentication on WEP-2ac# get bss wlan0bssvap1 open-system-authentication on
	shared-key-authentication	If Shared key authentication is allowed	add, get, set	add bss <bss_id> shared-key-authentication <value> get bss <bss_id> shared-key-authentication set bss <bss_id> open-system-authentication <value>	WEP-2ac# set bss wlan0bssvap1 shared-key-authentication off WEP-2ac# get bss wlan0bssvap1 shared-key-authentication off

Class	Subclass	Feature	Possible commands	Syntax	Examples
	wpa-cipher-tkip	Use TKIP as WPA encryption method	add, get, set	add bss <bss_id> wpa-cipher-tkip <value> get bss <bss_id> wpa-cipher-tkip set bss <bss_id> wpa-cipher-tkip <value>	WEP-2ac# set bss wlan0bssvap1 wpa-cipher-tkip on WEP-2ac# get bss wlan0bssvap1 wpa-cipher-tkip on
	wpa-cipher-ccmp	Use CCMP as WPA encryption method	add, get, set	add bss <bss_id> wpa-cipher-ccmp <value> get bss <bss_id> wpa-cipher-ccmp set bss <bss_id> wpa-cipher-ccmp <value>	WEP-2ac# set bss wlan0bssvap1 wpa-cipher-ccmp on WEP-2ac# get bss wlan0bssvap1 wpa-cipher-ccmp on
	wpa-allowed	Allow WPA	add, get, set	add bss <bss_id> wpa-allowed <value> get bss <bss_id> wpa-allowed set bss <bss_id> wpa-allowed <value>	WEP-2ac# set bss wlan0bssvap1 wpa-allowed on WEP-2ac# get bss wlan0bssvap1 wpa-allowed on

Class	Subclass	Feature	Possible commands	Syntax	Examples
	wpa2-allowed	Allow WPA2	add, get, set	add bss <bss_id> wpa2-allowed <value> get bss <bss_id> wpa2-allowed set bss <bss_id> wpa2-allowed <value>	WEP-2ac# set bss wlan0bssvap1 wpa2-allowed on WEP-2ac# get bss wlan0bssvap1 wpa2-allowed on
	rsn-preauthentication	Allow RSN pre-authentication	add, get, set	add bss <bss_id> rsn-preauthentication <value> get bss <bss_id> rsn-preauthentication set bss <bss_id> rsn-preauthentication <value>	WEP-2ac# set bss wlan0bssvap1 rsn-preauthentication off WEP-2ac# get bss wlan0bssvap1 rsn-preauthentication off
	broadcast-key-refresh-rate	Set interval after which user access passwords are changed (broadcasting key)	add, get, set	add bss <bss_id> rsn-preauthentication <value> get bss <bss_id> rsn-preauthentication set bss <bss_id> rsn-preauthentication <value>	WEP-2ac# set bss wlan0bssvap1 broadcast-key-refresh-rate 0 WEP-2ac# get bss wlan0bssvap1 broadcast-key-refresh-rate 0

Class	Subclass	Feature	Possible commands	Syntax	Examples
	check-signal-timeout	Timeout check min signal (sec)	add, get, set	add bss <bss_id> check-signal-timeout <value> get bss <bss_id> check-signal-timeout set bss <bss_id> check-signal-timeout <value>	WEP-2ac# set bss wlan0bssvap1 check-signal-timeout 10 WEP-2ac# get bss wlan0bssvap1 check-signal-timeout 10
	wlan-util	Use wireless LAN	add, get, set	add bss <bss_id> wlan-util <value> get bss <bss_id> wlan-util set bss <bss_id> wlan-util <value>	
	fixed-multicast-rate	Fixed band rate for Multicast traffic	add, get, set	add bss <bss_id> fixed-multicast-rate <value> get bss <bss_id> fixed-multicast-rate set bss <bss_id> fixed-multicast-rate <value>	

Class	Subclass	Feature	Possible commands	Syntax	Examples
`bridge-port` Bridge port	Enter the 'get bridge-port' command and get all bridge interface characteristics available for viewing or use commands listed below				

	`interface`	Bridge interface	add, get	`add bridge-port <all|brtrunk> interface <value>`
				
				`get bridge-port <all|brtrunk> interface`
					`WEP-2ac# get bridge-port brtrunk interface`
					`interface`
					`---------`
					`eth0`
					`wlan0wds0`
					`wlan0wds1`
					`wlan0wds2`
					`wlan0wds3`
					`wlan0wds4`
					`wlan0wds5`
					`wlan0wds6`
					`wlan0wds7`
					`wlan0`
					`wlan0vap1`
					`wlan0vap2`

