Firmware version 1.2.0 WB-15-W2. User manual

Wireless access point

WB-15-W2
User manual,
Firmware version 1.2.1 (02.2020)

IP address: http://192.168.1.1
User Name: admin
Password: password

Introduction

Annotation

WB-15-W2 is an all-weather wireless Wi-Fi access point with LTE support and a channel redundancy feature for connecting network equipment to the Internet or departmental/corporate networks. The device supports router mode, monitoring the quality of connection with the base station, traffic shaping.

This manual specifies intended purpose, main technical parameters, design, installation procedure, safe operation rules and installation recommendations and also specifies settings that available in WEB interface of the device.

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.

Device description

Purpose

WB-15-W2 is an all-weather wireless Wi-Fi access point with LTE support and a channel redundancy feature for connecting network equipment to the Internet or departmental/corporate networks. The device supports router mode, monitoring the quality of connection with the base station, traffic shaping.

WB-15-W2 is designed in a housing with an IP-54 protection, which allows you to operate the device in hard weather conditions.

Power is supplied through the terminals (in the car) or using Passive PoE technology.

Device specification

Interfaces:

- 1 port of 10/100Base-T(Ethernet)
- 1 interface of 2G/3G/4G with channel redundancy mode
- 2 SMA (female) connectors for connecting external 2G/3G/4G antennas (Omni, sector, panel, etc.)
- 1 SMA (female) connector for connecting external GPS antenna
- Wi-Fi 2.4 GHz IEEE 802.11b/g/n
- Wi-Fi 2.4 GHz (packet analyzer) based on Realtek RTL8192FR chip

Device is powered through a 24V PoE injector from a 220V network, or through a DC power adapter.

Do not use an injector with voltage different from 24V so as not to break down the device!

Functions:

WLAN capabilities:

- Support for IEEE 802.11b/g/n
- Data aggregation, including A-MPDU (Tx/Rx) and A-MSDU (Rx)
- WMM-based priorities and packet planning
- Support for hidden SSID
- Subscriber isolation within one VAP
- 4 virtual access points
- Channel autoselection
- Radio scan
- Wi-Fi traffic monitoring mode

Network functions:

- Autonegotiation of speed, duplex mode and switching between MDI and MDI-X modes
- Router operation mode
- Static routing
- DHCP server
- IPSec
- Subscriber traffic transmission beyond tunnels
- Static lease
- ACL
- NTP

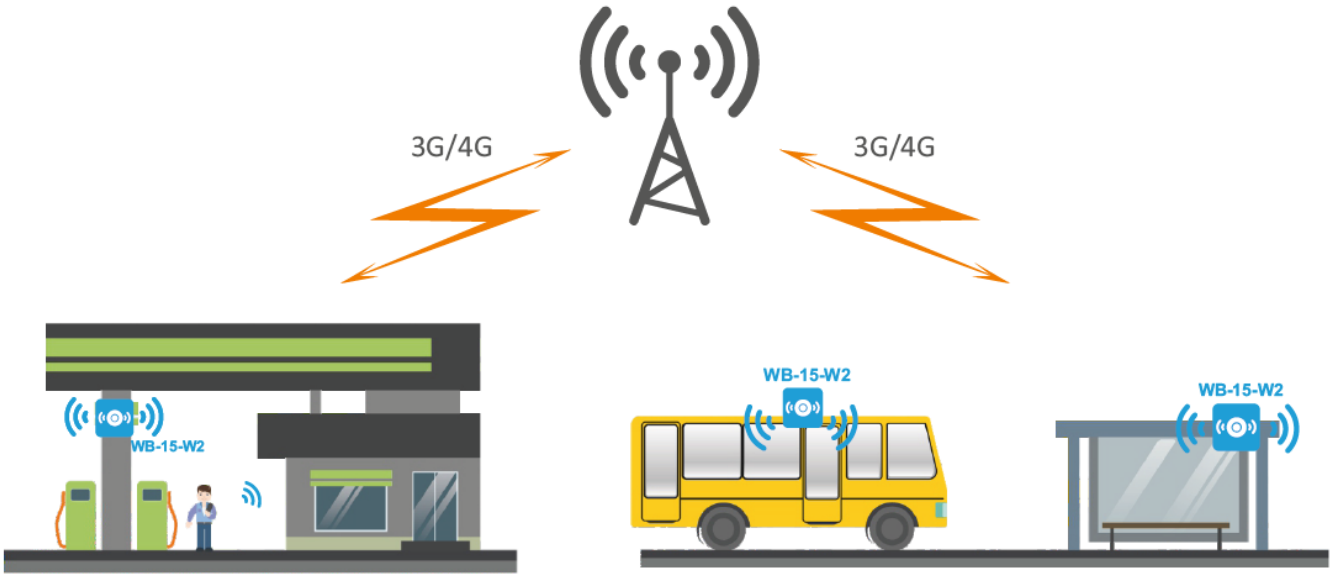
QoS functions

- Priority and profile-based packet scheduling
- Capacity limitation for each SSID
- Capacity limitation for each client
- Client limitation for each VAP
- WMM parameters changing

Security:

- WPA/WPA2 data encryption
- Device access restriction
- Support for Captive Portal

WB-15-W2 application diagram is shown oh the figure below.



Technical features

Technical features

Ethernet interface parameters	
Number of ports	1
Electrical connector	RJ-45
Data rate, Mbps	10/100
Standards	BASE-T

2G/3G/4G interface parameters	
Frequency ranges	4G LTE FDD: B1, B3, B5, B7, B8, B20 4G LTE TDD: B40 3G UMTS: B1, B8 2G GSM: 850M, 900M, 1800M, 1900M
Data transfer rate[1]	4G LTE FDD (Cat 4): 150 Mbps (DL) / 50 Mbps (UL) 4G LTE TDD (Cat 4): 130 Mbps (DL) / 35 Mbps (UL) 3G DC-HSPA+: 42 Mbps (DL) / 5,76 Mbps (UL) 2G EDGE: 384 Kbps (DL) / 384 Kbps (UL)
Maximum transmitter power[2]	4G LTE: up to 23 dBm 3G UMTS: up to 23 dBm 2G GSM: up to 33 dBm
Wireless interface parameters	
Standards	802.11b/g/n
Frequency range, MHz	2400– 2480 MHz
Modulation	K, BPSK, QPSK, 16QAM, 64QAM
Operating channels[2]	802.11b/g/n: 1-13 (2412–2472 MHz)
Data transfer rate[1], Mbps	802.11n: up to 300 Mbps
Maximum transmitter output power[2]	2.4 GHz: up to 18 dBm
Receiver sensitivity	2.4 GHz: up to -90 dBm
Security	64/128/152-bit WEP encryption of the data, WPA/WPA2 data encryption
Control	
Remote control	WEB, Telnet, SSH
General parameters	
Processor	Realtek RTL8197FS
RAM	128 MB
Flash memory	32 MB
Power supply	Passive PoE 24 V DC 9-36 V
Max. power consumption	8 W
Range of operation temperatures	from -45 to +60°
Ingress Protection Marking	IP54
Dimensions	88x232,5x47 mm

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

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

Design

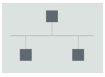
WB-15-W2 housed in a plastic case, industrial version. The size of the device: 88x232.5x47 mm. The layout of WB-15-W2 is shown in the figure below.

Under the cover at the bottom of the device are located: factory reset button (F), slot for installing two 2G/3G/4G nano-SIMs, 10/100Base-T (Ethernet) port for connecting to an internal network and Passive PoE power, socket for connecting 9-36 VDC power, 1 SMA type connector (female) for connecting an external GPS antenna.

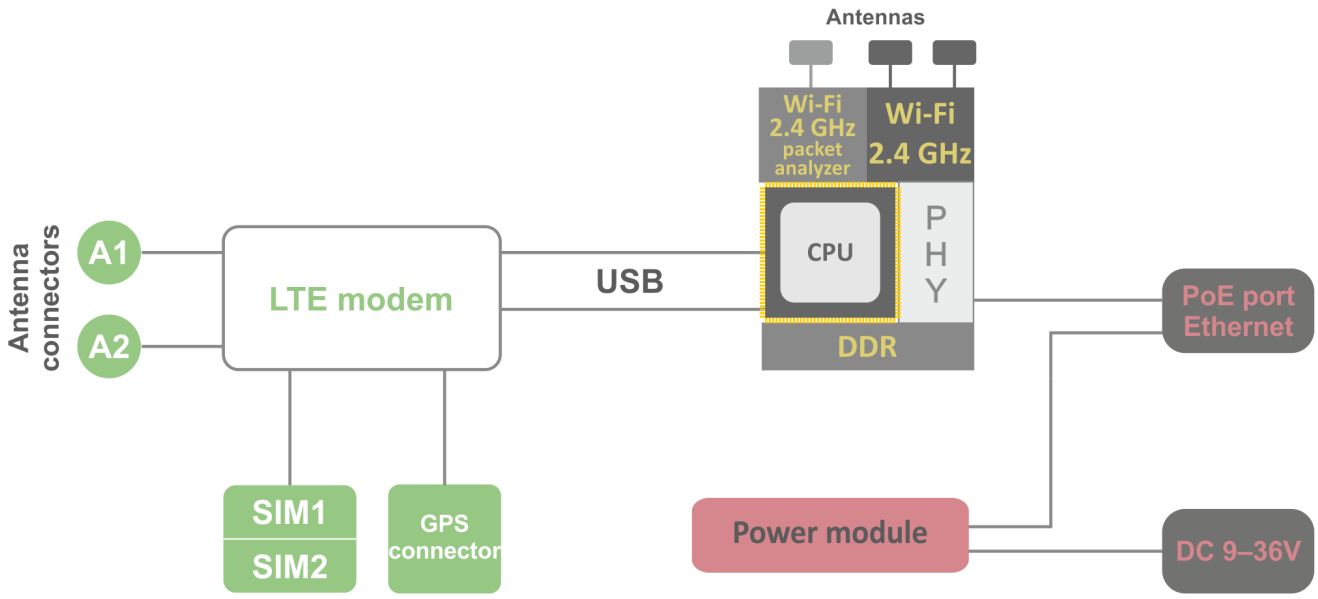
Light indication

The layout of WB-15-W2 indication panel is shown in the figure below.

The LED indicators located on the front panel show the current state of the WB-15-W2. The list of indicators and their description is shown in the table below.

LED		LED status	Description
	**Power** – device power and operation status LED	solid green	the device power supply is enabled, connected to the mobile network, normal operation
		solid orange	the device is not connected to the mobile network
		solid red	the device is loading
	**LAN** – ethernet interface port indicator	solid green	the channel between Ethernet interface of WB-15-W2 and connected device is active
		flashes	packet data transmission between Ethernet interface of WB-15-W2 and connected device
	**Wi-Fi** – wireless Wi-Fi interface indicator	solid green	at least one VAP is enabled on the device
	Indicator of link level from a cellular provider base station (RSSI)	solid red	the signal level is less than -81 dBm
		solid yellow	the signal level is less than -69 dBm
		solid green	the signal level is more or equal to -69 dBm
		none of the indicators is on	no signal, the device is not connected to the mobile network

The device schematic structure



Reset to the default settings

You can reset the device configuration using the «F» button on the device: When the device is loaded, press and hold the «F» button (approximately 10–15 seconds) until «Power» indicator is flashing orange. Device will be rebooted automatically. DHCP server will be launched by default (clients connected via Ethernet will receive address in the range from 192.168.1.2 to 192.168.1.254 with subnet mask 255.255.255.0). The device address is 192.168.1.1/24. User Name/Password to access via web interface: admin/password.

Delivery package

The WB-15-W2 standard delivery package includes:

- WB-15-W2 access point;
- Mounting kit;
- User manual (supplied on a CD);
- Conformity certificate;
- Technical passport.

Installation order

This section describes the safety measures, installation procedure and process of turning WB-15-W2 on.

Safety rules

1. Do not open the device case. There are no user serviceable parts inside.
2. Do not install the device during a thunderstorm. There is a risk of lightning stroke.
3. You must follow requirements for voltage, current and frequency specified in the user manual.
4. Measuring devices and computer must be grounded before connecting to the device. The electric potential differnce between devices' cases should not exceed 1 V.
5. Make sure that all the cables are intact and they are reliably attached to connectors.
6. You should satisfy established standards and requirements for working at height during the device installation on the high-rise constructions.
7. The device exploitation should be performed by specially prepared engineering and technical personnel.
8. Connect only to operational service equipment.

Installation recommendations

1. Recommended location for device installation: fix on a mast/pole/wall.
2. Before you install and enable device, check the device for visible mechanical defects. If defects are observed, you should stop the device installation, draw up corresponding act and contact the supplier.
3. Install the device on communications mast/pole/wall in the way that the Ethernet port is pointed down.
4. During the device installation to provide Wi-Fi coverage area with the best characteristics take into account the following rules:
    a. Install the device in the center of the intended wireless coverage area;
    b. Do not install the device near (about 2 m) electrical and radio devices.
    c. Use of radio phones and other devices, which work at 2.4 GHz, within the range of your Wi-Fi wireless network is not recommended;

d. Obstacles in the form of glass/metal constructions, brick/concrete walls, water cans and mirrors can significantly reduce Wi-Fi action radius.

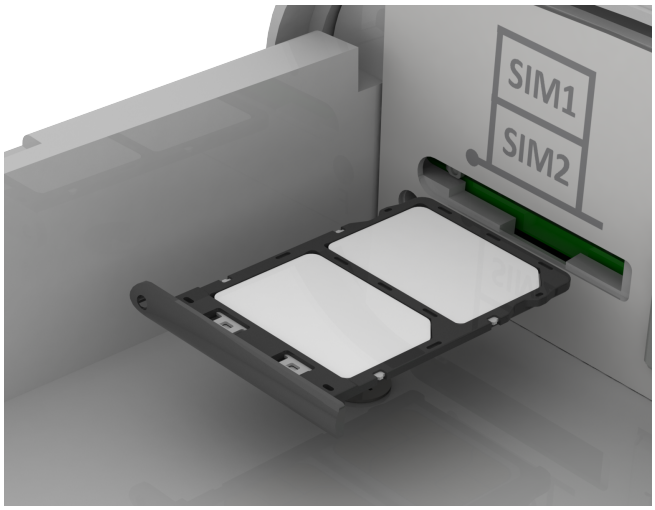
5. When mounting the device, you should pay attention to the location of the towers of the cellular base stations of providers whose SIM cards will be used in the device, and place the device as close to them as possible (or, if you use a sector antenna, direct the antenna to the base station).

WB-15-W2 mounting

Pre-tuning

Before installing, proceed pre-tuning of the device:

1. Insert 1 or 2 SIM cards into the slot (as shown in the figure below). SIM1 is active by default.
2. Connect the power supply (points 3, 4 in the Installation procedure section).



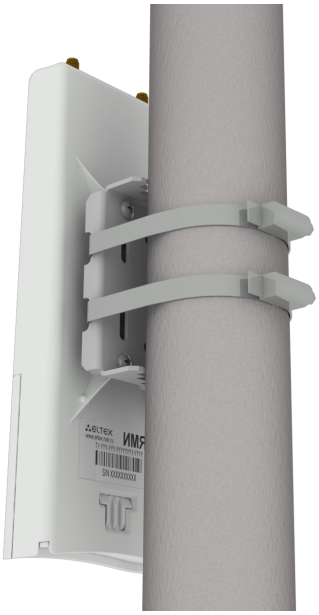
3. Ensure the 3G/4G network is available: RSSI indicators should be on (network connection will occur 1-2 minutes after the device boots up).
4. Configure the device: follow the algorithm from the Configuration example section.

