User station

WB-2P-LR5

User manual
Firmware version 2.1.0

IP address: 192.168.1.1
Username: admin
Password: password

Contents

1 Introduction 5
1.1 Symbols 5
2 Device description 6
2.1 Purpose 6
3 Device specifications 7
3.1 Main technical parameters 9
3.2 Design 11
3.3 Light indication 12
3.4 Reset to factory settings 13
3.5 Supply package 13
4 Installation rules 14
4.1 Safety rules 14
4.2 Installation recommendations 14
4.3 WB-2P-LR5 mounting 14
4.3.1 Pre-tuning 14
4.3.2 Mounting algorithm 14
4.4 Switching on 16
5 Managing the device through web configurator 18
5.1 Getting started 18
5.2 Changing user 19
5.3 Web interface operation modes 19
5.4 Applying configuration and discarding changes 20
5.5 Fast configuration mode (tiles) 21
5.5.1 Internet 21
5.5.2 Wi-Fi Client 22
5.5.3 IPTV 23
5.5.4 System 23
5.6 Advanced settings (preferences) 23
5.6.1 Main elements of the web interface 23
5.6.2 «Network» menu 24
5.6.2.1 «Internet» submenu 24
5.6.2.2 «WDS» submenu 28
5.6.2.3 «Radiointerface» submenu 29

5.6.2.4 DHCP server settings 30
5.6.2.5 «MAC Management» submenu 32
5.6.2.6 «Local DNS» submenu 33
5.6.2.7 «NAT and Port Forwarding» submenu 33
5.6.2.8 «Firewall» submenu 35
5.6.2.9 «Routes» submenu 36
5.6.2.10 «Dynamic DNS» submenu 38
5.6.2.11 «SNMP» submenu 39
5.6.3 «IPTV» settings 40
5.6.4 «System» menu 41
5.6.4.1 «Time» submenu 41
5.6.4.2 «Access» submenu 42
5.6.4.3 «Log» submenu 43
5.6.4.4 «Passwords» submenu 44
5.6.4.5 «Configuration management» submenu 45
5.6.4.6 «Firmware Upgrade» submenu 46
5.6.4.7 «Reboot» submenu 47
5.6.4.8 «Autoprovisioning» submenu 47
5.6.4.9 «Advanced» submenu 50
5.7 System monitoring 51
5.7.1 «Internet» submenu 51
5.7.2 «WDS» submenu 51
5.7.3 «Ethernet ports» submenu 52
5.7.4 «DHCP» submenu 53
5.7.5 «ARP» submenu 53
5.7.6 «PPPoE Relay» submenu 54
5.7.7 «Device info» submenu 55
5.7.8 «Conntrack» submenu 56
5.7.9 «Routes» submenu 57
6 Configuration example 58
7 Device automatic update algorithm based on DHCP 60
8 System recovering after firmware update failure 63
9 Application A. Launch user script when starting the system 64
10 Application B. Antenna patterns 65

1 Introduction

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 a short time from unstable low-speed communication networks of low radius to broadband networks equitable to speed of wired networks with high criteria for the quality of provided services.

WB-2P-LR5 is a user station designed for connection to Wi-Fi access network which might be constructed using base stations within long distances.The case of WB-2P-LR5 is sealed, that is allows to install the device outdoor with different climate conditions.

This manual specifies intended purpose, main technical parameters, design, installation procedure, safe operation rules and installation recommendations for WB-2P-LR5.

1.1 Symbols

Notes and warnings

Notes contain important information, tips or recommendations on the 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

User station WB-2P-LR5 (herein after «the device») is designed for access provision to secure wireless network. The device provides access to up-to-date interactive services: Internet, IPTV, VoIP. WB-2P-LR5 connects to a base station via Wi-Fi technology and operates at 5 and 6 GHz (the frequency range – 5830–6150 MHz – is supported on WB-2P-LR5 rev.B). The device is supposed to operate with WOP-2ac-LR5. WB-2P-LR5 might be also used for wireless bridge organization. WB-2P-LR5 supports up-to-date requirements to service quality and allows transmitting more important traffic in higher priorities queues. Prioritization is based on QoS technologies: CoS (special tags in VLAN packet field) and ToS (tags in IP packet field).

The device is capable to operate in wide temperature range and in high-humidity conditions (parks, factories, stadiums, etc.).

Power to the device is supplied via PoE technology 24V.

3 Device specifications

Interfaces :

- LAN: 1 port Ethernet RJ-45 10/100/1000BASE-T;
- WLAN: IEEE 802.11a/n/ac;

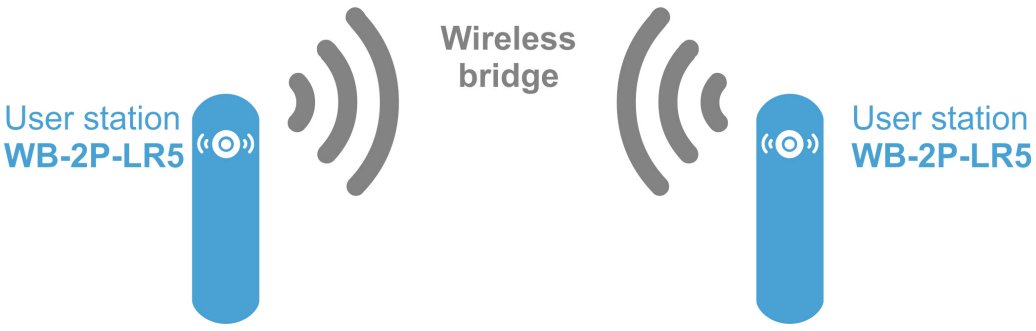
The power is supplied via PoE injector 24V connected to 220V network.

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

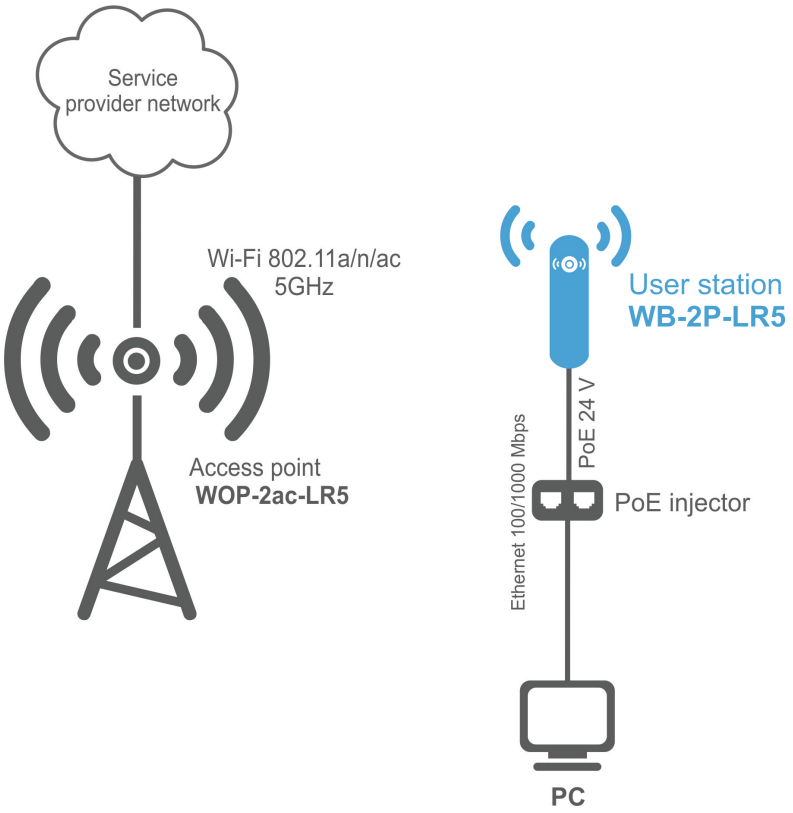
Network functions :

- operating in bridge and router modes;
- operating in «Wi-Fi Station» and «Wireless bridge» modes;
- support for VLAN Trunk;
- support for Management VLAN;
- support for General VLAN;
- static routing;
- support for Transparent wireless bridge function;
- time synchronization via NTP;
- support for static address and DHCP (DHCP client on WAN side, DHCP server on LAN side);
- support for DNS;
- support for D-DNS;
- support for NAT;
- support for UPnP;
- firewall;
- support for cloning of MAC address on WAN interface;
- support for quality of service mechanisms (QoS through DSCP and 802.1P).
- support for IPTV functions (IGMP-proxy, UDP-to-HTTP proxy);
- firmware update via web interface;
- support for DHCP-based autoprovisioning;
- support for TR-069;
- remote monitoring and configuration: web interface, Telnet, SSH.

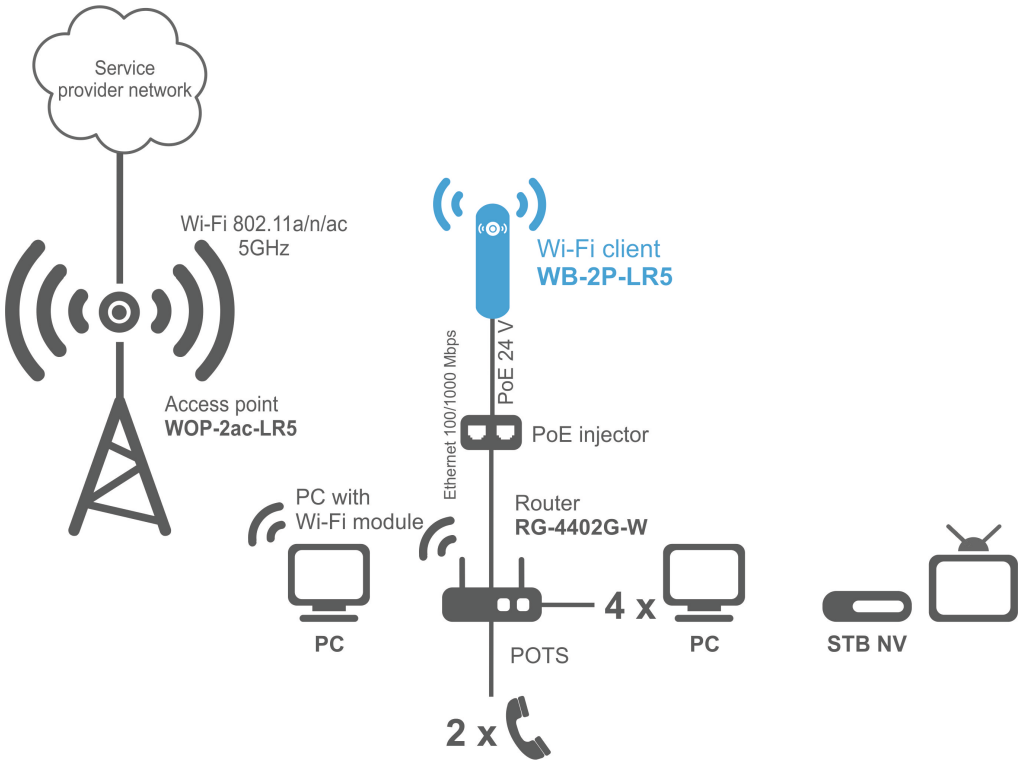
The figures below illustrate applications schemes of WB-2P-LR5.