	`path-cost`	Interface cost	add, get, set	`add bridge-port <all|brtrunk> path-cost <value>`
				
				`get bridge-port <all|brtrunk> path-cost`
				
				`set bridge-port <all|brtrunk> path-cost <value>`	

Class	Subclass	Feature	Possible commands	Syntax	Examples
	priority	Port priority	add, get, set	add bridge-port <all|brtrunk> priority <value> get bridge-port <all|brtrunk> priority set bridge-port <all|brtrunk> priority <value>	
	stp-state	Spanning tree state	get	get bridge-port <all|brtrunk> stp-state	WEP-2ac# get bridge-port brtrunk stp-state stp-state ---------- forwarding forwarding forwarding forwarding forwarding forwarding forwarding
mac-acl MAC addresses table elements	mac	Allow/deny MAC address	add, get, set	add mac-acl <value> get mac-acl set mac-acl <value>	
tx-queue Queue parameters transmission	Enter the 'get tx-queue <interface_name|all>' command and get all bridge interface characteristics available for viewing or use commands listed below			get tx-queue <interface_name|all>	WEP-2ac# get tx-queue all name queue aifs cwmin cwmax burst ---------- ---------- wlan0 data0 1 3 7 1.5 wlan0 data1 1 7 15 3.0 wlan0 data2 3 15 63 0 wlan0 data3 7 15 1023 0 wlan1 data0 1 3 7 1.5 wlan1 data1 1 7 15 3.0 wlan1 data2 3 15 63 0 wlan1 data3 7 15 1023 0

Class	Subclass	Feature	Possible commands	Syntax	Examples
	queue	Queue name	get	get tx-queue <interface_name|all> queue	WEP-2ac# get tx-queue all queue name queue ------------ wlan0 data0 wlan0 data1 wlan0 data2 wlan0 data3 wlan1 data0 wlan1 data1 wlan1 data2 wlan1 data3
	aifs	Adaptive Interframe Spacing	get, set	get tx-queue <interface_name|all> aifs set tx-queue <interface_name|all> aifs <value>	WEP-2ac# get tx-queue wlan0 aifs aifs ---- 1 1 3 7
	cwmin	Concurrent window minimal value	get, set	get tx-queue <interface_name|all> cwmin set tx-queue <interface_name|all> cwmin <value>	WEP-2ac# get tx-queue wlan0 cwmin cwmin ----- 3 7 15 15
	cwmax	Concurrent window maximum value	get, set	get tx-queue <interface_name|all> cwmax set tx-queue <interface_name|all> cwmax <value>	WEP-2ac# get tx-queue wlan0 cwmax cwmax ----- 7 15 63 1023

Class	Subclass	Feature	Possible commands	Syntax	Examples
	burst	Maximum queue length	get, set	get tx-queue <interface_name|all> burst set tx-queue <interface_name|all> burst <value>	WEP-2ac# get tx-queue wlan0 burst burst ----- 1.5 3.0 0 0
wme-queue Queue parameters transmission to stations	Enter the 'get wme-queue <interface_name|all>' xommand and get all bridge interface characteristics available for viewing or use commands listed below			get wme-queue <interface_name|all>	WEP-2ac# get wme-queue all name queue aifs cwmin cwmax txop-limit ---------- wlan0 vo 2 3 7 47 wlan0 vi 2 7 15 94 wlan0 be 3 15 1023 0 wlan0 bk 7 15 1023 0 wlan1 vo 2 3 7 47 wlan1 vi 2 7 15 94 wlan1 be 3 15 1023 0 wlan1 bk 7 15 1023 0
	queue	Queue name	get	get wme-queue <interface_name|all> queue	WEP-2ac# get wme-queue all queue name queue ------------ wlan0 vo wlan0 vi wlan0 be wlan0 bk wlan1 vo wlan1 vi wlan1 be wlan1 bk
	aifs	Adaptive Interframe Spacing	get, set	get wme-queue <interface_name|all> aifs get wme-queue <interface_name|all> aifs <value>	WEP-2ac# get wme-queue wlan0 aifs aifs ---- 2 2 3 7