Please note that for the device to automatically connect to the mobile network, a SIM card must be inserted into the device before power is supplied to it.

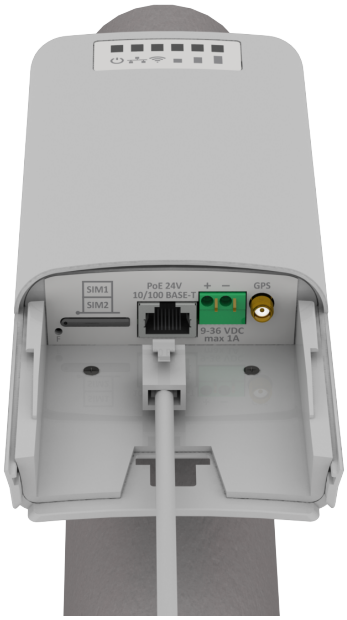
Mounting algorithm

1. Attach the bracket to the device with the screws provided, as shown in the figure below.

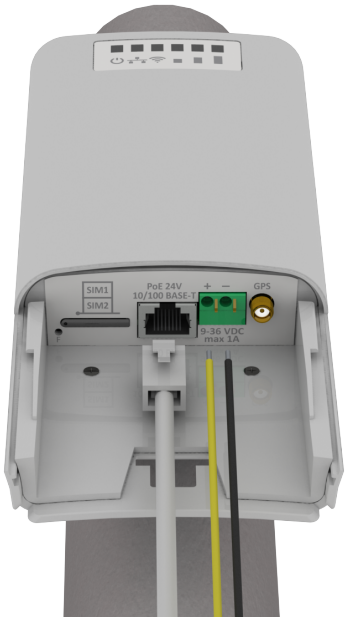
2. Install the device on communications mast/pole pointing Ethernet port down as it is shown on the figure below. Attach the device using clamps supplied in the device package. Comply the safety rules and recommendations given in Safety rules and Installation recommendations.



3. Remove the bottom cover which close bottom panel and connect the Ethernet cable to the PoE port.



4. If the device will be supplied by a DC network, connect the contacts of the DC power supply (9-36V), observing the polarity.



5. Close the bottom cover.

6. Connect the OMNI antennas to the device. If using a sector antenna, connect it using cable assemblies.

7. Adjust the position of the antenna so that it faces toward the base station.

8. Connect Ethernet cable of your WB-15-W2 to LAN port of PoE injector (Passive PoE 24V). If the device is connected to a DC power supply, if you need to connect to the switch, make sure that PoE is disabled on it.

9. If you using PoE injector connect it to 220 V power supply network using the cable.

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

Managing the device through web interface

Getting started

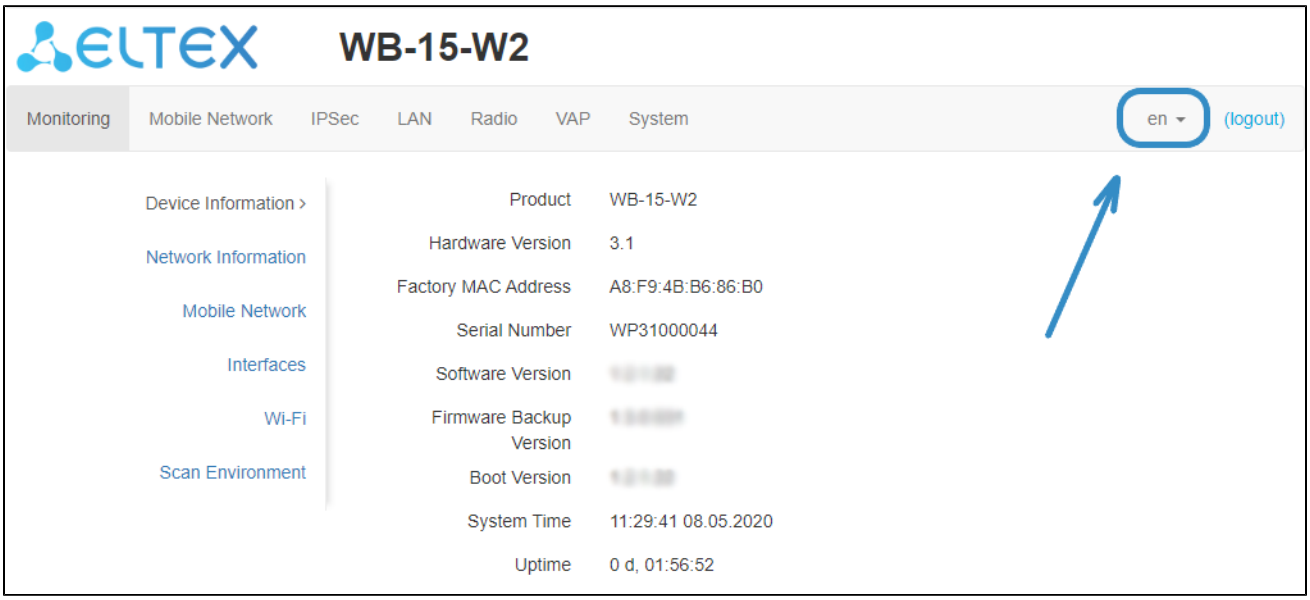
To start, you need to connect the device through a browser:

1. Open a web browser (web-page explorer), for example, Firefox, Opera, Chrome.
2. Enter IP-address of the device to the browser address line.

> The default IP-address of the device – 192.168.1.1, subnet mask – 255.255.255.0. DHCP server is launched by default (clients connected to the LAN will receive address in the range from 192.168.1.2 to 192.168.1.254).
>
> Factory settings: username – *admin*, password – *password*.

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

3. Enter your username into ‘Login’ and password into ‘Password’ field.
4. Click the ‘Log in’ button. A menu for monitoring the status of the device will open in a browser window.
5. If necessary, you can switch the display language information. Russian and English languages are available for WEB interface.



Applying configuration and discarding changes

1. Applying configuration

After clicking the Apply button the configuration is saved to flash-memory of the device and new settings apply. All the settings come into operation without device rebooting.

Visual indication of the process current status of the setting application process is realised in the WEB interface.

Image	State description
Apply	After pressing «Apply», the process of settings saving to device memory is launched. This is indicated by the icon in the tab name and on the «Apply» button.
Apply	Successful settings saving and application are indicated by the icon in the tab name.

2. Discarding changes

Click Cancel to discard changes.

You can discard changes only before pressing «Apply» button. If you press «Apply» button, all the changed parameters will be applyed and saved to device memory.

Main elements of the web interface

Navigation elements of the WEB interface are shown on the figure below.

User interface window is divided into five general areas:

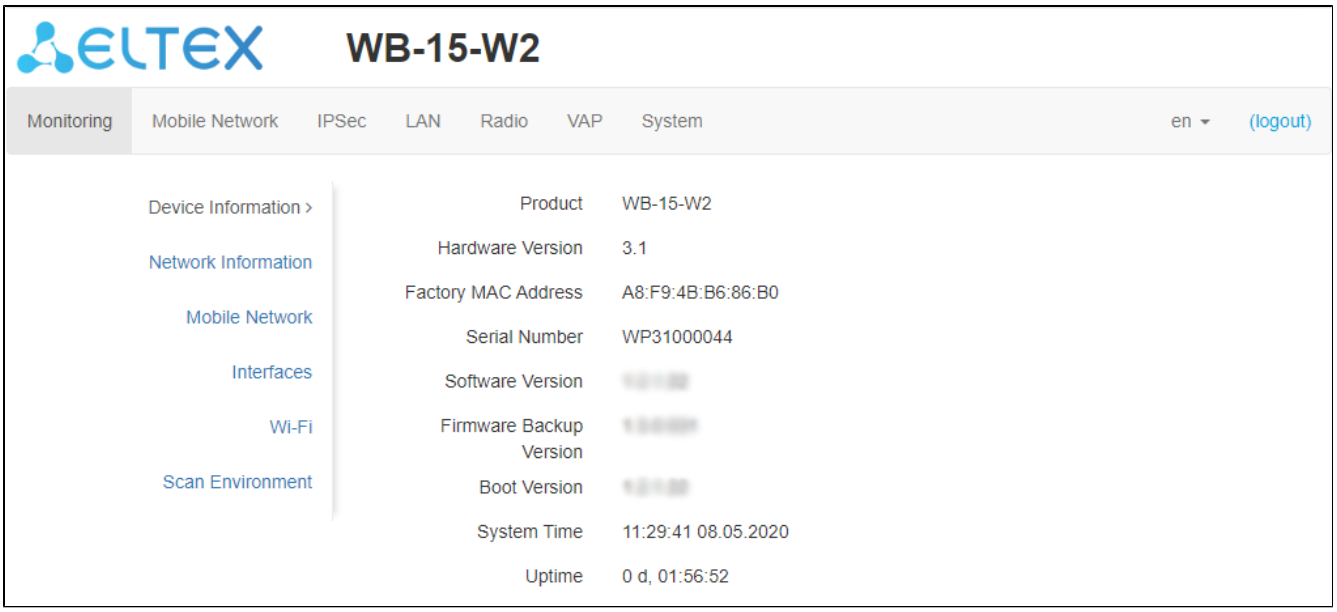
1. Menu tabs categorize the submenu tabs: Monitoring, Mobile Network, LAN, Radio, VAP, System.
2. Interface language selection and Logout button designed to to end a session in the WEB interface under a given user.
3. Submenu tabs allow you to control settings field.
4. Devcie configuration field displays data and configuration.
5. Information field displays current firmware version.

The «Monitoring» menu

In the «Monitoring» menu you can view the current system state.

The «Device Information» submenu

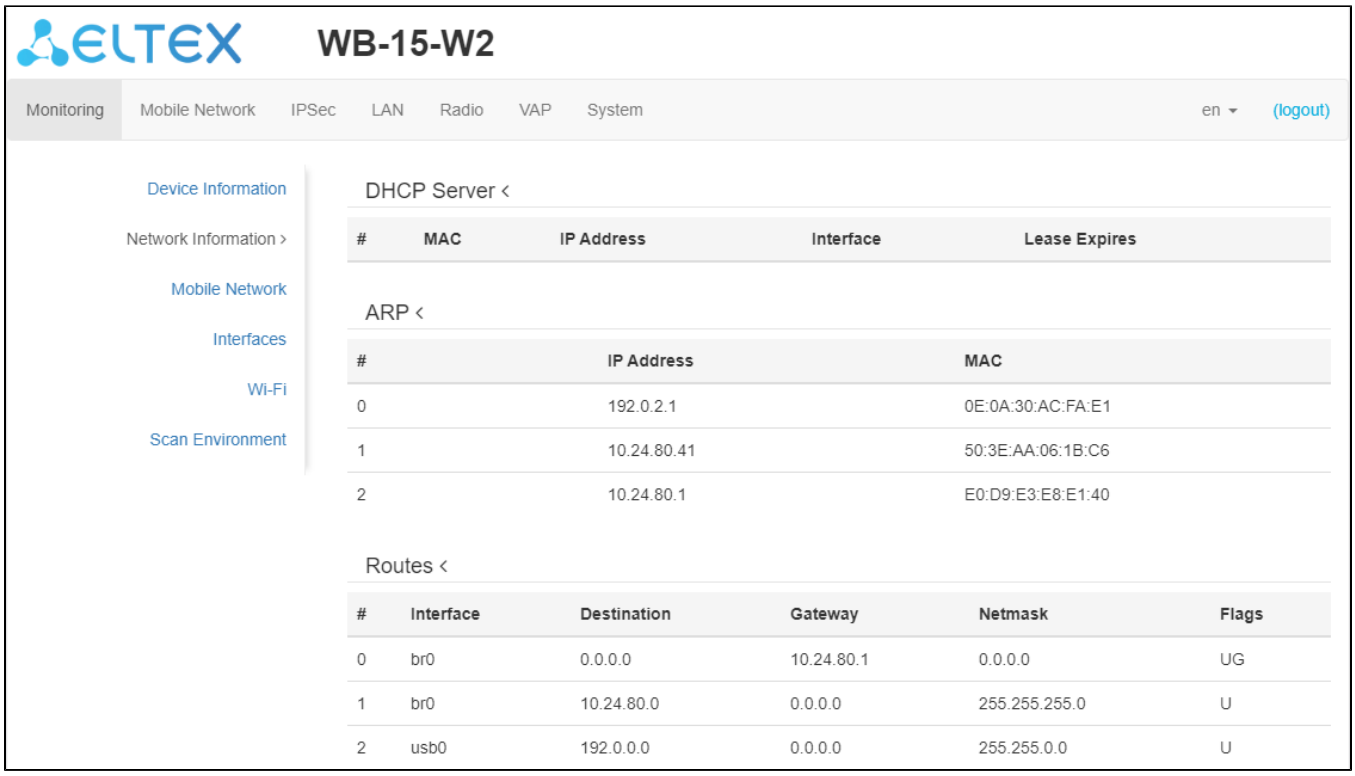
The «Device Information» submenu displays main WB-15-W2 parameters.



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

The «Network Information» submenu

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



DHCP server:

- *MAC address* – MAC address of the device that received the address from the internal DHCP server;
- *IP address* – IP address issued by the internal DHCP server to the connected device;
- *Interface* – the interface from which the IP address was issued;
- *Lease Expires* – the time after which the client will send a request to extend the lease of the issued address.