Functional scheme of using WB-2P-LR5 for wireless bridge organization



Functional scheme of using WB-2P-LR5 without router



Functional scheme of using WB-2P-LR5 with router

3.1 Main technical parameters

LAN Ethernet interface parameters	
Number of ports	1
Connector	RJ-45
Data rate, Mbps	10/100/1000, auto-negotiation
Standards	BASE-T
Parameters of the wireless interface	
Standards	802.11a/n/ac
Frequency range, MHz	5180–5825 MHz 5180-6150 MHz (for WB-2P-LR5 rev.B)
Modulation	BPSK, QPSK, 16QAM, 64QAM, 256QAM
Data rate, Mbps	**802.11a:** up to 54 Mbps **802.11n:** up to 300 Mbps **802.11ac:** up to 867 Mbps
Maximum output power of the transmitter	**5–6 GHz:** up to 24 dBm
Receiver sensitivity	**MCS0:** -93 dBm **MCS7:** -73 dBm
Security	64/128/152- bit WEP encryption, WPA/WPA2, centralized authorization via RADIUS server (WPA/WPA2 Enterprise)
Antenna's parameters	
Gain	2x12 dBi
Polarization	dualpolarized antenna
Beam angle (horizontal polarization)	60°
Beam angle (horizontal polarization)	15°
SWR	2.0:1
I mpedance	50 Ohm
Front to back ratio	> 20 dB

Management	
Remote management	Web interface, Telnet, SSH, SNMP, TR-069
Access restriction	by password
General parameters	
Processor	Realtek RTL8197FS 1 GHz
RAM	128 MB
Flash	32 MB
Power supply	PoE 24 V
Power consumption	no more than 8 W
Operating temperature	from -45 to +65°C
Operating humidity	up to 95%
Ingress Protection Marking	IP54
Dimensions	80x66x282 mm
Weight	0.35 kg

3.2 **Design**

WB-2P-LR5 housed in a plastic case, industrial version. The size of the device: 80x66x282 mm.

The layout of WB-2P-LR5 is shown in the figure below.



WB-2P-LR5 layout

LAN port 10/100/1000Base-T (RJ-45 connector) for local network connection and power supply via PoE and the button for resetting to factory settings («Reset») are located on the bottom panel of the device.



WB-2P-LR5 bottom panel's elements

3.3 Light indication

The light indication panel of WB-2P-LR5 is shown below.



WB-2P-LR5 light indication panel

The current state of the device is shown with the help of light indicators located on the back panel of WB-2P-LR5. The list of indicators and their description is shown in the table below.

Indicator		Indicator's status	Description
	Power – power and operation status indicator	solid green	the device power supply is enabled, normal operation
		solid orange	the device is loaded but IP address is not received via DHCP
		solid red	the device is loading
	LAN – LAN interface indicator	solid green (10, 100 Mbps)/ solid orange (1000 Mbps)	the channel between LAN interface of WB-2P-LR5 and connected device is active
		flashes	packet data transmission between LAN interface of WB-2P-LR5 and connected device
	WLAN – received signal strength indicator (RSSI)	solid red	the deice is connected to a base station. The base station signal level is more than -99 dBm
		solid yellow	the deice is connected to a base station; the base station signal level is more than -80 dBm
		solid green	the deice is connected to a base station; the base station signal level is more than -70 dBm
		solid green	the deice is connected to a base station; the base station signal level is more than -60 dBm
		none of the indicators is on	the device is not connected to the base station

3.4 Reset to factory settings

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

1. Using «Reset» button on the device. When the device is loaded, press and hold «Reset» button located on the bottom panel (approximately 10–15 seconds) until «Power» indicator is flashing orange.
2. Using PoE injector supplied with the device. When the device is loaded, press and hold «RST» button of the injector (approximately 10–15 seconds) until «Power» indicator of WB-2P-LR5 is flashing orange.
   The device will be rebooted automatically. DHCP client will be launched according to factory settings. If the address is not obtained via DHCP, the device will have the following address — *192.168.1.1*, and the following netmask — *255.255.255.0*. Username/password to access the web interface are admin/password.

3.5 Supply package

The basic supply package of WB-2P-LR5 includes:

- User station WB-2P-LR5;
- Mounting kit: 2 clamps for attaching;
- PoE injector 24 V;
- Patch cord RJ-45, 1.5 m;
- Cord for europlug - C13-F-1.8 m;
- Sheet with light indication description;
- Conformity certificate;
- Technical passport.

A bracket with horizontal and vertical adjustment might be included to the supply package upon a request.

4 Installation rules

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

4.1 Safety rules

1. Do not open the case of the device. There are no user serviceable parts inside.
2. Do not install the device during storm. There is a risk of lightning stroke.
3. Adhere requierements for voltage, current and frequency mentioned in the manual.
4. Ground measuring instruments and computer before connecting to WB-2P-LR5. 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. During the high-rise operation, all the requirements and safety rules for high-rise operations should be complied.
7. The maintenance of the device should be implied by engineers who have undergone special training.
8. Only properly functioning equipment should be connected to the device.

4.2 Installation recommendations

1. Recommended location for device installation: communications mast/pole.
2. Before you install and enable the 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 or pole in the way that the LAN port is pointed down.
4. In order to provide better receiving signal level, the sectoral antenna of a base station should be in line of sight of WB-2P-LR5.
5. You may achive the highest signal level by antenna alignment with the help of RSSI indicators.
6. The transmitting part of the device is located on the other side from brackets. This area should be directed to base station sectoral antenna.

After installing, the acceptable level of the received signal from the base station is -65 ÷ -70 dBm. Increasing this level up to -75 dBm is permitted if it does not involve the use of VoIP, streaming video and other traffic that is sensitive to losses in a wireless network.

Install the device on communications mast/pole so that the device is directed to base station sectoral antenna. The LAN port should be pointed down.

4.3 WB-2P-LR5 mounting

4.3.1 Pre-tuning

Before installing, proceed pre-tuning of the device (see section Configuration example). For this, power on the device (paragraph 2-7, section Mounting algorithm) and follow the instructions given in the section Configuration example. Make sure that the user station connects required wireless network: RSSI indicators should be on.

4.3.2 Mounting algorithm

1. Install the device on communications mast/pole pointing LAN 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.



2. Remove the bottom cover which close LAN-port.



3. Connect Ethernet cable to LAN port.



4. Close the bottom cover.

5. Connect Ethernet cable connected to WB-2P-LR5 to PoE port of injector.



6. Connect Ethernet cable of your LAN network or PC to LAN port of PoE injector.



7. Connect PoE injector to 220V socket with the help of power line cord.



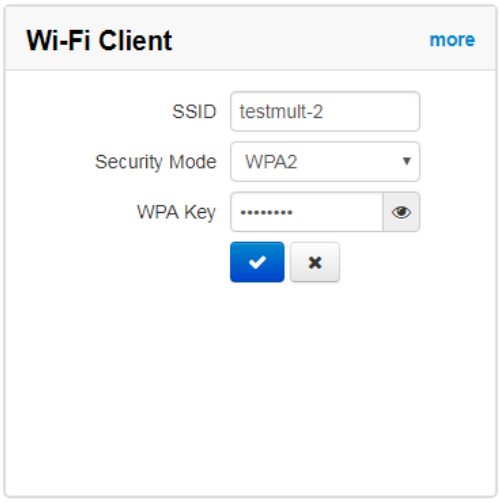
8. Align the position of the device for best signal level receiving. The level of received signal is shown by the indication located on the back panel of the device.
9. Fasten the clamps.

4.4 Switching on

1. Plug the injector into 220 V outlet. Connect a PC to LAN port of the injector.
2. WB-2P-LR5 loads in a minute after switching on. Connect to the web configurator of WB-2P-LR5 through a browser.

> **IP address by default: 192.168.1.1.**
> **Login: *admin*, password: *password*.**

3. Enter the following in Wi-Fi Client tab:
    - SSID of the base station;
    - Authorization type;
    - Authentication data: login and password if required.



Press  to apply the settings.

5 Managing the device through web configurator

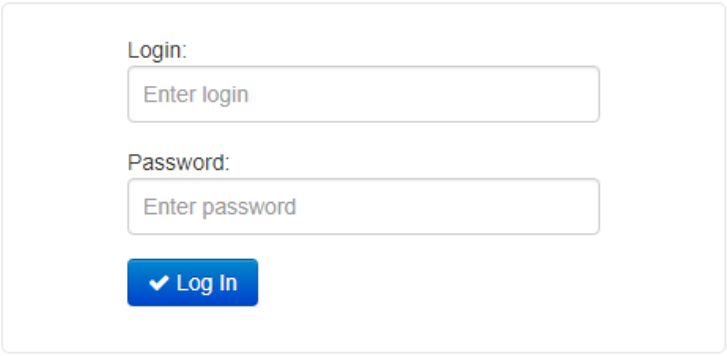
5.1 Getting started

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.