Class	Subclass	Feature	Possible commands	Syntax	Examples
	cwmin	Concurrent window minimal value	get, set	get wme-queue <interface_name|all> cwmin get wme-queue <interface_name|all> cwmin <value>	WEP-2ac# get wme-queue wlan0 cwmin cwmin ----- 3 7 15 15
	cwmax	Concurrent window maximum value	get, set	get wme-queue <interface_name|all> cwmax get wme-queue <interface_name|all> cwmax <value>	WEP-2ac# get wme-queue wlan0 cwmax cwmax ----- 7 15 1023 1023
	burst	Maximum queue length	get, set		
	txop-limit	Transmission limit	get, set	get wme-queue <interface_name|all> txop-limit set wme-queue <interface_name|all> txop-limit <value>	WEP-2ac# get wme-queue wlan0 txop-limit txop-limit ---------- 47 94 0 0
static-ip-route Static IP route entry	destination	Destination IP address prefix	get	get static-ip-route destination	WEP-2ac# get static-ip-route destination 0.0.0.0
	mask	Subnet mask	get	get static-ip-route mask	WEP-2ac# get static-ip-route mask 0.0.0.0
	gateway	Route IP address	get	get static-ip-route gateway	WEP-2ac# get static-ip-route gateway 192.168.1.254

Class	Subclass	Feature	Possible commands	Syntax	Examples
	table	Number in routing table	get	get static-ip-route table	WEP-2ac# get static-ip-route table 254
ip-route IP route entry	destination	Destination IP address prefix	get	get ip-route destination	WEP-2ac# get ip-route destination 0.0.0.0
	mask	Subnet mask	get	get ip-route mask	WEP-2ac# get ip-route mask 0.0.0.0
	gateway	Route IP address	get	get ip-route gateway	WEP-2ac# get ip-route gateway 192.168.15.1
	table	Number in routing table	get	get ip-route table	WEP-2ac# get ip-route table 254
log Logging configuration	depth	Number of entries that can be logged	get, set	get log depth set log depth <value>	WEP-2ac# set log depth 512 WEP-2ac# get log depth 512
	persistence	Save log to non-volatile memory	get, set	get log persistence set log persistence <value>	WEP-2ac# set log persistence no WEP-2ac# get log persistence no
	severity	Set severity level of a saved entry	get, set	get log severity set log severity <value>	WEP-2ac# set log severity 7 WEP-2ac# get log severity 7
	remove	Delete all entries in log	set	set log remove	

Class	Subclass	Feature	Possible commands	Syntax	Examples
	relay-enabled	Activate system log (syslog) transmission	get, set	get log relay-enabled set log relay-enabled <value>	WEP-2ac# set log relay-enabled 0 WEP-2ac# get log relay-enabled 0
	relay-host	Host to send syslog to	get, set	get log relay-host set log relay-host <value>	
	relay-port	Port to send syslog to	get, set	get log relay-port set log relay-port <value>	WEP-2ac# set log relay-port 514 WEP-2ac# get log relay-port 514
log-entry Log entry	number	Entry number	get	get log-entry number	WEP-2ac# get log-entry number number ------ 1 2 3 4 5
	priority	Entry priority	get	get log-entry priority	WEP-2ac# get log-entry priority priority -------- err info info err err info
	time	Entry time	get	get log-entry time	WEP-2ac# get log-entry time time -------------------- Oct 11 2018 00:00:19 Oct 11 2018 00:00:18 Oct 11 2018 00:00:16 Oct 11 2018 00:00:12

Class	Subclass	Feature	Possible commands	Syntax	Examples
	daemon	Daemon	get	get log-entry daemon	WEP-2ac# get log-entry daemon daemon ------------- dnsd[28523] dman[1239] dman[1239] dnsd[28410] dnsd[18233]
	message	Message	get	get log-entry message	WEP-2ac# get log-entry message Property Value ----------------------------------- --------- message accepting UDP packets on 0.0.0.0:4553
association Associated stations	interface	Station interface is associated with	get	get association interface	
	station	Station MAC address	get	get association station	
	authenticated	If authentication passed	get	get association authenticated	
	associated	Associated	get	get association associated	
	rx-packets	Received from station (packets)	get	get association rx-packets	
	tx-packets	Transmitted to station (packets)	get	get association tx-packets	
	rx-bytes	Received from station (bytes)	get	get association rx-bytes	

Class	Subclass	Feature	Possible commands	Syntax	Examples
	tx-bytes	Transmitted to station (bytes)	get	get association tx-bytes	
	tx-rate	Transmission rate	get	get association tx-rate	
	rx-rate	Reception rate	get	get association rx-rate	
	listen-interval	Listen interval	get	get association listen-interval	
	last-rssi	RSSI received in the last frame	get	get association last-rssi	
	tx-drop-bytes	Number of bytes dropped during transmission to the station	get	get association tx-drop-bytes	
	rx-drop-bytes	Number of bytes dropped during reception from the station	get	get association rx-drop-bytes	
	tx-drop-packets	Number of packets dropped during transmission to the station	get	get association tx-drop-packets	