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

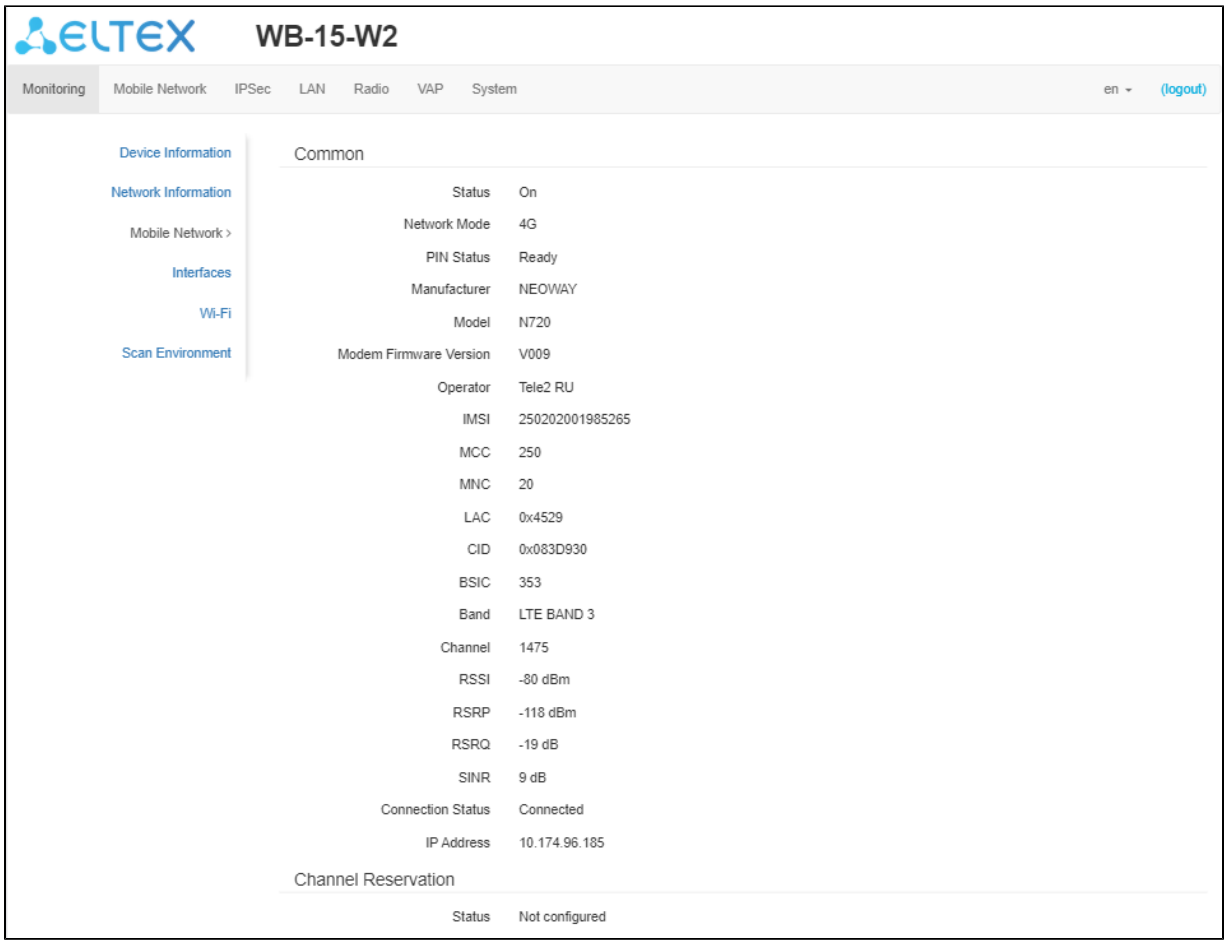
- *IP address* – the device IP address;
- *MAC address* – the device MAC address.

Routes:

- *Interface* – device interface name;
- *Destination* – IP address of destination host or subnet that the route is established to;
- *Gateway* – gateway IP address that allows for the access to the Destination;
- *Netmask* – subnet mask;
- *Flags* – specific route attributes. The following flag values exist:
  - **U** – means that the route is created and passable.
  - **H** – identifies the route to the specific host.
  - **G** – means that the route lies through the external gateway. System network interface provides routes in the network with direct connection. All other routes lie through the external gateways. G flag is used for all routes except for the routes in the direct connection networks.
  - **R** – means that the route most likely was created by a dynamic routing protocol running on a local system through the «reinstate» parameter;
  - **D** – means that the route was added on reception of the ICMP Redirect Message. When the system learns the route from the ICMP Redirect message, the route will be added into the routing table in order to exclude redirection of the following packets intended for the same destination.
  - **M** – means that the route was modified – likely by a dynamic routing protocol running on a local system with the «mod» parameter applied.
  - – means buffered route with corresponding record in the ARP table.
  - – means that the route source is the core routing buffer.
  - **L** – means that the route destination is an address of this PC. Such «local routes» exist in the routing buffer only.
  - – means that the route destination is a broadcasting address. Such «broadcast routes» exist in the routing buffer only.
  - **I** – means that the route is related to the loopback interface and not to address to a ring network. Such «internal routes» exist in the routing buffer only.
  - **!** – means that datagrams sent to this address will be rejected by the system.

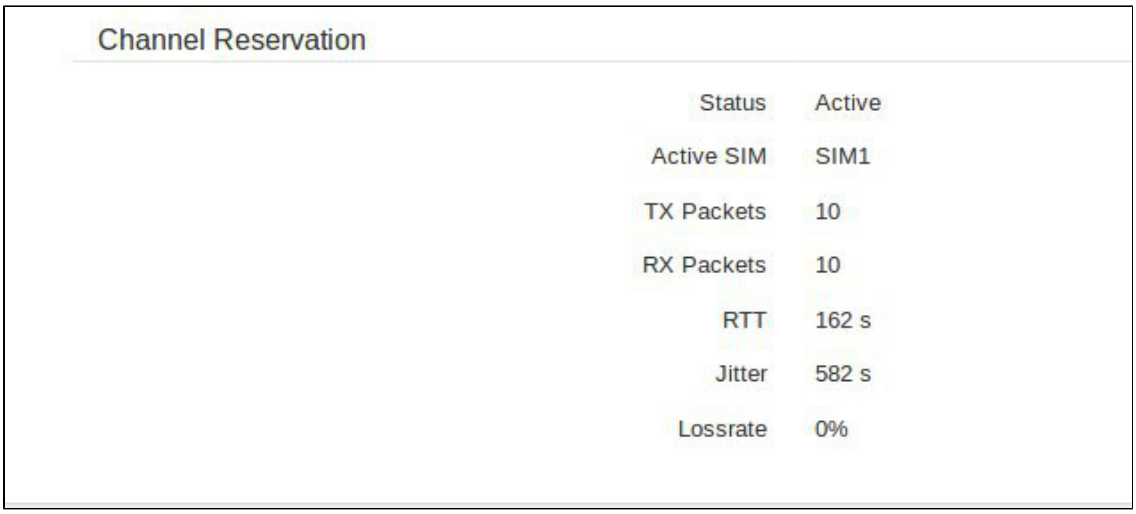
The «Mobile network» submenu

In the «Mobile network» submenu you can view the current status and parameters of the connection to the mobile network.



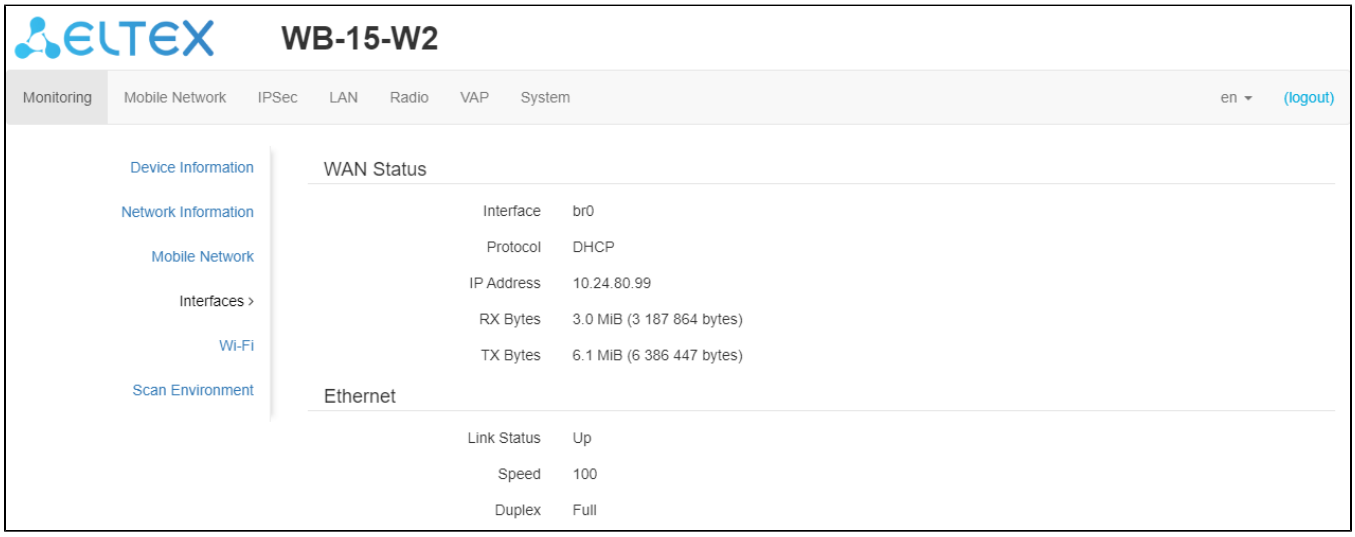
- *Status* – connection status;
- *Network mode* – mode in which the modem is connected to the mobile network;
- *PIN Status* – status that indicates whether the PIN is set correctly in the configuration for the SIM used. Ready status – PIN code is not required or is set correctly; Waiting status- PIN code is incorrect;
- *Manufacturer* – manufacturer of the internal modem;
- *Model* – model of the internal modem;
- *Modem Firmware Version* – installed firmware version for the internal modem;
- *Operator* – provider of the mobile network to which the device is connected;
- *IMSI* – active SIM IMSI code;
- *MCC,MNC* – identifiers of the active SIM-card belonging to a specific mobile operator;
- *LAC,CID,BSIC* – identifiers of the geographical area, cell and base station of the mobile network to which the device is connected;
- *Band* – bandwidth that used;
- *Channel* – frequency channel;
- *RSSI* – the average value of the signal power level from the base station;
- *RSRP* – level of received signal from the base station (for LTE standard);
- *RSRQ* – quality level of received pilot signals (for LTE standard);
- *SINR* – ratio of the useful signal level to the noise level at the receiving point (for LTE standard).

Channel redundancy:



- *Status* – operation status:
  - Not configured – the parameter is disabled in the device configuration;
  - Active – channel redundancy is enabled;
  - Changing the active SIM card – communication through the current SIM card does not meet the channel redundancy parameters specified in the configuration, the active SIM card is changed (the active SIM card in this case will be the SIM card that is being switched to).
- *Active SIM* – number of the SIM card that is currently active;
- *TX Packets* – number of ping-request packets sent to the ping-server specified in the configuration;
- *RX packets* – number of ping-reply packets received by the device from the ping-server specified in the configuration;
- *RTT* – average ping-request response time, ms;
- *Jitter* – permissible deviation from the response time, ms;
- *Lossrate* – the percentage of ping-request packets to which no response was received from the ping-server.

The «Interfaces» submenu



WAN Status:

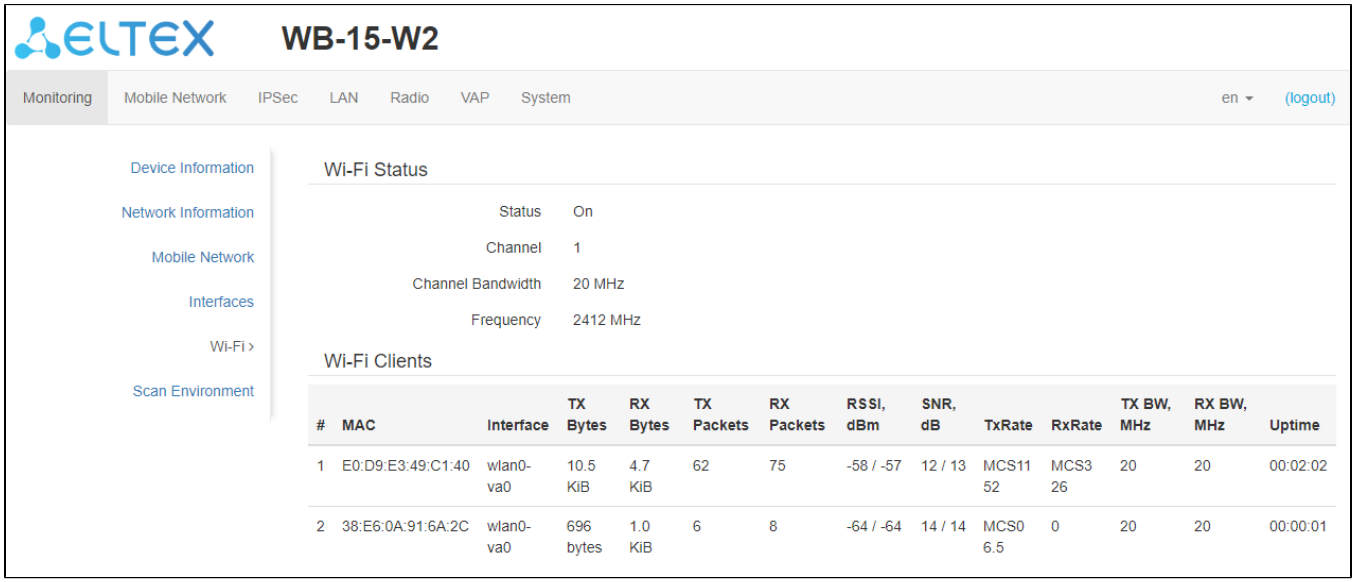
- *Interface* – device interface used as a WAN;
- *Protocol* – protocol for obtaining an IP address on the WAN interface for network communication with the internal modem;
- *IP address* – IP address of the WAN interface;
- *RX Bytes* – amount of traffic received on the WAN interface;
- *TX Bytes* – amount of traffic transmitted from the WAN interface.

Ethernet:

- *Link Status* – current link status;
- *Speed* – set speed on the link;
- *Duplex* – used mode.

The «Wi-Fi» submenu

The «Wi-Fi» submenu displays information about current radio interface configuration and the status of connected Wi-Fi clients.



Wi-Fi Status:

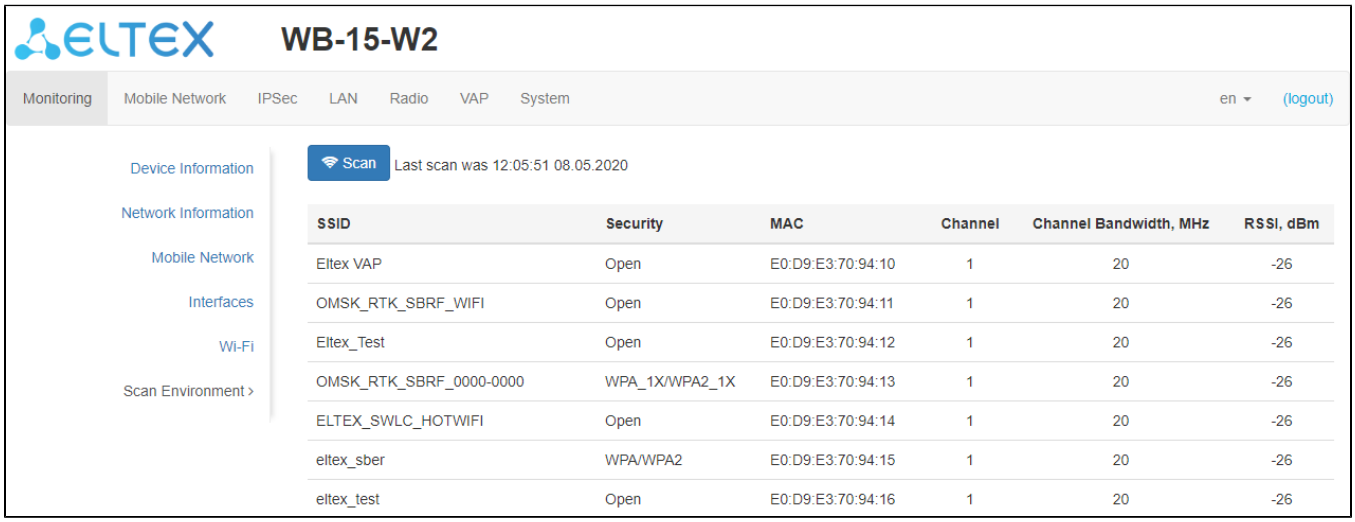
- *Status* – Wi-Fi interface status;
- *Channel* – number of used Wi-Fi channel;
- *Bandwidth* – bandwidth of used Wi-Fi channel, MHz;
- *Frequency* – frequency of used Wi-Fi channel, MHz.