> IP address by default: 192.168.1.1, subnet mask: 255.255.255.0. The device is capable to obtain an IP address via DHCP.

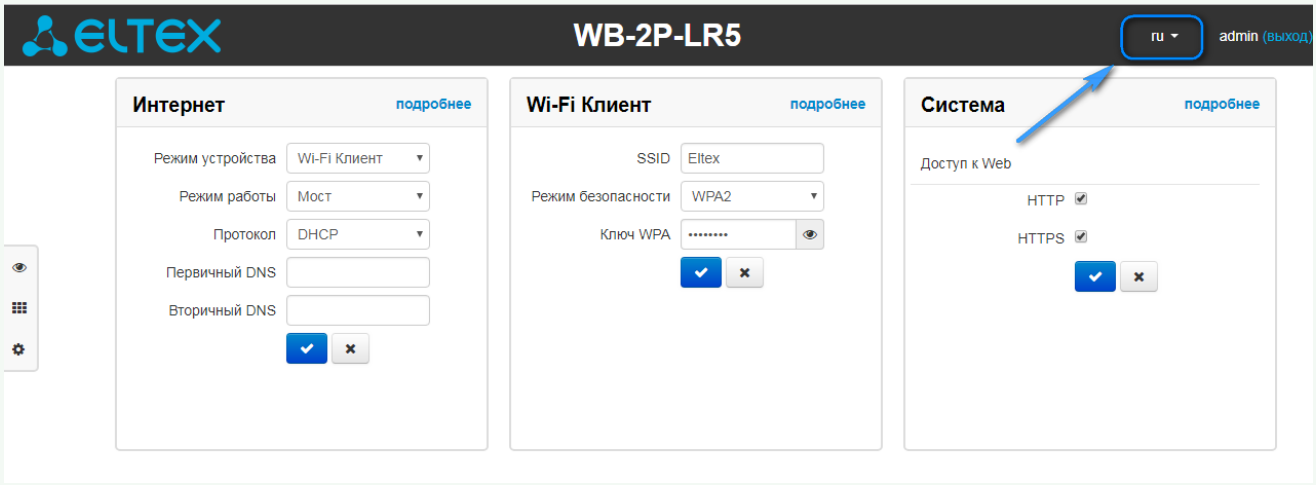
If connection is successful, request form with user name and password will be displayed on a browser window.



> By default: login: *admin*, password: *password*.

3. Enter the login in the *"Login"* line and password in the "*Password*" line.
   Click *"Logon"* button. Device Web configurator home page will be opened in the browser window.

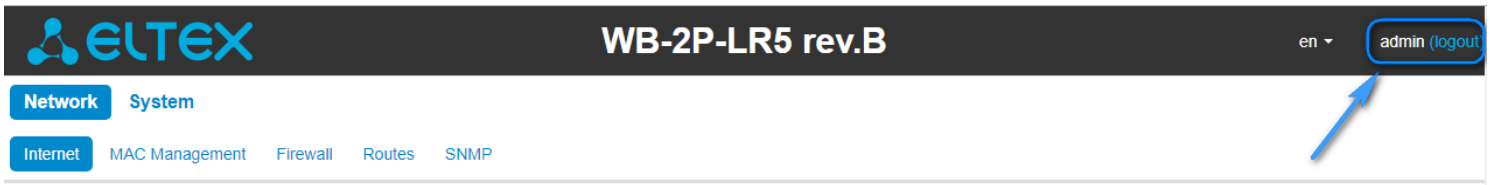
> You may select languages on the top-right of the page. Russin and English languages are available.



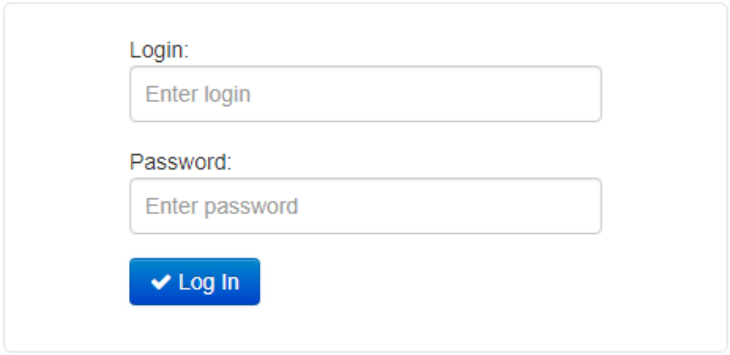
5.2 Changing user

There are three types of users: **admin**, **user** and **viewer**:

- **admin** (password by default: **password**) has complete access to the device: reading and writing of all the setting, full monitoring for the device status.
- **user** (password by default: **user**) has the opportunity to implement only Wi-Fi configuration, does not have access to monitoring.
- **viewer** has rights to view the configuration without access to editing, full monitoring is available.



Press *«logout»* to complete the current user session. The authentication window will be displayed:



To change a user account, enter the corresponding login and password and press *«Log in»*.

5.3 Web interface operation modes

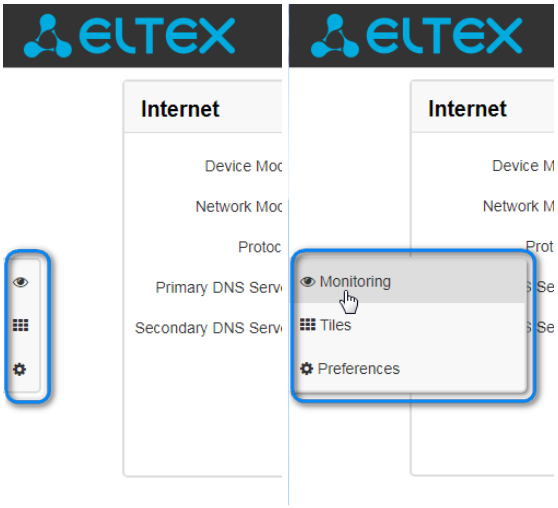
Web interface of WB-2P-LR5 operates in three modes:

- **Monitoring** – system monitoring mode. The mode is used for different device data monitoring: Internet connection status, amount of received/transmitted data via network interfaces, etc.
- **Tiles** – fast system configuration mode. Each tile contains settings according to functional purpose: Internet, Wi-Fi Client, Wireless bridge, IPTV, System. Only main parameters are displayed on tiles, it allows you to configure required function rapidly.

  «Wireless bridge» tile is displayed when operating in the corresponding mode. Choose «Wireless bridge» mode on the «Internet» tile and press .
  «IPTV» tile is displayed when operating in «Router» mode. Choose «Router» mode on the «Internet» tile and press .

- **Preferences** – advanced system configuration mode (full configuration mode). It allows you to configure main and additional parameters of the device.

To navigate among the modes, use the left panel of the web interface. Point the panel with the mouse cursor, panel will expend:



You may move from the «Tiles» mode to «Preferences» by clicking «more» link next ro the tiles names.

5.4 Applying configuration and discarding changes

1. Applying configuration

> Press «Apply» to save configuration to flash memory and apply new settings. All the settings come into operation without device rebooting.

The visual indication of the settings applying is realized in the web interface.
The visual indication of the settings applying:

Image	State description
Time	After pressing «Apply», the process of settings saving to device memory is launched. The mark next to the tab name and on «Apply» button means the process of saving setting.
Time	If the setting are saved successfully, the mark will be displayed next to the tab name and on «Apply» button.
Настройки сети	If any parameter value have been set incorrectly, the error notification with description will be displayed after pressing «Apply» button. The mark will be displayed next to the tab name and on «Apply» button.

«Apply» button in tiles and preferences modes appears as follows: ; Apply.

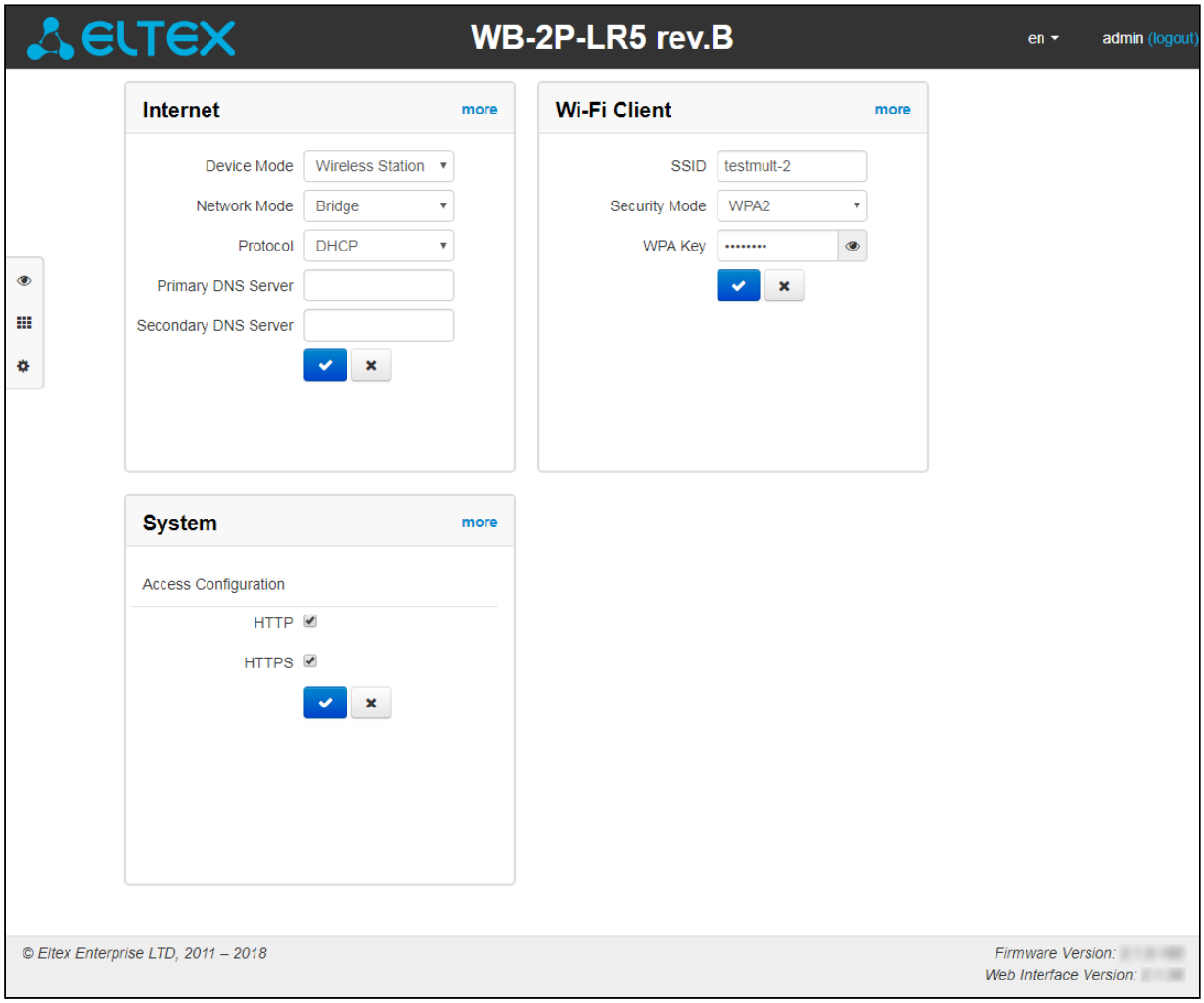
2. Discarding changes

> 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. You will not be able to return to previous configuration after pressing «Apply».