Class	Subclass	Feature	Possible commands	Syntax	Examples
	rx-drop-packets	Number of packets dropped during reception from the station	get	get association rx-drop-packets	
basic-rate Basic radio interface rates	rate	Rate 0.5 Mbps	add, get, remove	add basic-rate <interface_id |all> rate <value> get basic-rate <interface_id |all> rate remove basic-rate <interface_id |all> rate <value>	WEP-2ac# get basic-rate all rate name rate ----------- wlan1 24 wlan1 12 wlan1 6 wlan0 11 wlan0 5.5 wlan0 2 wlan0 1
supported-rate Supported radio interface rates	rate	Rate 0.5 Mbps	add, get, remove	add supported-rate <interface_id |all> rate <value> get supported-rate <interface_id |all> rate remove supported-rate <interface_id |all> rate <value>	WEP-2ac# get supported-rate wlan0 rate rate ---- 54 48 36 24 18 12 11 9 6 5.5 2 1
detected-ap Access points detection	mac	MAC address	get	get detected-ap mac	
	radio	Radio interface in use	get	get detected-ap radio	

Class	Subclass	Feature	Possible commands	Syntax	Examples
	beacon-interval	Beacon interval	get	get detected-ap beacon-interval	
	capability	IEEE 802.11 capabilities	get	get detected-ap capability	
	type	Type (AP, Ad hoc, or Other)	get	get detected-ap type	
	privacy	WEP or WPA enabled	get	get detected-ap privacy	
	ssid	Network	get	get detected-ap ssid	
	wpa	WPA security	get	get detected-ap wpa	
	phy-type	PHY mode detection	get	get detected-ap phy-type	
	band	Frequency band	get	get detected-ap band	
	channel	Channel	get	get detected-ap channel	
	rate	Rate	get	get detected-ap rate	
	signal	Signal power	get	get detected-ap signal	
	erp	ERP	get	get detected-ap erp	
	beacons	Number received beacons	get	get detected-ap beacons	

Class	Subclass	Feature	Possible commands	Syntax	Examples
	last-beacon	Last beacon reception time	get	get detected-ap last-beacon	
	supported-rates	List of supported rates	get	get detected-ap supported-rates	
	security	Security	get	get detected-ap security	
	hi-rate	Highest possible supported rate	get	get detected-ap hi-rate	
	noise	Noise level	get	get detected-ap noise	
	nmode	802.11n support	get	get detected-ap nmode	
	wired	Access point is connected to the wired network	get	get detected-ap wired	
	wds	Access point is a part of WDS network	get	get detected-ap wds	
	rssi	Access point's RSSI	get	get detected-ap rssi	
portal Captive portal settings	status	Administrative status	get, set	get portal status	

Class	Subclass	Feature	Possible commands	Syntax	Examples
	welcome-screen	If guest screen is displayed	get, set	get portal welcome-screen set portal welcome-screen <value>	
	welcome-screen-text	Text displayed in the welcome screen	get, set	get portal welcome-screen-text set portal welcome-screen-text <value>	
snmpv1 Access via SNMPv1 and SNMPv2 protocol	status	Administrative status	get, set	get snmpv1 status set snmpv1 status <value>	
snmp-view SNMP MIB view	type	OID subtree type (included or excluded)	add, get, set	add snmp-view <view-all|view-none|all> type <value> get snmp-view <view-all|view-none|all> type set snmp-view <view-all|view-none|all> type <value>	WEP-2ac# get snmp-view all type name type -------------------- view-all included view-none excluded

Class	Subclass	Feature	Possible commands	Syntax	Examples
	oid	OID subtree (string)	add, get, set	add snmp-view <view-all|view-none|all> oid <value> get snmp-view <view-all|view-none|all> oid set snmp-view <view-all|view-none|all> oid <value>	WEP-2ac# get snmp-view all oid name type ---------- view-all included view-none excluded
	mask	OID mask – list of octets in hex format separated by the '.' character Leave an empty string if the mask is not required	add, get, set	add snmp-view <view-all|view-none|all> mask <value> get snmp-view <view-all|view-none|all> mask set snmp-view <view-all|view-none|all> mask <value>	WEP-2ac# get snmp-view all mask name mask ---------- view-all view-none
snmp-group SNMP users group	secur-level	Security level (noAuthNoPriv, authNoPriv or authPriv)	add, get, set	add snmp-group <RO|RW|all> secur-level <value> get snmp-group <RO|RW|all> secur-level set snmp-group <RO|RW|all> secur-level <value>	WEP-2ac# set snmp-group RO secur-level authPriv WEP-2ac# get snmp-group RO secur-level authPriv