Wi-Fi clients:

- *#* – sequence number of the connected device in the list;
- *MA* – MAC address of the connected device;
- *Interface* – WB-15-W2 interface to which the device is connected;
- *TX Bytes* – number of bytes transmitted to the connected device;
- *RX Bytes* – the number of bytes received from the connected device;
- *TX Packets* – number of packets transmitted to the connected device;
- *RX Packets* – the number of packets received from the connected device;
- *RSSI* – received signal level, dBm;
- *SNR* – signal/noise ratio, dB;
- *TxRate* – channel data rate of transmission, Mbps;
- *RxRate* – channel data rate of receiving, Mbps;
- *Tx BW* – transmission bandwidth, MHz;
- *Rx BW* – reception bandwidth, MHz;
- *Uptime* – Wi-Fi client connection uptime.

The «Scan Environment» submenu

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



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

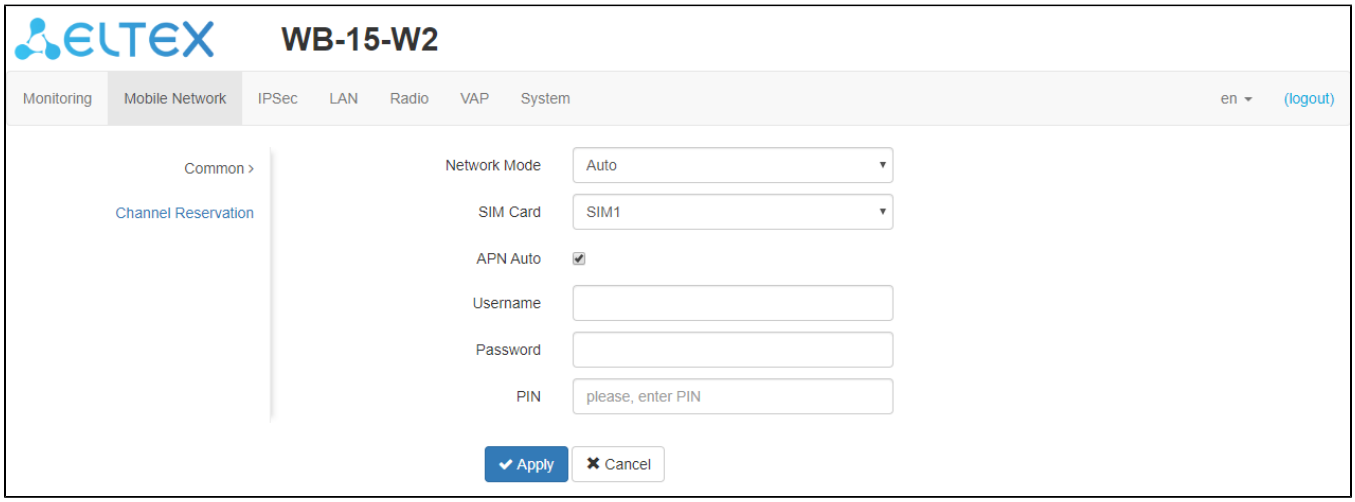
- *SSID* – SSID of the detected access point;
- *Security* – security mode of the detected access point;
- *MAC* – MAC address of the detected access point;
- *Channel* – radio channel on which the detected access point operates;
- *Bandwidth* – width of the radio channel used by the detected access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

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

The «Mobile Network» menu

In the «Mobile Network» menu, the 2G/3G/4G interface is configured.

The «Common» submenu

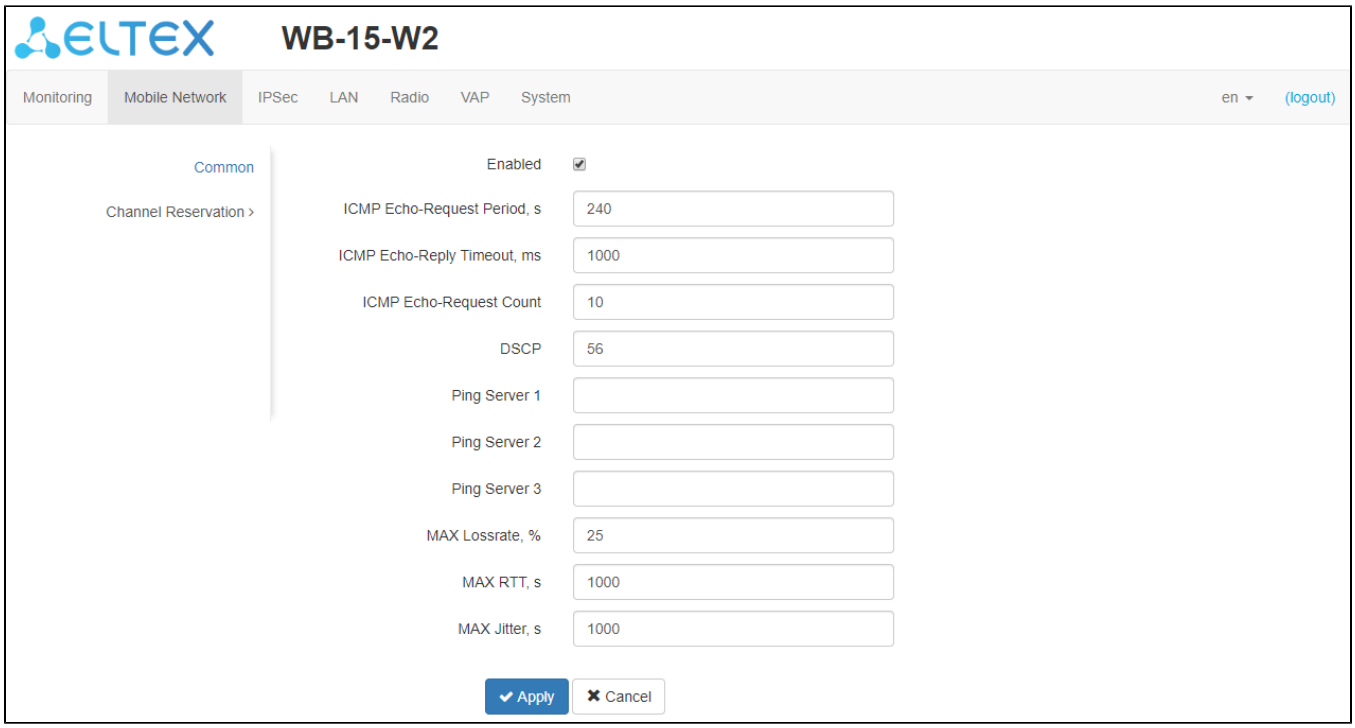


- *Network Mode* – select a standard for connecting the device to a cellular network. Auto is default. Also you can choose 2G, 3G, 4G, 2G-3G, 2G-4G, 3G-4G. When choosing the double option, the connection preference will be given to a more modern standard (for example, when the 3G-4G mode is set, then 4G connection will be priority);
- *SIM Card* – selects an active SIM card to connect to a mobile network. The default value is SIM1 (that is, a SIM card that is located in SIM slot 1);
- *APN Auto* – auto detection of APN for connection depending on the used mobile operator. If necessary, you can specify a static APN by deselecting APN Auto and entering the desired APN in the APN window that appears;
- *Username, Password* – additional parameters for connecting to a cellular network, optional;
- *PIN* – PIN code of the used SIM card.
  If there is no PIN code the field can be left blank.

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

The «Channel Reservation» submenu

In the «Channel Reservation» submenu, you can configure the switching of the active SIM card if the quality of the connection with the current active SIM card does not meet the specified parameters. The channel quality control mechanism is based on sending ICMP messages to a server and analyzing the resulting statistics.



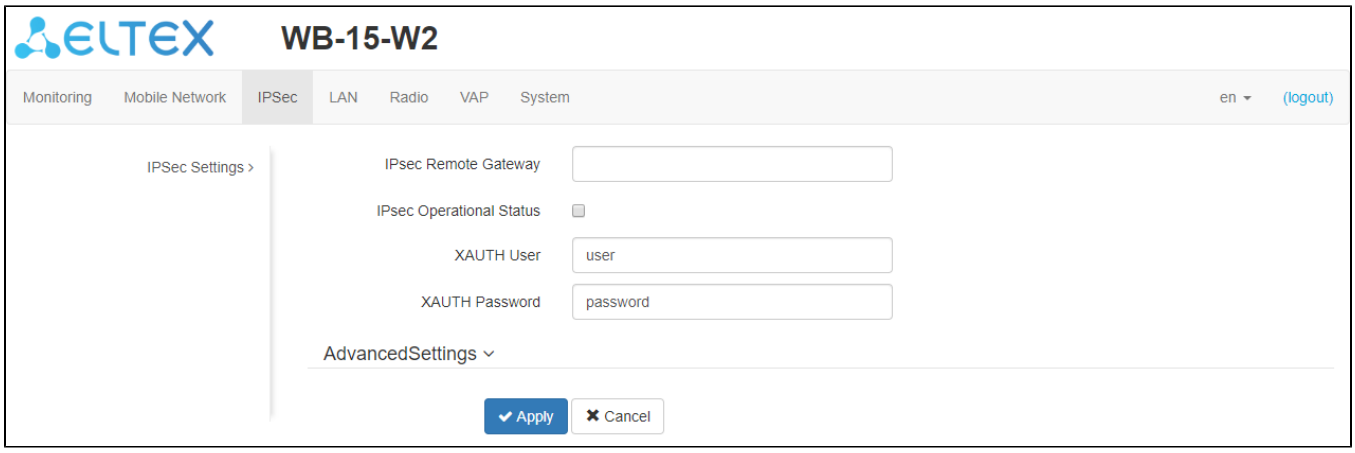
- *Enabled* – you must set a flag to activate the channel reservation function;
- *ICMP Echo-Request Period, s* – period with which the device will send ICMP requests to the specified ping-server;
- *ICMP Echo-Reply Timeout* – time during which the device will wait for an ICMP reply from the server. If the response from the server received later than the set wait timeout, or did not been received at all, this ICMP request is considered unanswered;
- *ICMP Echo-Request Count* – number of consecutive ICMP requests sent each time the procedure starts (after the time period for sending ICMP requests). The decision to switch the SIM card is based on the statistics obtained as a result of the procedure;
- *DSCP* – priority of sent ICMP requests;
- *Ping server 1, Ping server 2, Ping server 3* – servers to which the device sends ICMP requests. First, ping starts up to ping server 1, if it is unavailable (or if the received statistics do not meet the specified quality), ping starts up to ping server 2, then similarly to ping server 3.
  If the results are unsatisfactory on all configured servers, the active SIM card will switch. If the results are successful on at least one of the specified servers, the switch will not occur. For the mechanism to work, be sure to add at least one ping-server to the configuration;
- *MAX Lossrate, %* – maximum allowable percentage of ICMP requests for which no ICMP response was received during the timeout period for waiting for the ICMP response. If this loss value is exceeded, the active SIM card will switch, or go to the next ping-server;
- *MAX RTT, ms* – maximum average response time for all sent ICMP requests. If this value is exceeded, the active SIM card will switch, or go to the next ping-server;
- *MAX Jitter, ms* – maximum deviation from the average response time. If this loss value is exceeded, the active SIM card will switch, or go to the next ping-server.

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

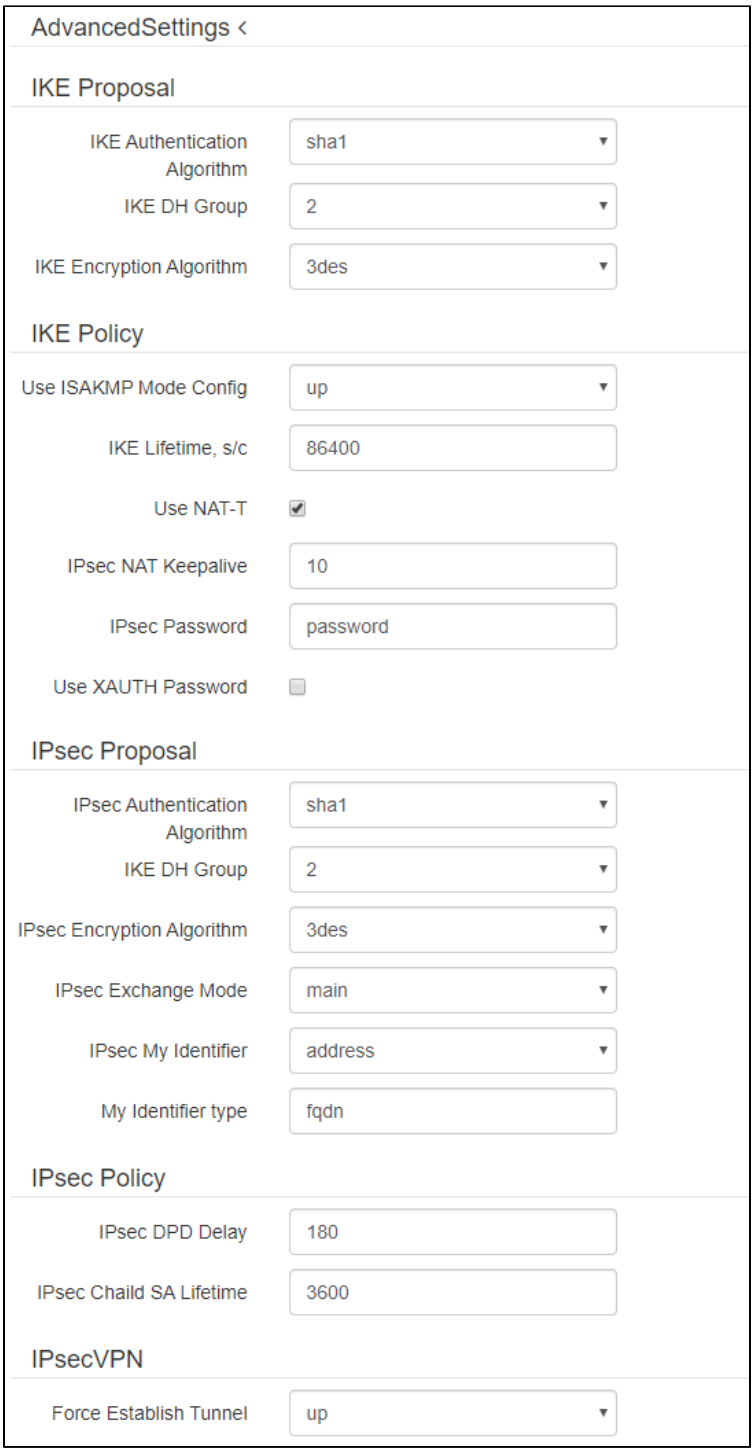
Please note that switching the active SIM card, or moving to the next ping-server, is carried out in the case when at least one of the received quality parameters does not satisfy the specified conditions.
In case there is a switch to a backup SIM card, this configuration will be automatically saved on the device. That is, when the device is rebooted, the SIM card that was active immediately before the reboot will be active.

The «IPSec» menu.