The button for discarding changes in tiles and preferences mode appears as follows: ; Cancel.

5.5 Fast configuration mode (tiles)

Only main settings are displayed in fast configuration mode (tiles)



The settings are divided into the following categories:

- *Internet* – fast configuration of Internet settings;
- *Wi-Fi Client* – wireless connection configuration (for Wi-Fi Client (Wireless Station) mode);
- *IPTV* – device configuration for IPTV support (only for Router);
- *System* – system parameters configuration (access to the device, time synchronization, etc.).

5.5.1 Internet

For access to the Internet, you should set main settings in «Internet» tile. For additional parameters configuration, press «more» link.

- *Device mode* – device connection mode:
  - *Wireless station* – device connection to wireless Wi-Fi network;
  - *Wireless bridge* – association with another device to a wireless bridge via WDS technology.
- *Network mode* – device operation mode:
  - *Router* – router mode between LAN and WAN interfaces (WAN interface is the wireless Wi-Fi interface, LAN is isolated from WAN). The mode is not available in Wireless bridge connection mode.
  - *Bridge* – bridge mode between wired and wireless interfaces of the device.

- *Protocol* – select protocol via which the connection of the device via Wi-Fi interface to service provider network will be implemented:
  - *Static* – operation mode, when IP address and other necessary parameters of WAN interface are set statically (manually). If «Static» is selected, the following parameters will be available to set:
    - *WAN IP* – set IP address of WAN interface of the device in service provider network;
    - *Netmask* – set subnet mask of device's WAN interface in service provider network;
    - *Default Gateway* – address, to which a packet will be transmitted in case the route has not been found in the route table.
  - *DHCP* – operation mode, when IP address, subnet mask, DNS server address, default gateway and other parameters required for operation are obtained from DHCP server automatically. Before obtaining the parameters via DHCP, the access to the device is implemented via the address set in IP address field.
- *Primary DNS server, Secondary DNS server* – IP address of DNS servers. If DNS servers' addresses are not allocated automatically via DHCP, if necessary, set them manually.

For applying a new configuration and saving settings to non-volatile memory, press button. To discard changes, press .

To connect the device to service provider network, inquire service provider about network settings. When static settings are used, select «Static» in «Protocol» field, fill the following fields with the information provided by service provider: IP addres, Netmask, Default Gateway, Primary and Secondary DNS. If devices connected to the service provider network obtain network parameters via DHCP, select «DHCP» in the «Protocol» field and follow the instructions given by service provider for full and correct configuration.

The device operates at bridge mode by default.

5.5.2 Wi-Fi Client

To connect the device to a base station, set main settings in «Wi-Fi Client» tile. To set additional parameters, press «more» link.

- *SSID* – ID of the wireless network to which you need to connect. The maximum lenght of the name – 32 symbols. The name should be entered considering the keyboard register. The parameter may consist of digits, latin letters and symbols «-», «_», «.», «!», «;», «#», although it is forbidden to start with the symbols «! », «;» and «#».
- *Security mode* – select wireless network security mode:
  - *Off* – disable wireless network data encryption, low security.
  - *WEP* – WEP authentication. WEP-key should consist of hexadecimal digits and be of 10 or 26 symbols lenght or it might be a string (a-z, A-Z, 0-9, ~!@#$%^&*()_-+= symbols) with lenght of 5 or 13 symbols. The mode is hidden in the web interface.
  - *WPA, WPA2* – WPA and WPA2 authentication. The key lenght is from 8 to 63 symbols. There following symbols are allowed: a-z, A-Z, 0-9, ~!@#$%^&*()_-+=;:|/?.,<>"`' or space.
  - *WPA, WPA2-Enterprise* – WPA and WPA2 encryption with client authentication via 802.1x. Enter username and password as authentication data.

For applying a new configuration and saving settings to non-volatile memory, press button. To discard changes, press .

5.5.3 IPTV

IPTV tile is displayed only in «Router» mode. Select «Router» mode on «Internet» tile and press .

For IPTV function operation, set parameters on IPTV tile. To configure additional parameters, press «more» link.

- *Enble IPTV* – when checked, IPTV signals broadcasting is enable (from WAN interface of the device to the devices connected to the LAN interface);
- *Enable HTTP Proxy* – when checked, use HTTP Proxy. Do not use one otherwise. HTTP Proxy transform UDP stream to HTTP stream that allows to improve quality of transmitted image if the channel in local network is in inferior quality.
- *HTTP port* – number of HTTP Proxy port, which will be used for video-stream transmission. Use this port for connection to translated IPTV streams.

For instance, if the device has the 192.168.0.1 address on the LAN interface, Proxy server's value is 2345 and you need to playback 227.50.50.100 channel broadcasted to UDP port 1234, set stream address for VLC programm in the form of: http://@192.168.0.1:2345/udp/227.50.50.100:1234.

For applying a new configuration and saving setting to non-volatile memory, press button. To discard changes, press .

5.5.4 System

This tile helps to set parameters of access to the web interface. To set additional parameters, press «more» link.

Access to the web interface through WAN:

- *HTTP* – when checked, the connection to the web configurator through WAN via HTTP is enabled (insecure connection);
- *HTTPS* – when checked, the connection to the web configurator through WAN via HTTPS is enabled (secure connection).

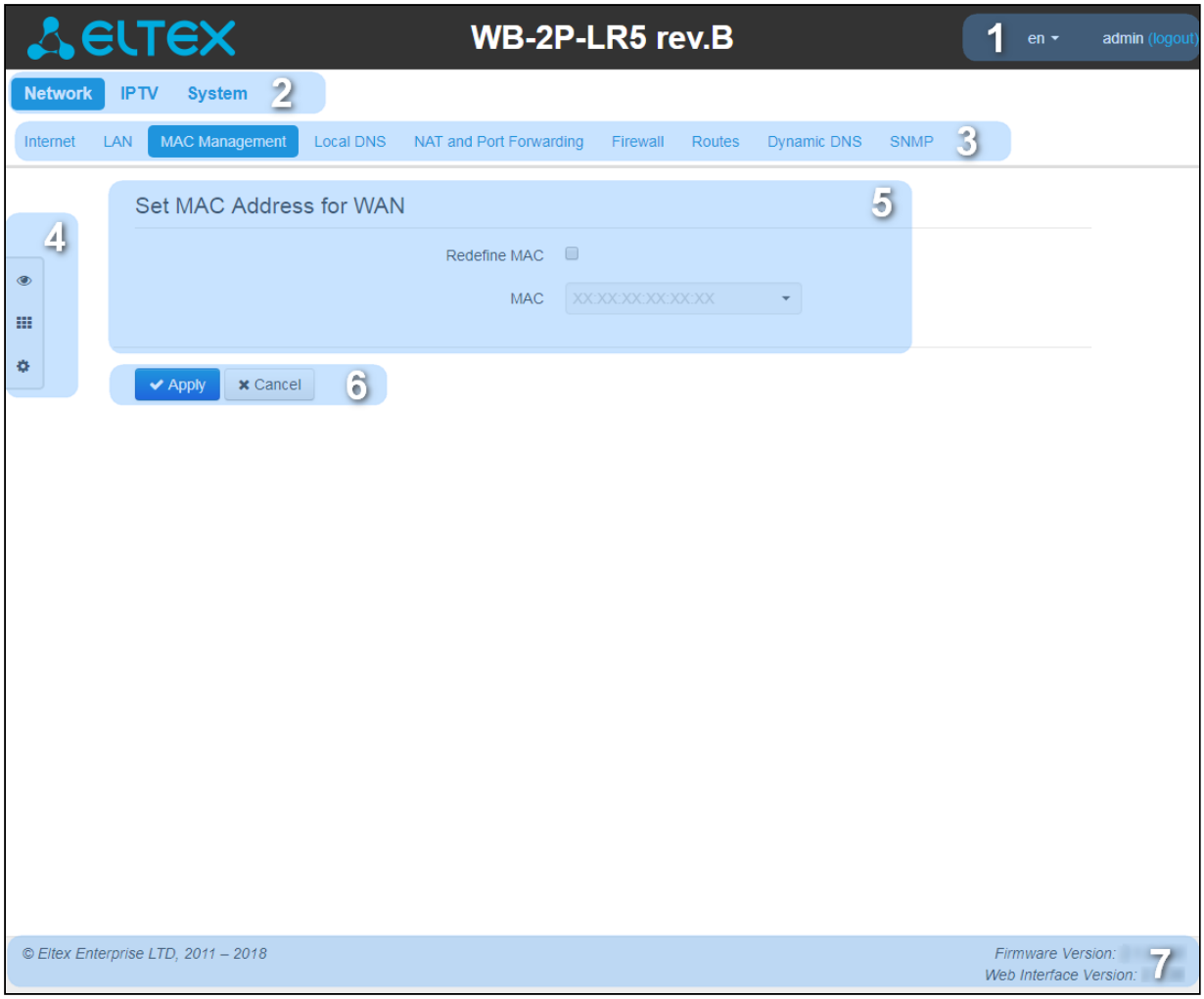
For applying a new configuration and saving settings to non-volatile memory, press button. To discard changes, press .