Class	Subclass	Feature	Possible commands	Syntax	Examples
	write-view	SNMP name for write access	add, get, set	add snmp-group <RO|RW|all> write-view <value> get snmp-group <RO|RW|all> write-view set snmp-group <RO|RW|all> write-view <value>	WEP-2ac# set snmp-group RO write-view view-none WEP-2ac# get snmp-group RO write-view view-none
	read-view	SNMP name for read access	add, get, set	add snmp-group <RO|RW|all> read-view <value> get snmp-group <RO|RW|all> read-view set snmp-group <RO|RW|all> read-view <value>	WEP-2ac# set snmp-group RO read-view view-all WEP-2ac# get snmp-group RO read-view view-all
snmp-user SNMPv3 users	group	SNMP group name	add, get, set	add snmp-user group <value> get snmp-user group set snmp-user group <value>	
	auth-type	protocol ('md5' or 'none')	add, get, set	add snmp-user auth-type <value> get snmp-user auth-type set snmp-user auth-type <value>	

Class	Subclass	Feature	Possible commands	Syntax	Examples
	auth-pass	Authentication password	add, get, set	add snmp-user auth-pass <value> get snmp-user auth-pass set snmp-user auth-pass <value>	
	priv-type	Set encryption type ('des' – use DES encryption type, 'none' – do not use encyption)	add, get, set	add snmp-user priv-type <value> get snmp-user priv-type set snmp-user priv-type <value>	
	priv-pass	Encryption key	add, get, set	add snmp-user priv-pass <value> get snmp-user priv-pass set snmp-user priv-pass <value>	
snmp-target SNMPv3 targets for receiving SNMP traps	host	IP address to which SNMP traps will be sent	add, get, set	add snmp-target host <value> get snmp-target host set snmp-target host <value>	

Class	Subclass	Feature	Possible commands	Syntax	Examples
	port	Port number to which SNMP traps will be sent	add, get, set	add snmp-target port <value> get snmp-target port set snmp-target port <value>	
	user-name	SNMPv3 user name	add, get, set	add snmp-target user-name <value> get snmp-target user-name set snmp-target user-name <value>	
serial Serial access to CLI	status	Status	get, set	get serial status set serial status <value>	WEP-2ac# set serial status up WEP-2ac# get serial status up
	baud-rate	Data transmission rate (serial baud rate)	get, set	get serial baud-rate set serial baud-rate <value>	WEP-2ac# set serial baud-rate 115200 WEP-2ac# get serial baud-rate 115200
telnet Access to CLI via Telnet	status	Status	get, set	get telnet status set telnet status <value>	WEP-2ac# set telnet status up WEP-2ac# get telnet status up
ftp-server FTP server	status	Status	get, set	get ftp-server status set ftp-server status <value>	WEP-2ac# set ftp-server status down WEP-2ac# get ftp-server status down

Class	Subclass	Feature	Possible commands	Syntax	Examples

`firmware-upgrade`
 	
Access point firmware update via HTTP
	`upgrade-url`	http://<server IP>[:<server port>]/filename	get, set	`get firmware-upgrade upgrade-url`
				
				`set firmware-upgrade upgrade-url <value>`
					`WEP-2ac# get firmware-upgrade upgrade-url`

	`progress`	Display firmware update process status	get	`get firmware-upgrade progress`	`WEP-2ac# get firmware-upgrade progress`
	`validate`	Set 'yes' to confirm file	set	`set firmware-upgrade validate`	
	`start`	Set 'yes' to start firmware update	set	`set firmware-upgrade start`	

`untagged-vlan`
 	
Untagged VLAN configuration
	`vlan-id`	VLAN ID to use untagged VLANs	get, set	`get untagged-vlan vlan-id`
				
				`set untagged-vlan vlan-id <value>`
					`WEP-2ac# set untagged-vlan vlan-id 1`
					
					`WEP-2ac# get untagged-vlan vlan-id 1`

	`status`	Status	get, set	`get untagged-vlan status`
				
				`set untagged-vlan status <value>`
					`WEP-2ac# set untagged-vlan status up`
					
					`WEP-2ac# get untagged-vlan status up`

`managed-ap`
 	
Managed access point
	`mode`	Mode	get, set	`get managed-ap mode`
				
				`set managed-ap mode <value>`
					`WEP-2ac# set managed-ap mode down`
					
					`WEP-2ac# get managed-ap mode down`

Class	Subclass	Feature	Possible commands	Syntax	Examples
	ap-state	Access point state	get	get managed-ap ap-state	WEP-2ac# set managed-ap ap-state down WEP-2ac# get managed-ap ap-state down
	switch-address-1	Switch IP address 1	get, set	get managed-ap switch-address-1 set managed-ap switch-address-1 <value>	WEP-2ac# get managed-ap switch-address-1
	switch-address-2	Switch IP address 2	get, set	get managed-ap switch-address-2 set managed-ap switch-address-2 <value>	
	switch-address-3	Switch IP address 3	get, set	get managed-ap switch-address-3 set managed-ap switch-address-3 <value>	
	switch-address-4	Switch IP address 4	get, set	get managed-ap switch-address-4 set managed-ap switch-address-4 <value>	
	pass-phrase	Switch password	set	set managed-ap pass-phrase <value>	