The «IPSec parameters»



- *IPsec Remote Gateway* – gateway for IPsec, set in IP address or domain name format;
- *IPsec Operation Status* – the status of the configured IPsec connection;
- *XAUTH User* – user name for advanced authorization, required for the mode config mechanism operation (range: 4-16 characters);
- *XAUTH Password* – user password for advanced authorization, required for the mode config mechanism operation (range: 8-48 characters)

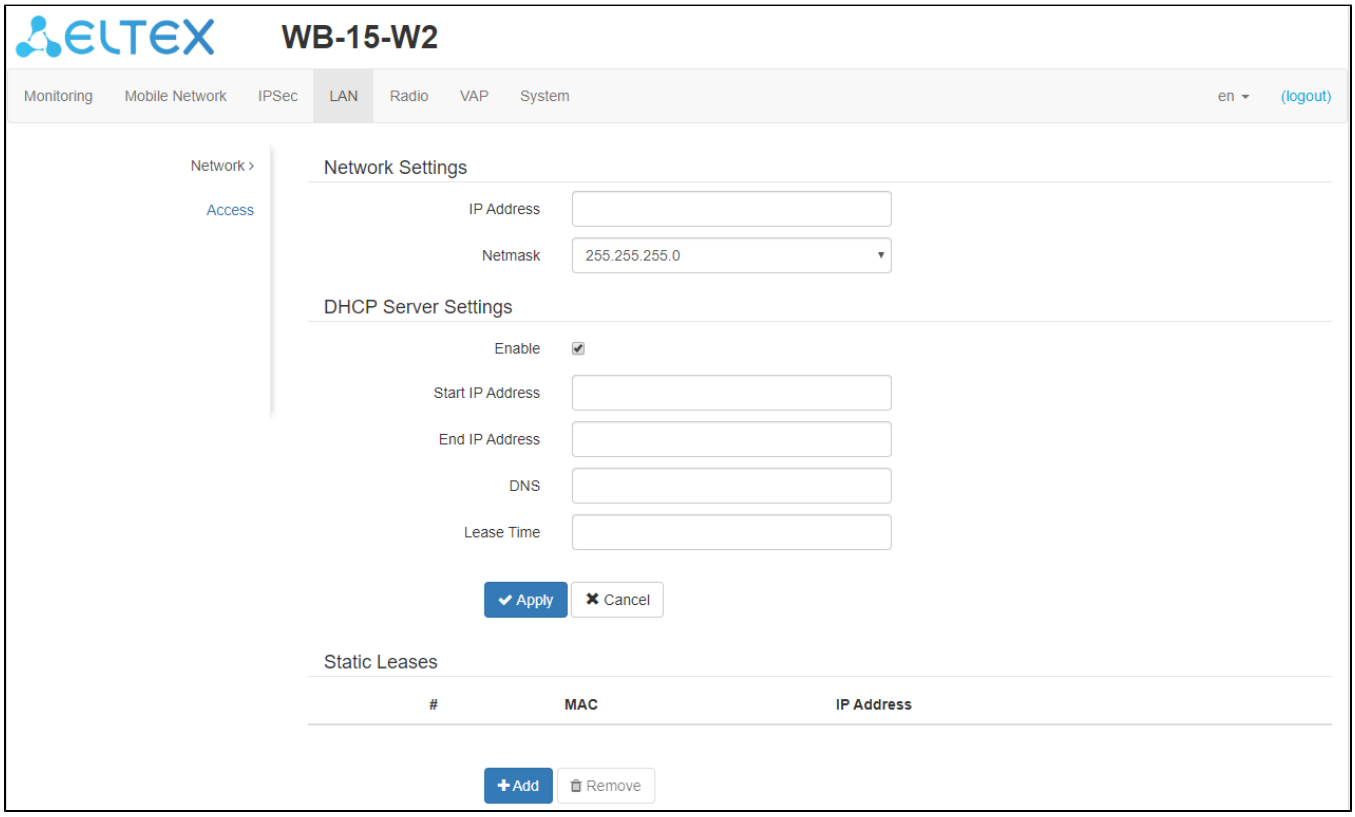


- *IKE Authentication Algorithm* – IKE hashing algorithm selection, designed to check data integrity;
- *IKE DH Group* – Diffy-Hellman's algorithm selection is used to set a shared secret on an insecure network;
- *IKE Encryption Algorithm* – selecting an encryption algorithm for phase 1 of IPsec connection;
- *Use ISAKMP Mode Config* – activate the mode of automatic obtain of virtual address, remote subnet, addresses for lifting GRE tunnels from ESR, to which we connect via IPSec;
- *IKE Lifetime* – IKE life time (phase 1), must be identical on both sides of the IKE/IPsec connection (Range: 180-86400 seconds);
- *Use NAT-T* – you must check the flag if AP is behind NAT*;*
- *IPsec NAT Keepalive* – frequency with which packets are sent to keepalive when working through NAT, so that NAT translation is kept on upstream routers when the client is not active for a long time. (Range: 0-300 seconds);
- *IPsec Password* – password for IKE/IPSEC connection (range: 8-48 characters);
- *IPsec Authentication Algorithm* – IPsec hashing algorithm selection, designed to check data integrity;
- *IPsec DH Group* – Diffy-Hellman's algorithm selection is used to set a shared secret on an insecure network;
- *IPsec Encryption Algorithm* – selecting an encryption algorithm for phase 1 of IPsec connection;
- *IPsec DPD Delay* – interval at which packets of connection failure detection are sent. If there are no IPsec VPN responses on the opposite side to 5 packets in a row, AP will consider the VPN to be broken and restart the IPsec VPN on its side. (Range: 5-600 seconds);

- *IPsec Chaild SA Lifetime* – lifetime of IPsec VPN SA (phase 2), must be the same on both sides of the IKE/IPsec tunnel. Should be lower than IKE Lifetime (Range: 180-86400 seconds);
- *Force Establish Tunnel* – enable to establish an IPsec VPN connection immediately. Otherwise, an IPsec VPN connection will be established upon request.

The «LAN» menu

The «Network» submenu



Network Settings:

- *IP Address* – IP address of the device in the LAN subnet;
- *Mask* – mask of the device's LAN subnet and DHCP server, which issues addresses to clients connected to Wi-Fi or Ethernet.

DHCP server settings:

Enable – set the flag so that clients connected to Wi-Fi or Ethernet interfaces can get an IP address. Specify the following parameters for the DHCP server:

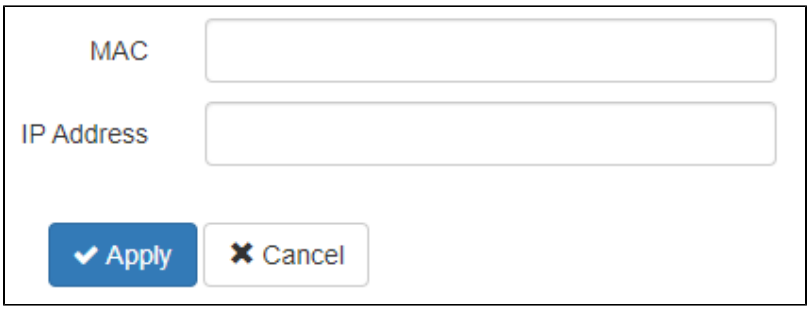
- *Start IP Address, End IP Address* – configuring a pool of addresses that can be issued to clients
- *DNS* – address of the DNS server that is passed to the client in the corresponding option. For the clients to work correctly on the Internet, the IP address of the device should be indicated as a DNS server;
- *Lease Time* – time after which the client will send a request to extend the lease of the issued address.

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

Please note that the address pool for issuing to clients must be on the same subnet as the device. A DHCP server issues IP addresses to clients on a LAN subnet, and in this case, the IP address of the device is a gateway for redirecting client requests to the WAN, that is, it performs the function of masquerading.

Static leases

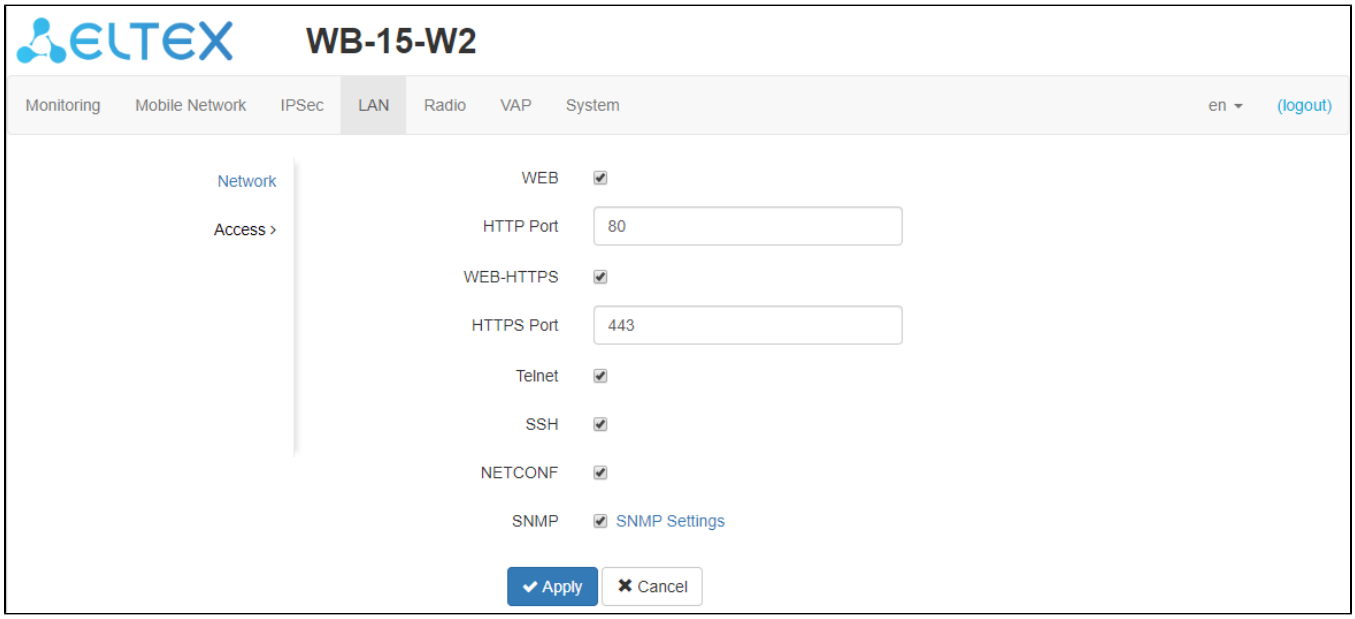
Click the «Add» button to add static addresses and enter MAC and IP addresses of the client. When connected to the device's Wi-Fi or Ethernet interfaces, the client with the specified MAC address will be given the specified IP address.



The «Access» submenu

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

Access via NETCONF is not supported in the current firmware version 1.2.1.



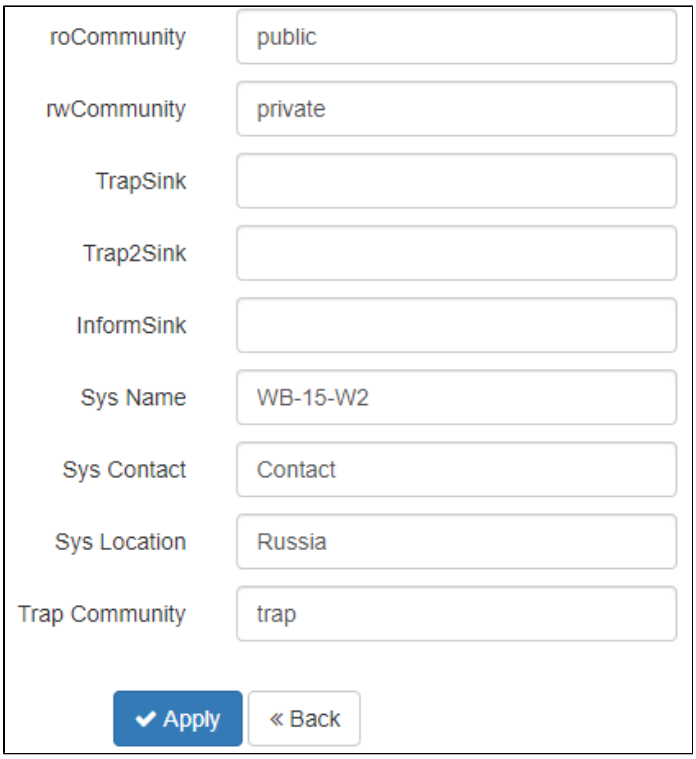
- To enable access to the device via the web interface via HTTP protocol, set the flag next to «WEB». In the window that appears, it is possible to change the HTTP port (by default, 80). The range of acceptable values of ports, in addition to the default, from 1025 to 65535 inclusive;
- To enable access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

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

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

WB-15-W2 software allows monitoring status of the device and configuring it via SNMP. In the SNMP submenu, you can configure settings of SNMP agent. The device supports SNMPv1, SNMPv2, SNMPv3.

To change the SNMP settings, check the box next to «SNMP», apply the configuration and then go to the «SNMP configuration» submenu.



- *roCommunity* – password for parameter reading (common: *public*);
- *rwCommunity* – password for parameter writing (common: *private*);
- *TrapSink* – an IP address or domain name of SNMPv1-trap messages receiver in HOST [COMMUNITY [PORT]] format;
- *Trap2Sink* – an IP address or domain name of SNMPv2-trap messages receiver in HOST [COMMUNITY [PORT]] format;
- *InformSink* – IP address or domain name of Inform message recipient in HOST [COMMUNITY [PORT]] format;
- *Sys Name* – device name;
- *Sys Contact* – the manufacturer contact;
- *Sys Location* – information on the device location;
- *Trap Community* – a password which is contained in traps (by default: trap).

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

- Enterprise.2.1 – SNMP settings
- Enterprise.3.1 – syslog settings

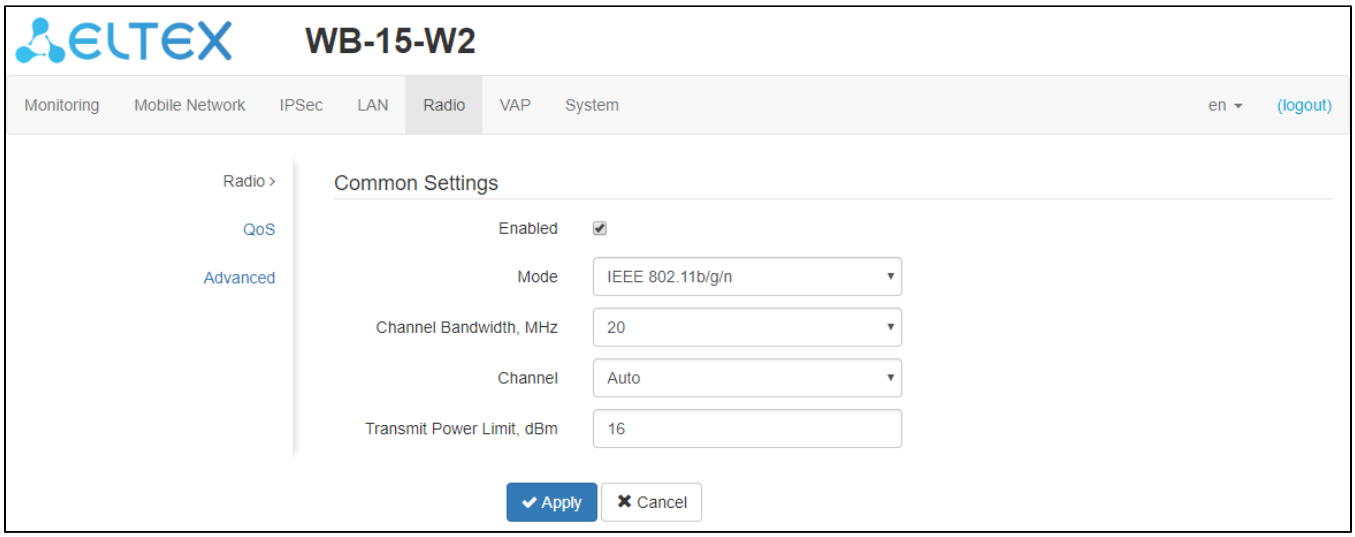
where Enterprise – 1.3.6.1.4.1.35265.1.56 is Eltex Enterprise identifier.
To apply a new configuration and save setting to non-volatile memory, press «Apply». Press «Cancel» to discard the changes.