5.6 Advanced settings (preferences)

To move to advanced settings mode, press «more» link or select «Preferences» on the left panel.

5.6.1 Main elements of the web interface

The figure below shows navigation elements of the web configurator in advanced settings (preferences) mode.



The user interface is divided into seven areas:

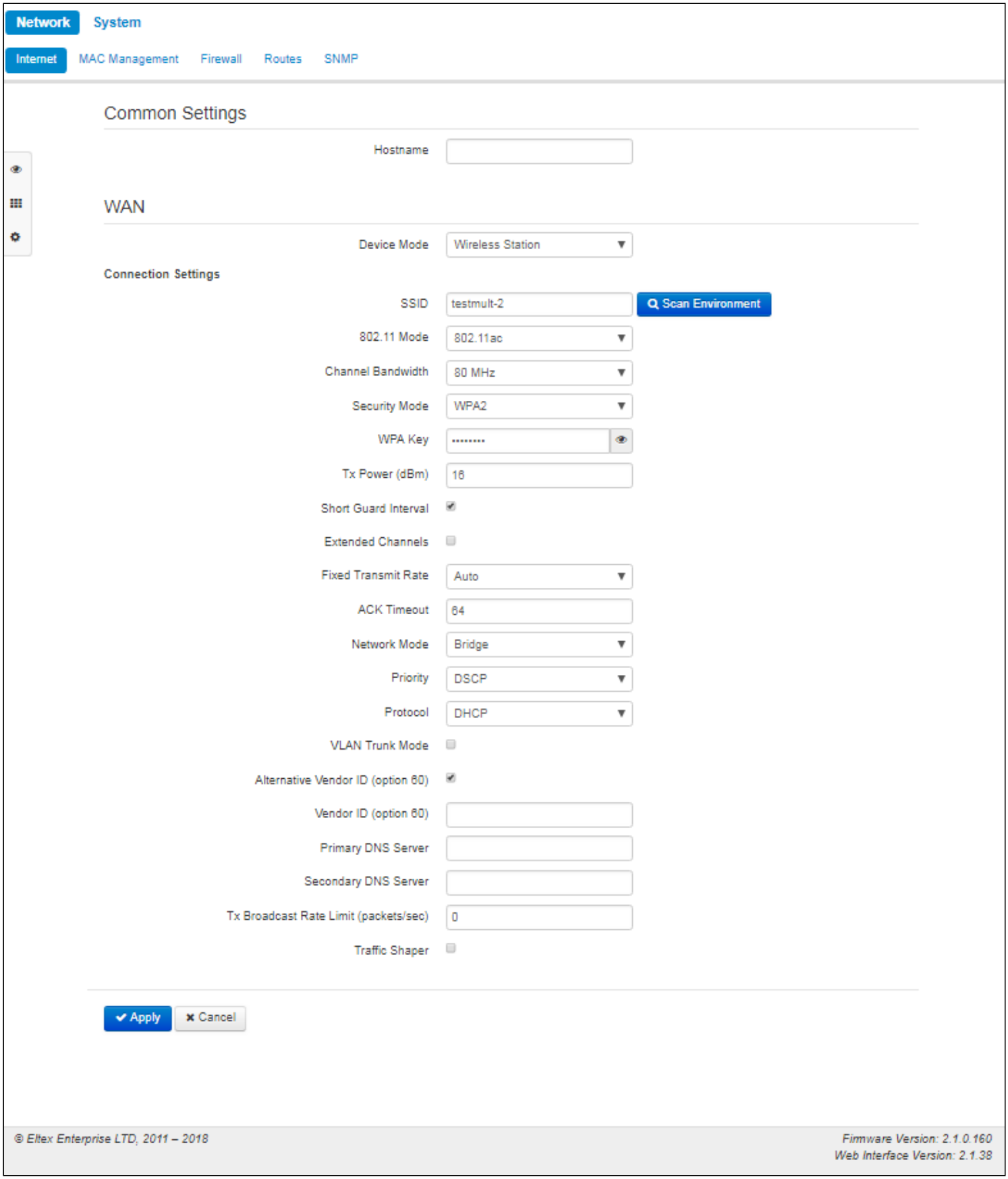
1. Username, which was used to enter the system and «logout» button to finish the user session.
2. Menu tabs which contain submenu tabs are divided into categories: **Network**, **System, IPTV** (for router mode).
3. Submenu tabs manage the settings field below.
4. A panel for web configurator's mode changing (see the description in section Web interface operation modes).
5. Settings field, which is based on the user select. The field is dedicated to view device settings and setting configuration data.
6. Configuration management buttons, the detailed description is given in section Applying configuration and discarding changes.
7. Information field. The field contain information on firmware version and web interface version.

5.6.2 «Network» menu

You may implement main network settings in «Network» menu.

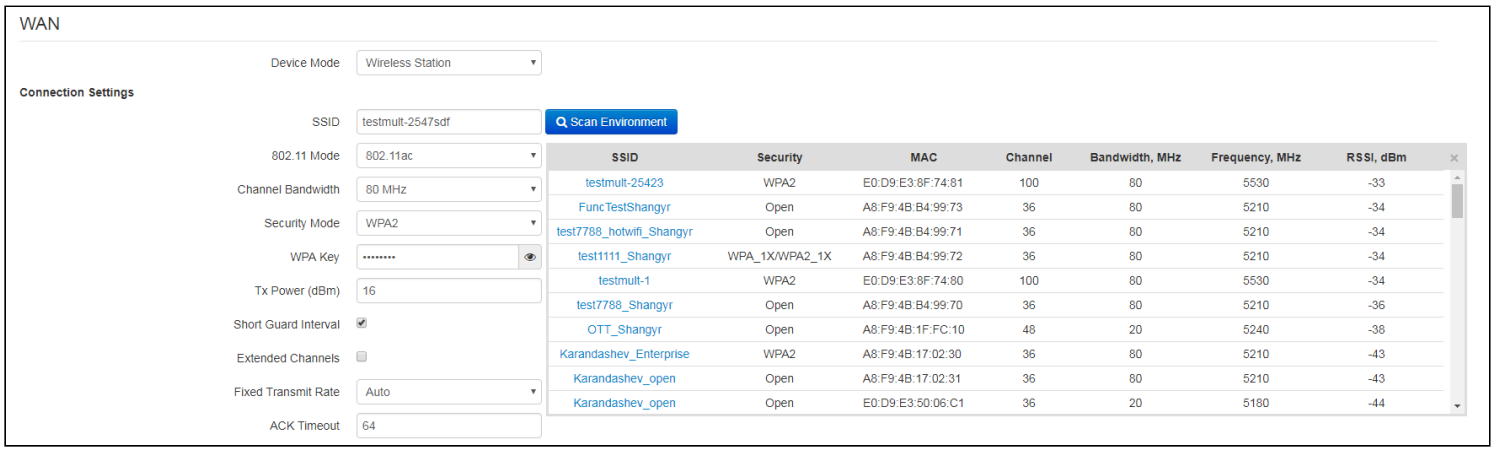
5.6.2.1 «Internet» submenu

In «Internet» submenu, you may configure parameters to connect to a base station via Wi-Fi and select connection mode.



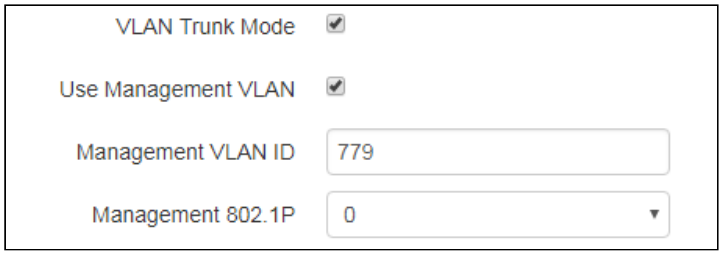
- *Hostname* – a name of the network device;
- *Device mode* – a mode of device connection;
- *Scan Environment* – press the button to start scanning at the defined range. The list of found access point will be displayed after scanning. The list of access points consists of seven coloumns: access point SSID,

security mode, MAC address, channel, channel bandwidth, frequency, signal level. If you select any access point from the list, SSID field will be filled automatically, and the corresponding mode will be selected.