Class	Subclass	Feature	Possible commands	Syntax	Examples
	dhcp-switch-address-1	DHCP witch IP address 1	get	get managed-ap dhcp-switch-address-1	WEP-2ac# get managed-ap dhcp-switch-address-1 104.116.116.112.58.47.47.49.57.50.46. 49.54.56.46.49.54.46.49.54.48.58.57. 53.57.53
	dhcp-switch-address-2	DHCP witch IP address 2	get	get managed-ap dhcp-switch-address-2	WEP-2ac# get managed-ap dhcp-switch-address-2 2
	dhcp-switch-address-3	DHCP witch IP address 3	get	get managed-ap dhcp-switch-address-3	WEP-2ac# get managed-ap dhcp-switch-address-3
	dhcp-switch-address-4	DHCP witch IP address 4	get	get managed-ap dhcp-switch-address-4	WEP-2ac# get managed-ap dhcp-switch-address-4
	managed-mode-watchdog	ime after which the watchdog will reboot the system if necessary (in minutes) (0-1440)	get, set	get managed-ap managed-mode-watchdog set managed-ap managed-mode-watchdog <value>	WEP-2ac# set managed-ap managed-mode-watchdog 0 WEP-2ac# get managed-ap managed-mode-watchdog 0
	dhcp-ip-base-port	DHCP Base IP port	get, set	get managed-ap dhcp-ip-base-port set managed-ap dhcp-ip-base-port <value>	WEP-2ac# get managed-ap dhcp-ip-base-port
	cfg-ip-base-port	Configure Base IP port (1-65000)	get, set	get managed-ap cfg-ip-base-port set managed-ap cfg-ip-base-port <value>	WEP-2ac# set managed-ap cfg-ip-base-port 57775 WEP-2ac# get managed-ap cfg-ip-base-port 57775

Class	Subclass	Feature	Possible commands	Syntax	Examples
	ip-base-port	Base IP port	get, set	get managed-ap ip-base-port set managed-ap ip-base-port <value>	WEP-2ac# set managed-ap ip-base-port 25459 WEP-2ac# get managed-ap ip-base-port 25459
	ip-tnl-udp-port	Tunnel UDP IP port	get, set	get managed-ap ip-tnl-udp-port set managed-ap ip-tnl-udp-port <value>	WEP-2ac# set managed-ap ip-tnl-udp-port 25459 WEP-2ac# get managed-ap ip-tnl-udp-port 25459
	ip-udp-port	UDP IP port	get, set	get managed-ap ip-udp-port set managed-ap ip-udp-port <value>	WEP-2ac# set managed-ap ip-udp-port 25460 WEP-2ac# get managed-ap ip-udp-port 25460
	ip-ssl-port	Secure SSL IP port	get, set	get managed-ap ip-ssl-port set managed-ap ip-ssl-port <value>	WEP-2ac# set managed-ap ip-ssl-port 25461 WEP-2ac# get managed-ap ip-ssl-port 25461
	ip-capwap-src-port	CAPWAP Src IP port	get, set	get managed-ap ip-capwap-src-port set managed-ap ip-capwap-src-port <value>	WEP-2ac# set managed-ap ip-capwap-src-port 25462 WEP-2ac# get managed-ap ip-capwap-src-port 25462
	ip-capwap-dst-port	CAPWAP Dst IP port	get, set	get managed-ap ip-capwap-dst-port set managed-ap ip-capwap-dst-port <value>	WEP-2ac# set managed-ap ip-capwap-dst-port 25463 WEP-2ac# get managed-ap ip-capwap-dst-port 25463

Class	Subclass	Feature	Possible commands	Syntax	Examples
dot1x-supplicant 802.1X supplicant	status	Status	get, set	get dot1x-supplicant status set dot1x-supplicant status <value>	WEP-2ac# set dot1x-supplicant status down WEP-2ac# get dot1x-supplicant status down
	user	802.1X supplicant user	get, set	get dot1x-supplicant user set dot1x-supplicant user <value>	WEP-2ac# get dot1x-supplicant user
	password	802.1X user password	set	set dot1x-supplicant password <value>	
mgmt-acl List of addresses allowed for management	mode	Mode	get, set	get mgmt-acl mode set mgmt-acl mode <value>	WEP-2ac# set mgmt-acl mode down WEP-2ac# get mgmt-acl mode down
	mgmt-address-1	Management IP address 1	get, set	get mgmt-acl mgmt-address-1 set mgmt-acl mgmt-address-1 <value>	WEP-2ac# get mgmt-acl mgmt-address-1
	mgmt-address-2	Management IP address 2	get, set	get mgmt-acl mgmt-address-2 set mgmt-acl mgmt-address-2 <value>	WEP-2ac# get mgmt-acl mgmt-address-2