The «Radio» menu

In the «Radio» menu you can configure the wireless interface

The «Radio» submenu

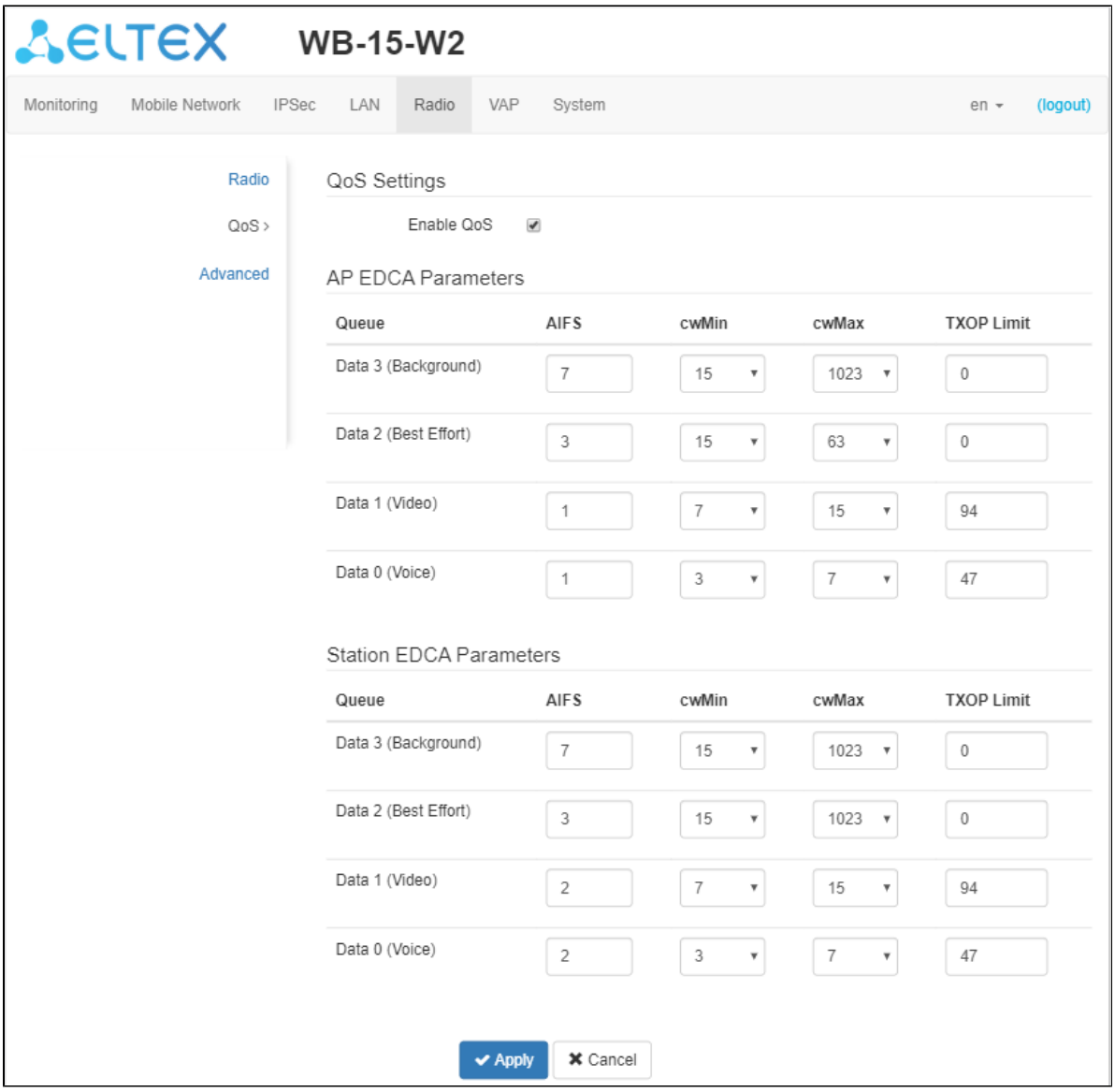
In the «Radio» submenu, you can configure the device's radio interface.



- *Mode* – select interface operation mode:
  - IEEE 802.11b;
  - IEEE 802.11g;
  - IEEE 802.11n;
  - IEEE 802.11b/g;
  - IEEE 802.11b/g/n;
- *Channel Bandwidth, MHz* – bandwidth of the channel on which the radio interface of the device operates, takes values 20, 40;
- *Primary Channel* – primary channel of the radio interface. The setting is available when you select a bandwidth of 40 MHz - in this case, the total channel of 40 MHz is formed from two adjacent frequency channels of 20 MHz. The choice of the main channel is determined by the position relative to the additional:
  - Upper – the frequency of the main channel is higher than the frequency of the additional;
  - Lower – the frequency of the main channel is lower than the frequency of the additional;
- *Channel* – select channel for data transmission;
- *Transmission Power Limit, dBm* – transmitting Wi-Fi signal power adjustment, dBm.

The «QoS» submenu

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

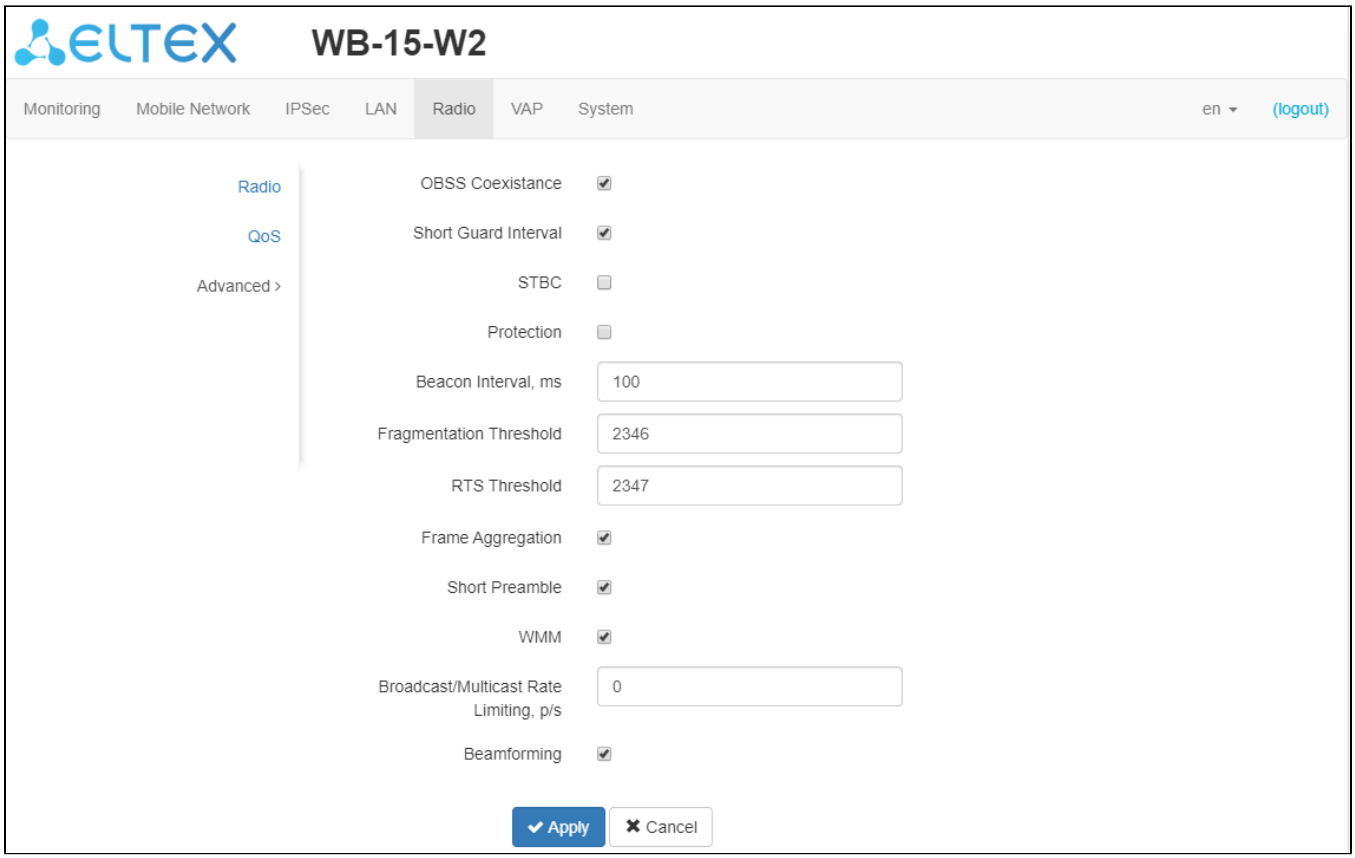


- *Enable QoS* – when the flag is set, the setting of Quality of Service functions is available;
- *AP EDCA parameters* – access point settings table (traffic is transmitted from the access point to the client):
  - *Queue* – predefined queues for various kinds of traffic:
    - *Data 3 (Background)*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

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

The «Advanced» submenu

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



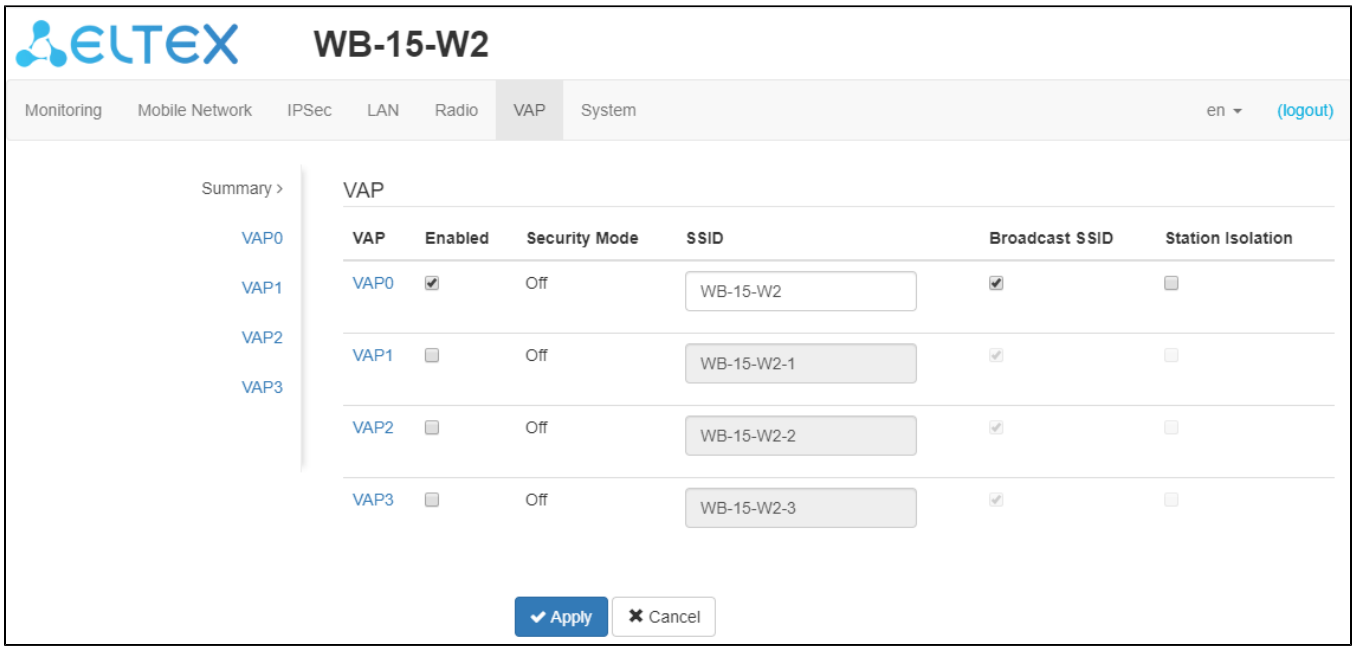
- *OBSS Coexistance* – automatic change of channel width when the air is busy;
- *Short Guard interval* – support for Short Guard interval. Access point transmits data using 400 ns Guard interval (instead of 800 ns) to clients which also support Short GI;
- *STBC* – Soace-Time Block Coding method dedicated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

The «VAP» menu

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

The «Summary» submenu

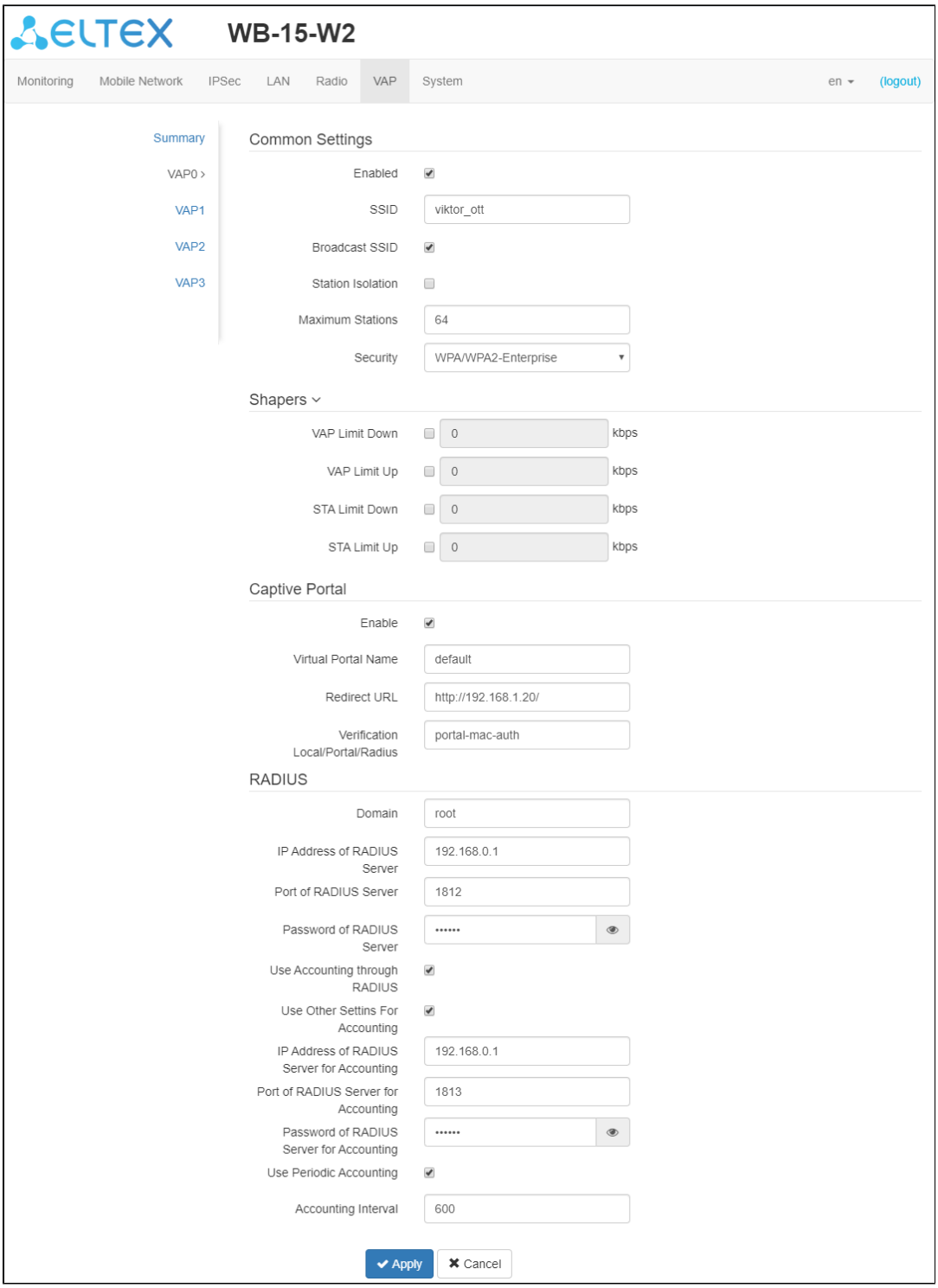
The «Summary» submenu displays the settings of all virtual Wi-Fi APs (VAP). You can see the settings of each virtual AP in sections VAP0..3.