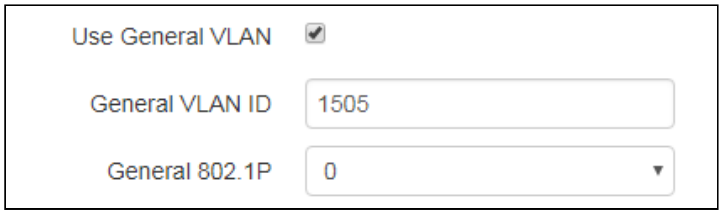


- *SSID* – wireless network ID, which is used for base station connection. The maximum name lenght – 32 symbols, the keyboard register is important. The name may consist of digits, latin letters and symbols «-», «_», «.», «!», «;», «#» and space, although it is forbidden to start with the symbols «!», «;», «#» and space.
- *802.11 Mode* – select wireless interface operation mode:
  - *802.11a* – the standard supposes maximum rate of up to 54 Mbps;
  - *802.11n* – the standard supposes maximum rate of up to 300 Mbps;
  - *802*.11ac – the standard supposes maximum rate of up to 866.7 Mbps.
- *Channel Bandwidth* – channel bandwidth, on which a Wi-Fi client operates. The parameter may take values from 5, 10, 20, 40 and 80 MHz. Note, that channel bandwidth of 80 MHz will operate only according to 802.11ac standard. If the base station has 5 or 10 MHz bandwidth, you should select the same bandwidth on the user station.
- *Security mode* – select security mode for wireless network:
  - *Off* – encryption of the wireless network is off, low security.
  - *WEP* – WEP authentication. WEP-key should consist of hexadecimal digits and be of 10 or 26 symbols lenght or it might be a string (a-z, A-Z, 0-9, ~!@#$%^&*()_-+= symbols) with lenght of 5 or 13 symbols. The mode is hidden in the web interface.
  - *WPA, WPA2* – WPA and WPA2 authentication. The key lenght is from 8 to 63 symbols. The following symbols are allowed: a-z, A-Z, 0-9, ~!@#$%^&*()_-+=;:|/?.,<>"`' or space. It is recommended to use WPA and WPA2 encryption modes as the safetest.
  - *WPA-Enterprise, WPA2-Enterprise* – WPA and WPA2 encryption with client authentication via 802.1x. Enter username and password as authentication data.
- *Tx Power (dBm)* – transmitting Wi-Fi signal power adjustment, dBm.
- *Short Guard Interval* – time interval, which is used to protect against intersymbol interference.
- *Extended Channels* – the parameter which allows to use additional channels to connect to a base station (channels 49-51, 65-99, 145-148). The channels 166-230 are available for WB-2P-LR5 rev. B for connection to a base station even with not set «Extended Channels» parameter.
- *Fixed Transmit Rate* – fixed wireless data transmission rate which is defined by IEEE 802.11a/n/ac standards.
- *ACK Timeout* – packet confirmation waiting timeout. When the distance is long, the parameter is recommended to be increased.
- *Network Mode* – device operation mode:
  - *Router* – router mode between LAN and WAN interfaces (WAN interface is the wireless Wi-Fi interface, LAN is isolated from WAN);
  - *Bridge* – bridge mode between wired and wireless interfaces of the device.
- Priority – select prioritization means:
  - *DSCP* – classification mechanism for traffic control and quality of service provision through priorities.

    - *802.1p* – attribute (also called CoS – Class of Service) is attached to egress IP packets. The value is from 0 (the least priority) to 7 (the highest priority).
- *Protocol* – select protocol for connection of the device via Wi-Fi interface to service provider network:
    - *Static* – operation mode, when IP address and other necessary parameters of WAN interface are set statically (manually). If «Static» is selected, the following parameters will be available to set:
        - *WAN IP* – set IP address of WAN interface of the device in service provider network;
        - *Netmask* – set subnet mask of device's WAN interface in service provider network;
        - *Default Gateway* – address, to which a packet will be transmitted in case the route has not been found in the route table.
    - *DHCP* – operation mode, when IP address, subnet mask, DNS server address, defualt gateway and other parameters required for operation are obtained from DHCP server automatically. Before obtaining the parameters via DHCP, the access to the device is implemented via address set in IP address field.
        - *Alternative Vendor ID (Option 60)* – when selected, the device transmits Vendor ID (Option 60) field value in Option 60 DHCP messages (Vendor class ID). If the field is empty, Option 60 will not be transmitted in DHCP messages.
          If the parameter *Alternative Vendor ID (Option 60)* is not checked, the defualt value will be transmitted in option 60. The default value has the following format:
          [VENDOR :device vendor**][DEVICE :**device type**][HW :**hardware version**] [SN :**serial number**][WAN :**WAN interface MAC address**][LAN :**LAN interface MAC address**][VERSION :**firmware version**]**
          Example:
          [VENDOR:Eltex][DEVICE:WB-2P-LR5][HW:1.2][SN:WP29000038] [WAN:E0:D9:E3:75:55:60] [LAN:E0:D9:E3:75:55:60][VERSION:2.0.0.161]
- *Primary DNS server, Secondary DNS server* – IP address of DNS servers. If DNS servers' addresses are not allocated automatically via DHCP, if necessary, set them manually.
- *VLAN Trunk* – if checked, the trunk port is activated for connected devices. There is an opportunity to use Management VLAN and General VLAN:
    - *Use Management VLAN* – when checked, VLAN used for access to the device is enabled:



        - *Management VLAN ID* – VLAN identifier, which is used to access the device;
        - *Management 802.1P* – 802.1P attribute (also called CoS – Class of Service), which is attached to egress IP packets transmitted from this interface. The value is from 0 (the least priority) to 7 (the highest priority).
    - *Use General VLAN* – when checked, VLAN used for service provision is enabled:



        - *General VLAN ID* – VLAN identifier, which is used for service provision;
        - *General 802.1P* – 802.1P attribute (also called CoS – Class of Service), which is attached to egress IP packets transmitted from this interface. The value is from 0 (the least priority) to 7 (the highest priority).

- *Tx Broadcast Rate Limit (packets/sec)* – limits broadcasting to external Wi-Fi network.
- *Traffic Shaper* – rate limit of both Downlink and Uplink directions. The maximum limit is 200 Mbps.

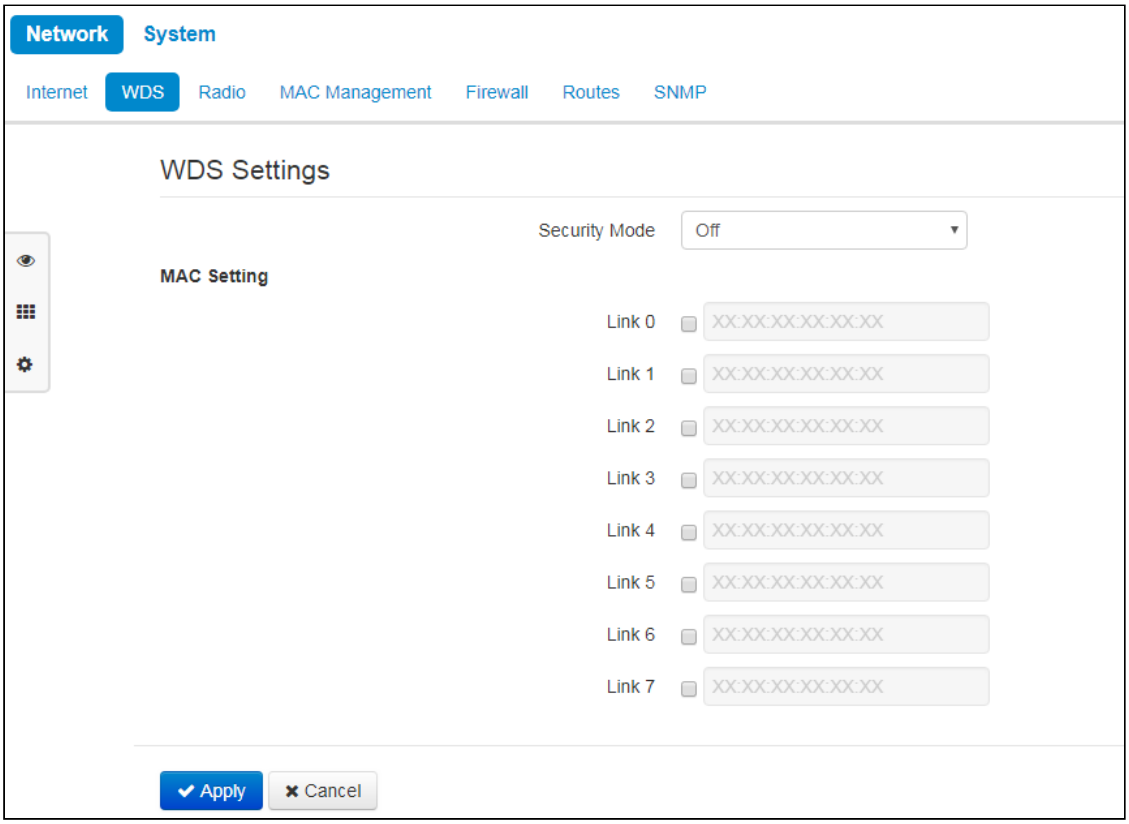
VLAN – virtual local area network.VLAN is a group of hosts allocated in a network not depending on the physical location. The devices grouped to a VLAN have the same identifier VLAN-ID.

When «Use Management VLAN» is checked and Management VLAN configured incorrectly, there is a posiibility of losing access to the device.

5.6.2.2 «WDS» submenu

«WDS» submenu is available only in «Wireless bridge» mode.

In WDS submenu, you may configure general parameters of the wireless bridge.