Class	Subclass	Feature	Possible commands	Syntax	Examples
	mgmt-address-3	Management IP address 3	get, set	get mgmt-acl mgmt-address-3 set mgmt-acl mgmt-address-3 <value>	WEP-2ac# get mgmt-acl mgmt-address-3
	mgmt-address-4	Management IP address 4	get, set	get mgmt-acl mgmt-address-4 set mgmt-acl mgmt-address-4 <value>	WEP-2ac# get mgmt-acl mgmt-address-4
	mgmt-address-5	Management IP address 5	get, set	get mgmt-acl mgmt-address-5 set mgmt-acl mgmt-address-5 <value>	WEP-2ac# get mgmt-acl mgmt-address-5
cluster Cluster settings	clustered	Enable/ disable cluster mode for this node	get, set	get cluster clustered set cluster clustered <value>	WEP-2ac# get cluster clustered softwlc WEP-2ac# set cluster clustered 0
	location	Cluster location	get, set	get cluster location set cluster location <value>	WEP-2ac# set cluster location Moscow WEP-2ac# get cluster location Moscow
	cluster-name	Cluster name to connect	get, set	get cluster cluster-name set cluster cluster-name <value>	WEP-2ac# set cluster cluster-name root WEP-2ac# get cluster cluster-name root

Class	Subclass	Feature	Possible commands	Syntax	Examples
	ipversion	Select IP version: IPv4 or IPv6	add, get, set	add cluster ipversion <value> get cluster ipversion set cluster ipversion <value>	WEP-2ac# set cluster ipversion ipv4 WEP-2ac# get cluster ipversion ipv4
	member-count	Number of devices in cluster	get	get cluster member-count	WEP-2ac# get cluster member-count 2
	clustering-allowed	If cluster mode is allowed for this node	get	get cluster clustering-allowed	WEP-2ac# get cluster clustering-allowed true
	compat	Model of the device in the cluster	get	get cluster compat	WEP-2ac# get cluster compat WEP-2ac
	operational-mode	Operating mode	get	get cluster operational-mode	WEP-2ac# get cluster operational-mode 1
	cluster-ipaddr	IP address of the device managing the cluster	get, set	get cluster cluster-ipaddr set cluster cluster-ipaddr <value>	WEP-2ac# set cluster cluster-ipaddr 192.168.1.1 WEP-2ac# get cluster cluster-ipaddr 192.168.1.1
	priority	Priority	get, set	get cluster priority set cluster priority <value>	WEP-2ac# set cluster priority 1 WEP-2ac# get cluster priority 1

Class	Subclass	Feature	Possible commands	Syntax	Examples
	reauth-timeout	Time interval until re-authenticati on	get, set	get cluster reauth-timeout set cluster reauth-timeout <value>	WEP-2ac# set cluster reauth-timeout 300 WEP-2ac# get cluster reauth-timeout 300
	secure-mode	Secure ass ociation mode	get, set	get cluster secure-mode set cluster secure-mode <value>	WEP-2ac# set cluster secure-mode 1 WEP-2ac# get cluster secure-mode 1
	pass-set	Parameter 1 value if password is set	get	get cluster pass-set	WEP-2ac# get cluster pass-set
	secure-mode-status	Secure mode operation state	get	get cluster secure-mode-status	WEP-2ac# get cluster secure-mode-status Disabled

Class	Subclass	Feature	Possible commands	Syntax	Examples
cluster-member Cluster devices statuses	mac	MAC address of the device in the cluster	get	get cluster-member mac	WEP-2ac# get cluster-member mac E0:D9:E3:50:06:C0 A8:F9:4B:B5:FB:A0
	ip	IP address of the device in the cluster	get	get cluster-member ip	WEP-2ac# get cluster-member ip 100.110.0.200 100.110.0.249
	compat	Model of the device in the cluster	get	get cluster-member compat	WEP-2ac# get cluster-member compat WEP-2ac WEP-2ac
	location	Device location	get	get cluster-member location	WEP-2ac# get cluster-member location Moscow Moscow
	uptime	Uptime since boot	get	get cluster-member uptime	WEP-2ac# get cluster-member uptime 2923 1260
	is-dominant	Dominant device	get	get cluster-member is-dominant	WEP-2ac# get cluster-member is-dominant true false
	priority	Priority	get	get cluster-member priority	WEP-2ac# get cluster-member priority 0 0
	firmware-version	Firmware version	get	get cluster-member firmware-version	WEP-2ac# get cluster-member firmware-version 1.21.1.14