- *VAP0..3* – the sequence number of the virtual access point;
- *Enabled* – when the flag is set, VAP is enabled; otherwise, it is disabled;
- *Security Mode* – the type of data encryption used on VAP;
- *SSID* – virtual wireless network name;
- *Broadcast SSID* – when checked, SSID broadcasting is on, otherwise it is disabled;
- *Station Isolation* – when checked, station isolation from each other within the same VAP is enabled.

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

The «VAP» submenu



Common Settings:

- *Enabled* – when checked, the virtual access point is enabled, otherwise it is disabled;
- *SSID* – virtual wireless network name;
- *Broadcast SSID* – when checked, SSID broadcasting is on, otherwise it is disabled;
- *Station Isolation* – when checked, station isolation from each other within the same VAP is enabled;
- *Maximum Stations* – the maximum number of clients connected to the virtual network;
- *Security* – security mode for wireless network:
  - *Off* – do not use encryption for data transfer. The access point is available for any subscriber to connect;
  - *WPA, WPA2, WPA/WPA2* – encryption methods, if you select one of the methods, the following setting will be available:
    - *WPA Key* – key/password required to connect to the virtual access point. The key lenght is from 8 to 63 symbols.

Shapers:

Show – display configuration field;

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

Captive Portal:

- *Enable – activates the portal authorization settings field;*
- *VirtualPortal Name* – captive portal name;
- *Redirect URL* – field to enter the URL to which the redirection will be made;
- *Verification Local/Portal/Radius* – method of authorization on the portal.

RADIUS:

- Domain – user domain;
- RADIUS server IP address;
- RADIUS server port;
- RADIUS server password;
- Use Accounting through RADIUS – when checked, «Accounting» messages will be sent to the RADIUS server.

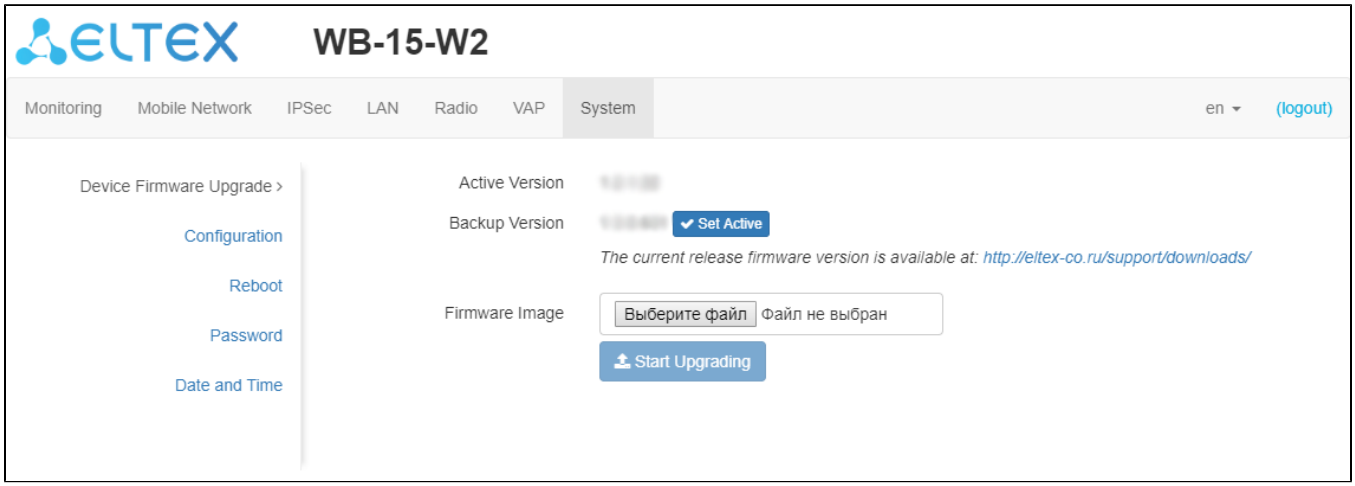
To apply a new configuration and save setting to non-volatile memory, press «Apply». Press «Cancel» to discard the changes.

The «System» menu

In the «System» menu you can configure system, time, change password and update device firmware.

The «Device Firmware Upgrade» submenu

The «Device Firmware Upgrade» submenu is intended for upgrading the device's firmware.



- *Active Version of Firmware* – installed firmware version, which is operating at the moment;
- *Backup version* – installed firmware version which can be used in case of problems with the current active firmware version;
  - *Set active* – the button which allows you to set a backup file active. The device reboot is required. The active firmware version will not be set as a backup.

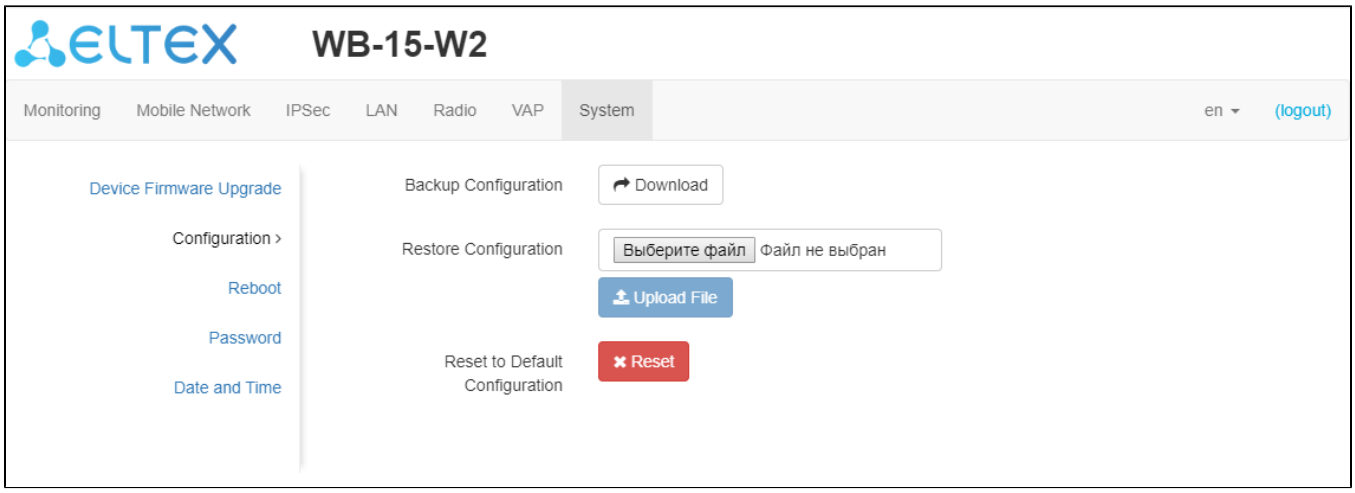
Firmware update

Download the firmware file from *https://eltex-co.com/support/downloads/* and save it on your computer. To do this, click the «Choose file» button in the *Firmware Image* field and specify the path to the firmware file in .tar.gz format.
To start the update process, you must click the «Start Upgrading» button. The process may take several minutes (its current status will be shown on the page). The device will be automatically rebooted when the update is completed.

> Do not switch off or reboot the device during the firmware update.

The «Configuration» submenu

In the «Configuration» submenu, the current configuration is saved to a file and the configuration is downloaded to the device.



Backup Configuration

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

Restore Configuration

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

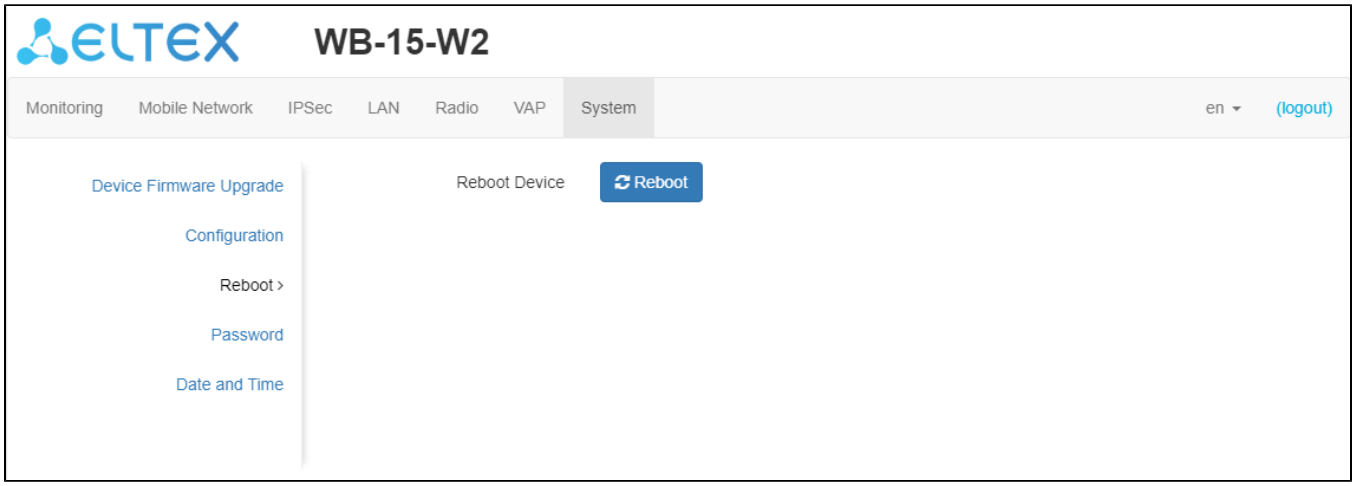
Note that all the passwords of configuration are encrypted with a key depending on device MAC address. When uploading a configuration from one device to another, you first need to reset the passwords, or change them in the configuration file before downloading to the device (encrypted fields).

Reset to Default Configuration

To reset all the settings to default values, press «Reset» button.

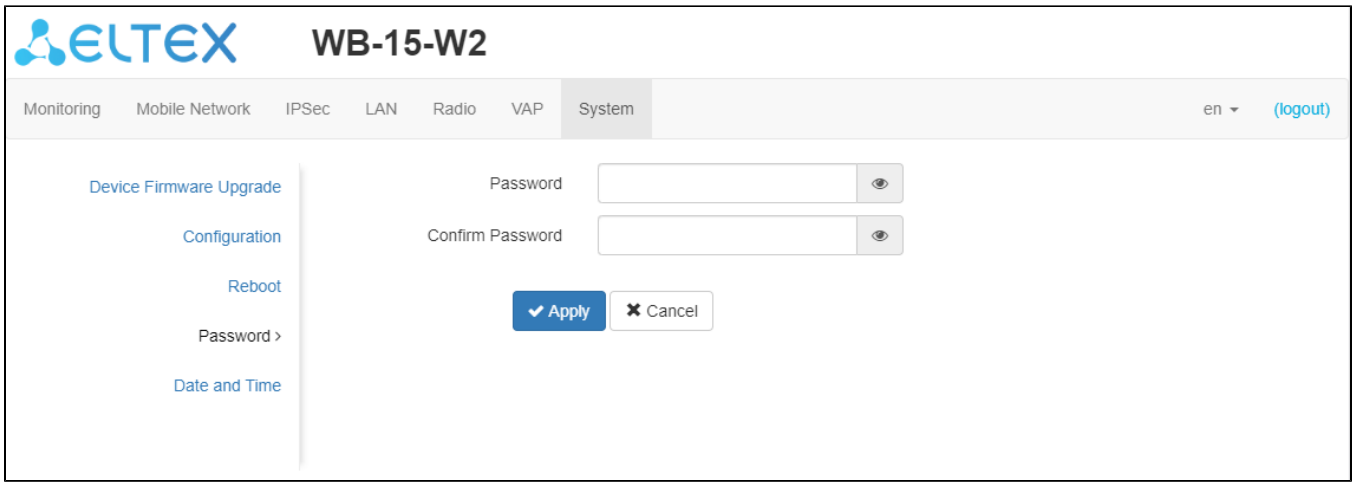
The «Reboot» submenu

To reboot the device, click on the «Reboot» button.



The «Password» submenu

When signing into web interface, administrator (default password: **password**) has the full access to the device: read/write any settings, full device status monitoring.
To change the password, enter the new password first in the «Password» field, then in the «Confirm Password» field and click the «Apply» button to save the new password.