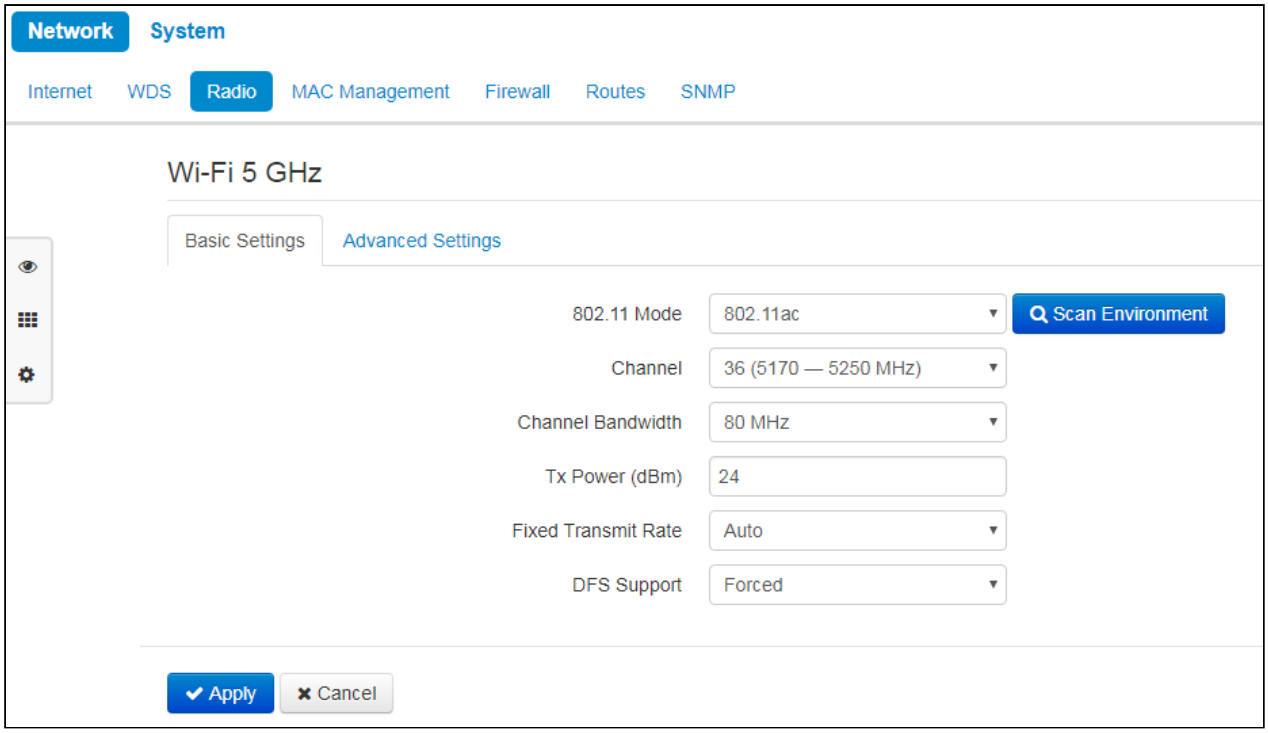
- *Security mode* – select security mode for wireless bridge:
  - *Off* – wireless network encryption is off, low security;
  - *WPA2* – WPA2 authentication. The key lenght is from 8 to 11 symbols. The following symbols are permitted to be used: a-z, A-Z, 0-9, ~!@#$%^&*()_-+=;: |/?.,<>"`' or space.
- *Link 0-7* – wireless links enabling. Enter MAC address of the device, to which you want to configure the wireless bridge, to a corresponding field next to Link checkbox.

5.6.2.3 «Radiointerface» submenu

«Radiointerface» submenu is available only in «Wireless bridge» mode.

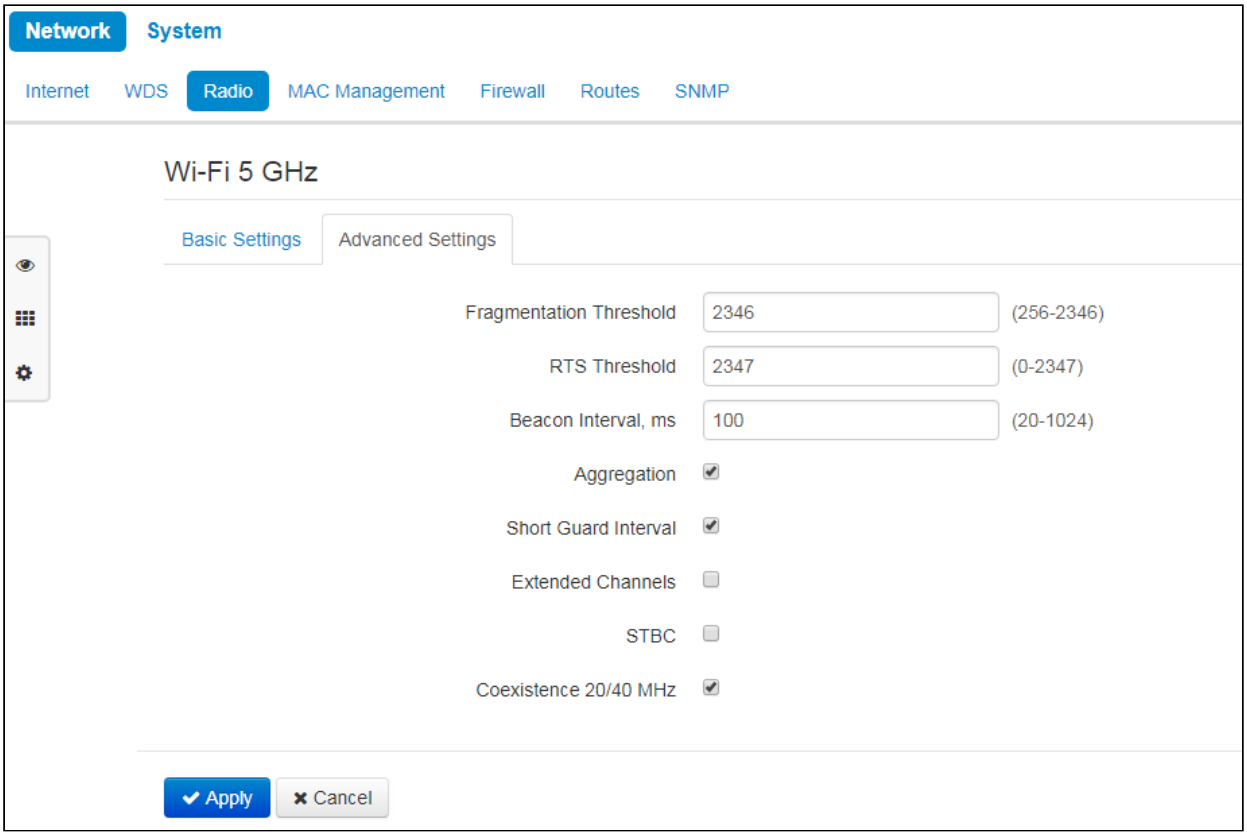
In Radiointerface menu, you may configure the radiointerface to organize wireless bridge.

Basic settings:



- *Scan Environment* – press the button to start scanning at the defined range. The list of found access points will be displayed. The list of access points consists of seven coloumns: access point SSID, security mode, MAC address, channel, channel bandwidth, frequency, signal level.
- *802.11 Mode* – select wireless interface operation mode:
  - *802.11a* – the standard supposes maximum rate of up to 54 Mbps;
  - *802.11n* – the standard supposes maximum rate of up to 300 Mbps;
  - *802.*11ac – the standard supposes maximum rate of up to 866.7 Mbps.
- *Channel* – select channel for data transmission.
- *Channel Bandwidth* – channel bandwidth, on which the radiointerface operates. The parameter may take values from 5, 10, 20, 40 and 80 MHz according to selected mode.
- *Tx Power (dBm)* – transmitting Wi-Fi signal power adjustment, dBm.
- *Fixed Transmit Rate* – fixed wireless data transmission rate which is defined by IEEE 802.11a/n/ac standards.
- *DFS Support* – dynamic frequency selection mechanism. The mechanism demands wireless devices to scan environment and avoid using channels which coincide with radiolocation system's channels at 5 GHz:
  - Disabled – the mechanism is disabled. DFS channels are not available for selection.
  - Enabled – enable the mechanism.
  - Forced – the mechanism is disabled. DFS channels are available for selection.

Advanced settings:



- *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.
- *Beacon Interval, ms* – beacon frames transmission period. The frames are sent to detect access points. The parameter takes values from 20 to 2000 ms, by default – 100 ms.
- *Aggregation* – enable support for AMPDU/AMSDU.
- *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.
- Extended Channels – a parameter which allows to use additional channels to connect to a base station (channels 49-51, 65-99, 145-148). The channels 166-230 are available for WB-2P-LR5 rev. B for connection.
- *STBC* – Soace-Time Block Coding method dedicated to improve data transmission reliability. When checked, the device transmits one data flow through several antennas. When unchecked, the device does not transmit one data flow through several antennas.
- Coexistence 20/40 MHz – automatic bandwidth changing when environment is loaded.

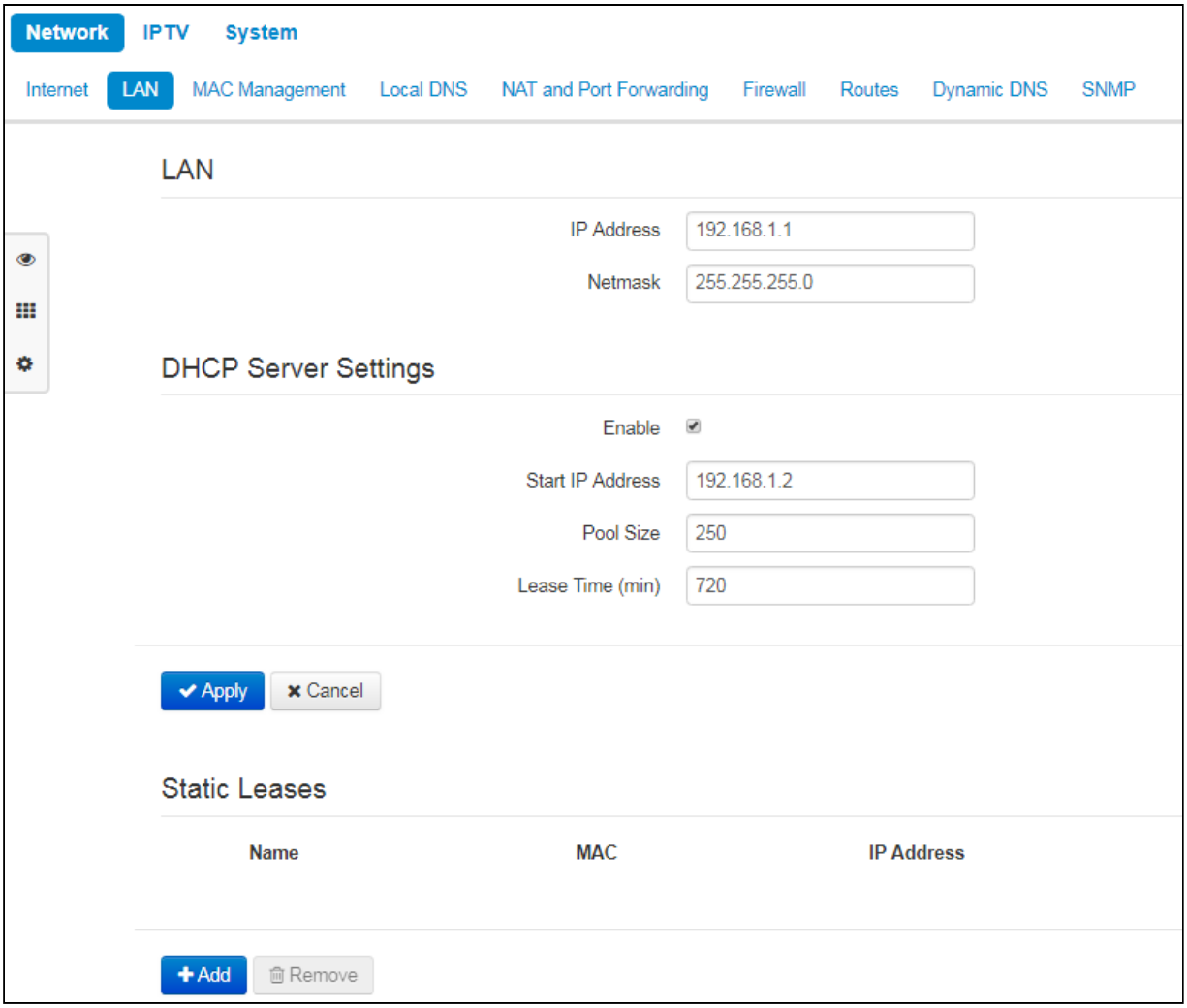
For wireless bridge operation, radiointerface parameters shoul be configurate identically on all the devices.