Class	Subclass	Feature	Possible commands	Syntax	Examples
	cluster-controller	Cluster controller	get	get cluster-member cluster-controller	WEP-2ac# get cluster-member cluster-controller no yes
cluster-fw-member Cluster devices firmware download statuses	ip	IP address of the device in the cluster	get	get cluster-fw-member ip	
	mac	MAC address of the device in the cluster	get	get cluster-fw-member mac	
	fw-download-status	Firmware download status	get	get cluster-fw-member fw-download-status	
cluster-firmware-upgrade Cluster settings	upgrade	Start/stop uploading	get, set	get cluster-firmware-upgrade upgrade set cluster-firmware-upgrade upgrade <value>	WEP-2ac# set cluster-firmware-upgrade upgrade Start WEP-2ac# get cluster-firmware-upgrade upgrade
	upgrade-url	Type URL in the tftp://<ip>/<image_name> format	get, set	get cluster-firmware-upgrade upgrade-url set cluster-firmware-upgrade upgrade-url <value>	WEP-2ac# set cluster-firmware-upgrade upgrade-url tftp://192.168.1.2/Wep-2ac_1.21.0.244.tar.gz WEP-2ac# get cluster-firmware-upgrade upgrade-url tftp://192.168.1.2/Wep-2ac_1.21.0.244.tar.gz

Class	Subclass	Feature	Possible commands	Syntax	Examples
	upgrade-method	all/ selective/< >, update method	get, set	get cluster-firmware-upgrade upgrade-method set cluster-firmware-upgrade upgrade-method <value>	WEP-2ac# set cluster-firmware-upgrade upgrade-method all WEP-2ac# get cluster-firmware-upgrade upgrade-method all
	upgrade-status	Current update status	get	get cluster-firmware-upgrade upgrade-status	WEP-2ac# get cluster-firmware-upgrade upgrade-status Not Initialized
	upgrade-members	List of IP addresses of devices in the cluster, separated by commas	get, set	get cluster-firmware-upgrade upgrade-members set cluster-firmware-upgrade upgrade-members <value>	WEP-2ac# set cluster-firmware-upgrade upgrade-members 192.168.1.1,192.168.1.3 WEP-2ac# get cluster-firmware-upgrade upgrade-members 192.168.1.1,192.168.1.3

7 List of changes

Document version	Issue date	Revisions
Version 1.20	21.04.2023	Synchronization with firmware version 1.23.0 Changes in section: • 5.6.3 Virtual Wi-Fi access points (VAP) configuration • 5.6.7 System settings
Version 1.19	09.09.2022	Synchronization with firmware version 1.22.4 Added: • 5.5.6.3 WGB-ARP-Timeout configuration Changes in section: • 4.12 Workgroup Bridge menu
Version 1.18	03.06.2022	Synchronization with firmware version 1.22.2
Version 1.17	22.04.2022	Synchronization with firmware version 1.22.1 Changes in section: • Device technical parameters
Version 1.16	03.12.2021	Synchronization with firmware version 1.21.1
Version 1.15	30.09.2021	Synchronization with firmware version 1.21.0
Version 1.14	07.12.2020	Synchronization with firmware version 1.20.0
Version 1.13	09.04.2020	Synchronization with firmware version 1.19.3
Version 1.12	24.02.2020	Synchronization with firmware version 1.19.0
Version 1.11	01.10.2019	Synchronization with firmware version 1.18.1
Version 1.10	05.06.2019	Synchronization with firmware version 1.17.0
Version 1.9	12.02.2018	Synchronization with firmware version 1.16.0
Version 1.8	30.11.2018	Synchronization with firmware version 1.15.0
Version 1.7	10.08.2018	Synchronization with firmware version 1.14.0
Version 1.6	8.05.2018	Synchronization with firmware version 1.12.2 Changes in section: • Device specifications
Version 1.5	26.12.2017	Synchronization with firmware version 1.11.4
Version 1.4	30.10.2017	Synchronization with firmware version 1.11.2
Version 1.3	02.08.2017	Synchronization with firmware version 1.10.0
Version 1.2	01.02.2017	Synchronization with firmware version 1.9.0

Document version	Issue date	Revisions
Version 1.1	16.12.2016	Synchronization with firmware version 1.8.0
Version 1.0	20.07.2016	First issue
Firmware version 1.23.0		

TECHNICAL SUPPORT

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

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

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

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

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