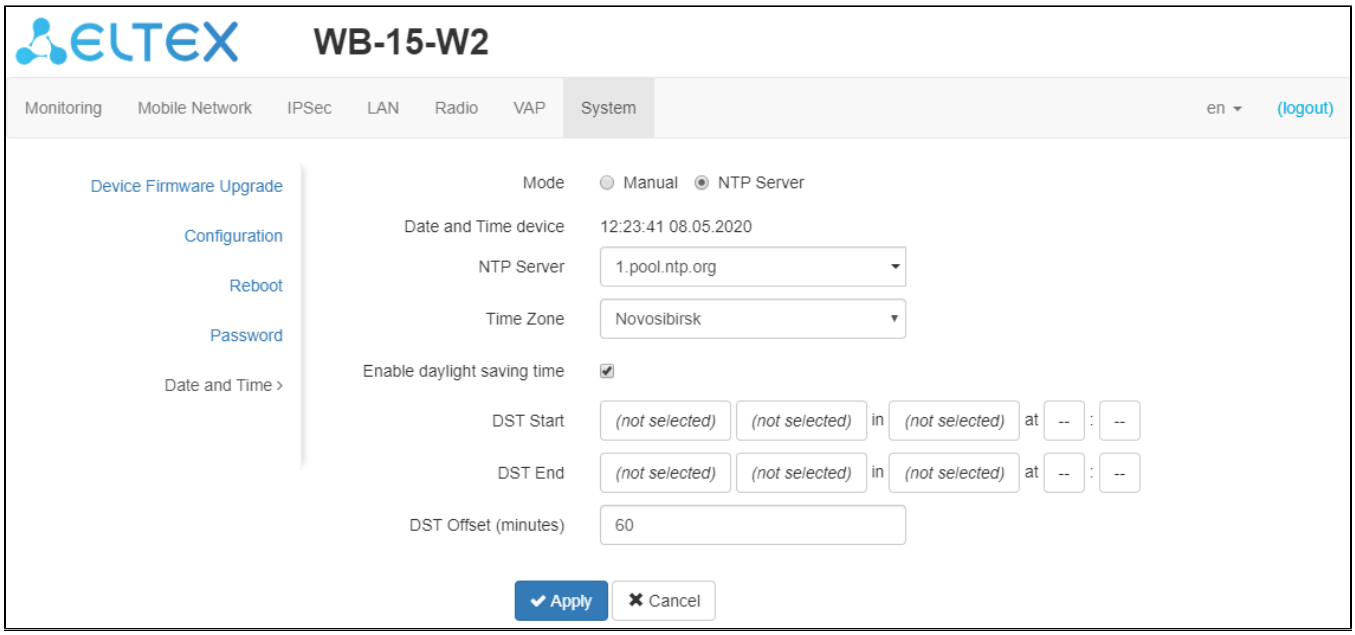
The «Date and Time» submenu

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

Manual:

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

NTP Server:



- *Date and Time device* – date and time currently displayed;
- *NTP Server* – time synchronization server IP address/domain name;
- *Time Zone* – allows to set the timezone according to the nearest city for your region from the list;

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

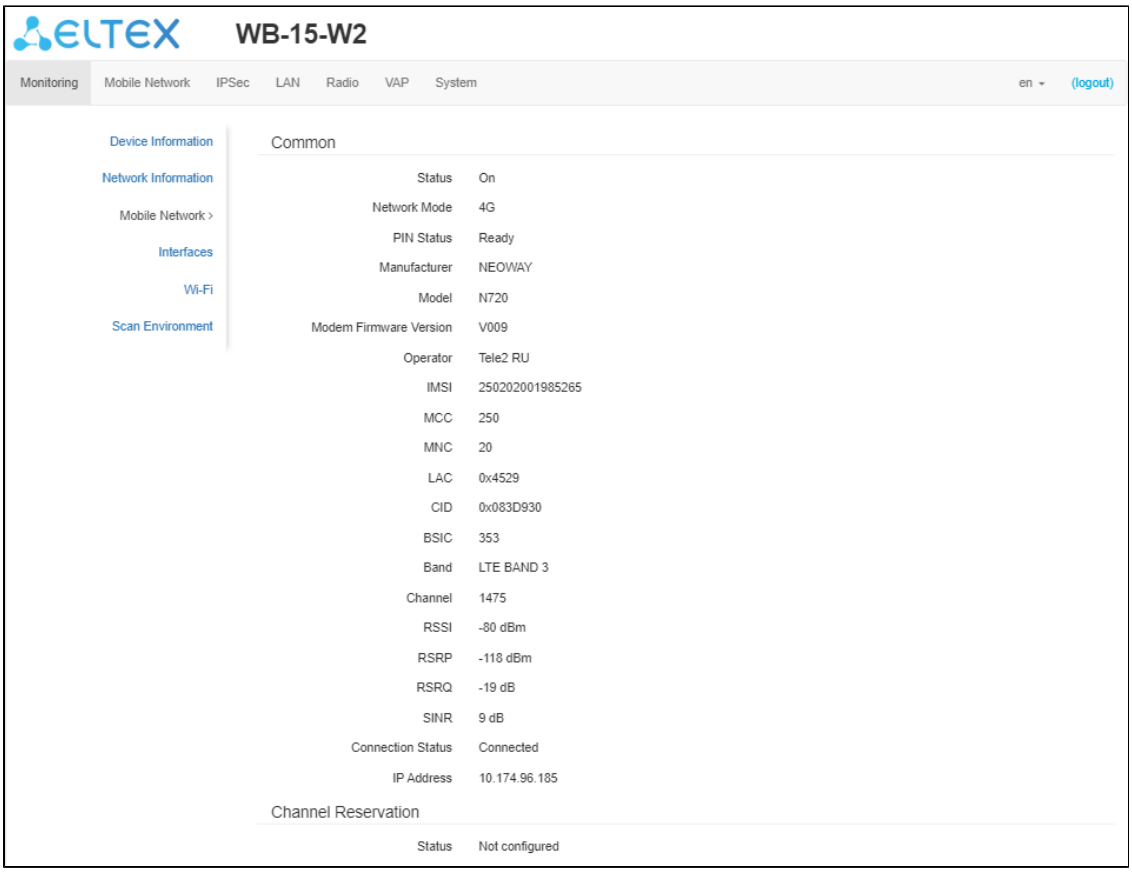
1. Connect the PC to the LAN port of the injector (when the device is powered by Passive PoE 24 V), or directly to the Ethernet port of the device (if the device is powered from the DC 9-36V unit);

2. In the address bar of the browser, enter the IP address of the device (default is 192.168.1.1). On a PC, you need to either enable obtaining addresses via DHCP, or set a static IP from the 192.168.1.0/24 subnet;

3. When connection is established successfully, the window with Login and password fields will be displayed. Fill the filds and press «Log in». (By default, login: **admin**, password: **password**).

If the window is not displayed, make sure that the PC and the device are in the same subnet.

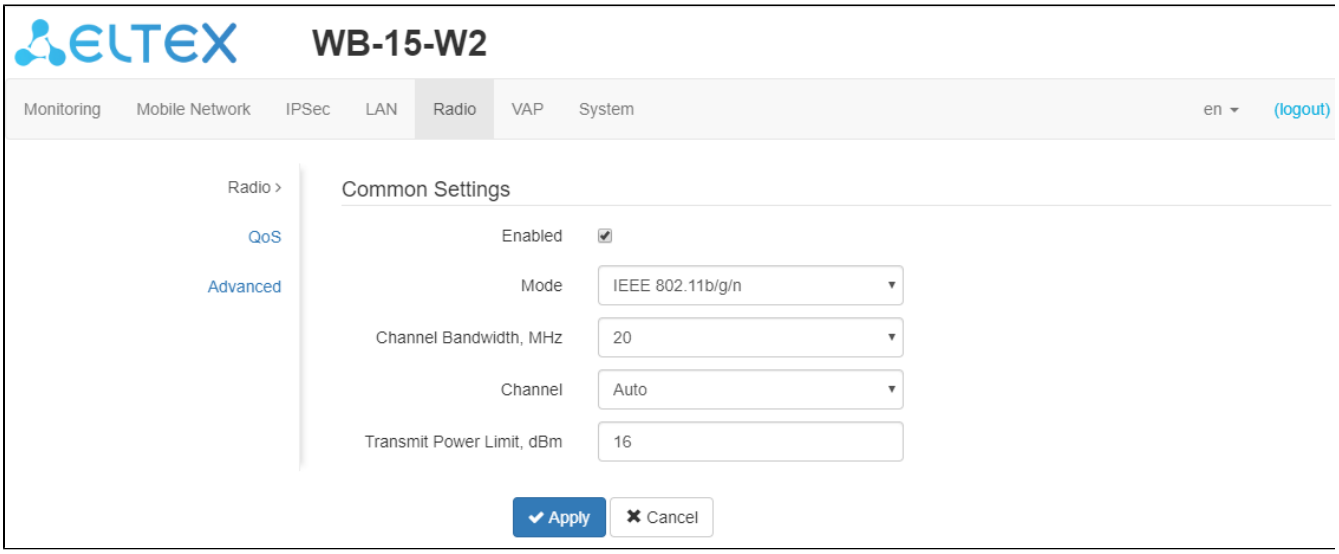
4. After connecting the device to the mobile network (1-2 minutes after loading the device, if there is a SIM card in the SIM1 slot), the Monitoring -> Mobile Network menu will display information about the network connection mode, mobile network operator, IMSI of the current SIM card etc. Also, the status LED will turn green.



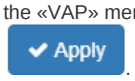
Please note that for the device to automatically connect to the mobile network, a SIM card must be inserted into the device before power is supplied to it.

From this moment, the device has access to the Internet and can provide services to customers. For further tuning, go to the «Radio» menu.

5. In the «Radio» menu, set the desired Wi-Fi network operation mode (preferably b/g/n), channel width, frequency channel number, radiation power.

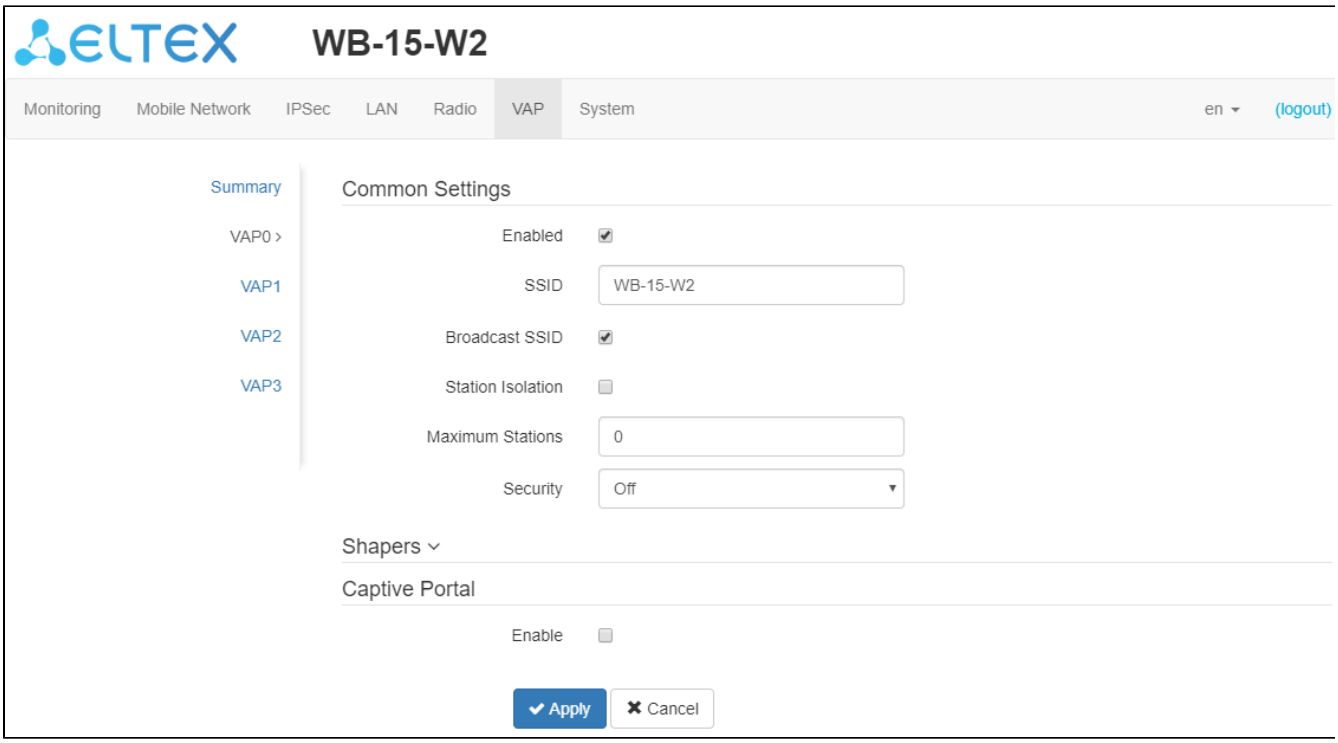


To configure VAP settings, go to the «VAP» menu.

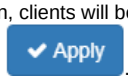
To save and apply changes click 

.

6. In the «VAP» menu, go to one of the four VAPs, turn it on, configure the settings necessary for connecting clients (SSID, security mode, security key, restriction of connected clients).



After completing the configuration, clients will be able to connect to VAP and gain access to the Internet.

To save and apply changes click 

.

7. To prevent unauthorized access to the device, after making the settings, go to the «System» menu and in the «Password» tab, change the default password value.

To save and apply changes click 

.

Radar

Configuration example

Radar configuration

```
WB-15-W2(root):/# configure
WB-15-W2(config):/# interface
WB-15-W2(config):/interface# wlan1
WB-15-W2(config):/interface/wlan1/wlan# radio
WB-15-W2(config):/interface/wlan1/wlan/radio# monitor
WB-15-W2(config):/interface/wlan1/wlan/radio/monitor# uplink-interface usb0:ipsec
WB-15-W2(config):/interface/wlan1/wlan/radio/monitor# url http://X.X.X.X (where http://X.X.X.X – address of the server where the messages from the monitor will be forwarded to)
WB-15-W2(config):/interface/wlan1/wlan/radio/monitor# enabled true
```

Configuration of ap-location to determine the geographical location of the access point

```
WB-15-W2(config):/system
WB-15-W2(config):/system# ap-location location
```

Parameters description

Parameter	Description
enabled	enable monitor mode
mode	• **mac** – macro address list issuance mode; • **tzsp** – remote capture via TZSP.
url	URL of the server for uploading macros via HTTP. Used only if mode = mac
server-ip	the IP address of the server to transmit TZSP traffic. Used only only if mode = tzsp
channel-time	channel scan time. Used if fixed-channel = false
allow-broken-packets	allows the analysis of packages received with errors
capture-beacons	select the traffic reception mode. Either take beacons or everything else.
fixed-channel	the parameter defines whether switching will be performed on all channels (taking into account limit-channels) or will listen only to the currently configured channel
uplink-interface	the name of the interface through which we will communicate with the server part. The parameter must always be defined
send-interval	periodicity of sending MAC address table to the server. Used only if mode = mac
max-macs	the maximum size of the MAC address table. Used only if mode = mac
mac-sources	a bit mask to filter the types of packets for which a macro address table is formed. Used only if mode = mac: • Bit 0 - Probe Req • Bit 1 - Assoc Req • Bit 2 - other types of traffic (mainly data) I.e. if mac-sources = 1 we will track only probe req, if mac-sources = 2 we will track only assoc req, if mac-sources = 7 we will track all three types of packages.

Radar configuration example

"monitor":{
"enabled":"false",
"mode":"mac",
"url":"http:\/\/172.16.0.16\/",
"server-ip":"172.16.0.16",
"packet-length":"252",
"channel-time":"1000",
"allow-broken-packets":"true",
"capture-beacons":"false",
"fixed-channel":"true",
"uplink-interface":"usb0:ipsec",
"send-interval":"1",
"max-macs":"1000",
"mac-sources":"7"
}

GPS

Information on the current location of the device (in the form of coordinates width, longitude) is displayed in the «GPS» submenu. To obtain this information, you need to connect an external GPS antenna to the device.

Configuration of GPS via CLI

```
WB-15-W2(root):/# configure
WB-15-W2(config):/# geolocation
WB-15-W2(config):/geolocation# workmode gps
```

You can view the received data with a command:

```
WB-15-W2(config):/# monitoring location-info
```

The list of changes

Document version	Issue date	Revisions
Version 1.0	28.02.2020	First issue
Firmware version 1.2.1		