5.6.2.4 DHCP server settings

DHCP server settings are available only in router mode.

In DHCP server settings section you may configure local network, DHCP server, set static addresses bindings.

The device is capable to assign IP addresses and other parameters required to the Internet access to computers connected to LAN interface and WiFi access point through DHCP (Dynamic Host Configuration Protocol). The use of DHCP allows to avoid limits occured while manual configuration of TCP/IP.



LAN:

- *IP address* – IP address of the device in a local network;
- *Netmask* – subnetmask in local network.

DHCP server settings:

- *Enable* – when cheked, a local DHCP server is enabled, otherwise the server is disabled;
- *Start IP address* – the initiate address of the IP addresses pool;
- *Pool size* – the number of addresses in the pool;
- *Lease time (min)* – set the maximum time range for using an IP address assigned by DHCP server, lease time is set in minutes.

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

When you try to change an initial destination IP address in a subnet different from the LAN interface subnet, the pool is set to the current LAN address value automatically.

Static leases

Configuring of static leases is helpful when you need that the certain computer always obtains certain IP address.

To set new static lease, press «Add» buttion and fill the following fields:

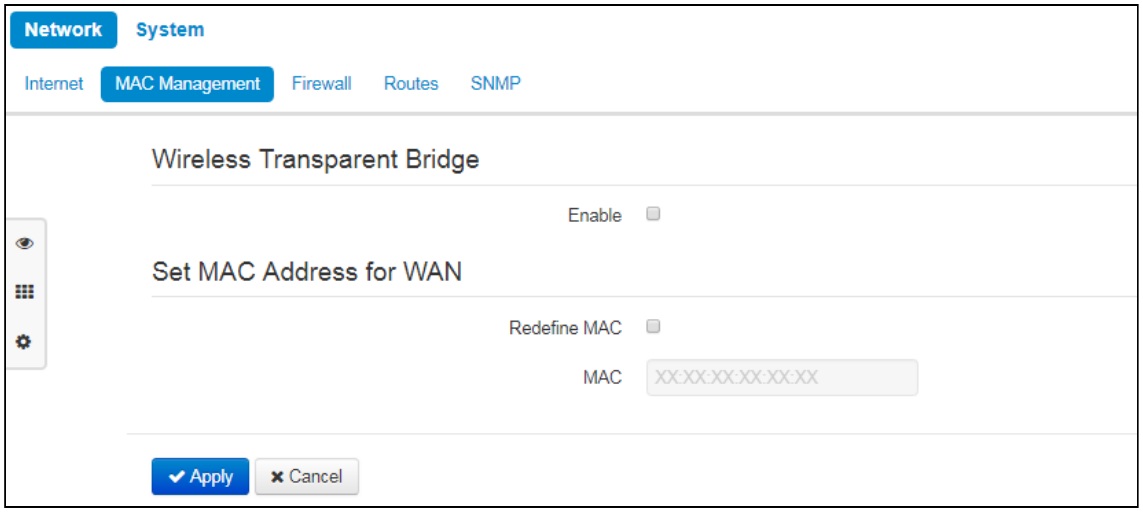
- *MAC address* – set static MAC address using the following format XX:XX:XX:XX:XX:XX;
- *IP-address* – set static IP address for the specified MAC address.

Press «Apply» to add IP address to the list of static IP addresses for DHCP server. Press «Cancel» to discard the changes.

To delete an address from the list, select the corresponding checkbox and press «Remove».

5.6.2.5 «MAC Management» submenu

In MAC address Management submenu, you may set MAC address of the device's WAN interface.



Wireless transparent bridge

«Wireless transparent bridge» settings are available for Bridge mode of Wi-Fi station only.

When you enable Wireless transparent bridge, WB-2P-LR5 will not substitute client MAC addresses from LAN with own MAC address. The limit is 15 MAC addresses without substitution. When the value is exceeded client's MAC address will be substituted. The section of connected clients on a base station will include MAC addresses of client devices from LAN.

Set MAC address for WAN

- *Redefine MAC* – when checked, the MAC address from the field MAC is used.
  In bridge mode, MAC takes the entered MAC value. Enterring of multicast MAC addresses and MAC addresses from ARP table is forbidden. In router mode, MAC address of the PC which you use to connect the web configurator should be enterred to «MAC» field. It is useful when MAC bindings are used on the network. When you need to use the device as a router, you should assign MAC address of your PC (which were used for Internet connection) to WAN interface of the device.

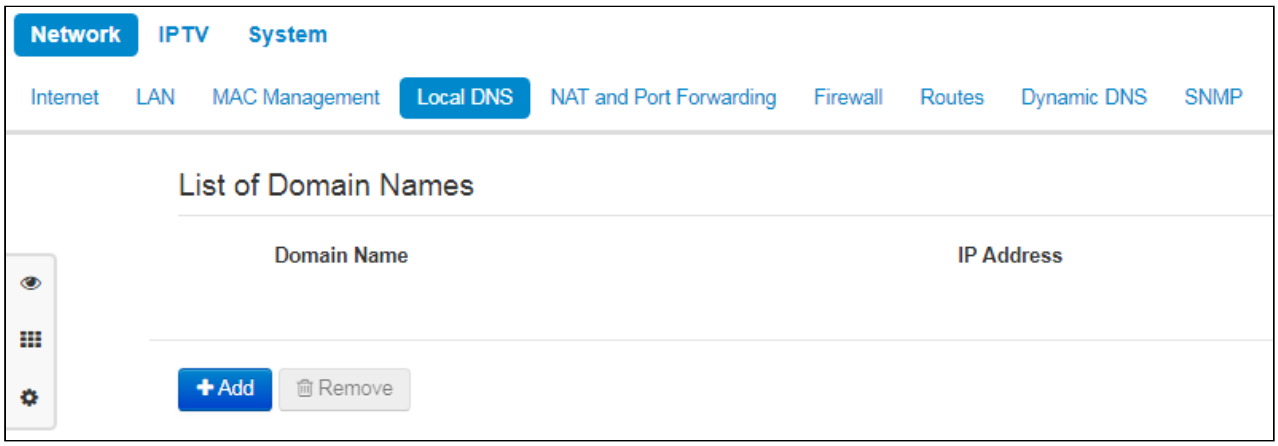
To apply a new configuration and save settings to non-volatile memory, press «Apply». Press «Cancel» to discard the changes.

5.6.2.6 «Local DNS» submenu

Local DNS submenu is available only in router mode.

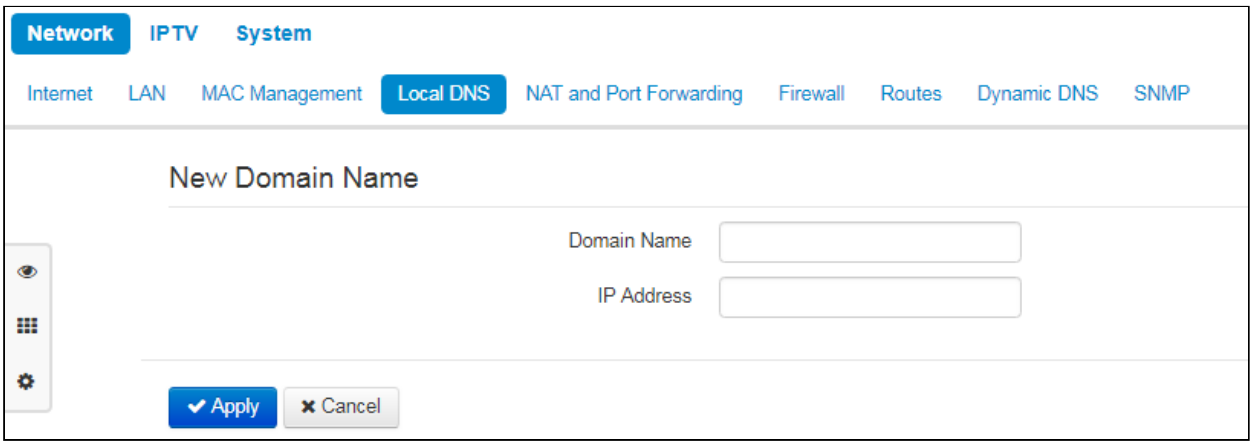
You may configure local DNS server of the device by adding IP address and domain name in local DNS submenu.

Local DNS allows gateway to obtain an IP address of connected device using its network name (host). In case of lack of DNS server in a network segment in which the gateway is located, you may use Local DNS to route using network names or to use its network name as a SIP server address. To implemet this, you should know concordances between nodes names (hosts) and their IP addresses.



Configuring nodes

Press «Add» to add new domain name. Fill the following fields:



- *Domain name* – name of a node;
- *IP Address* – node's IP address.

Press «Apply» to create concordance IP adrress – domain name. To discard changes, press «Cancel». To delete an entry from the list, select corresponding checkbox and press «Remove».

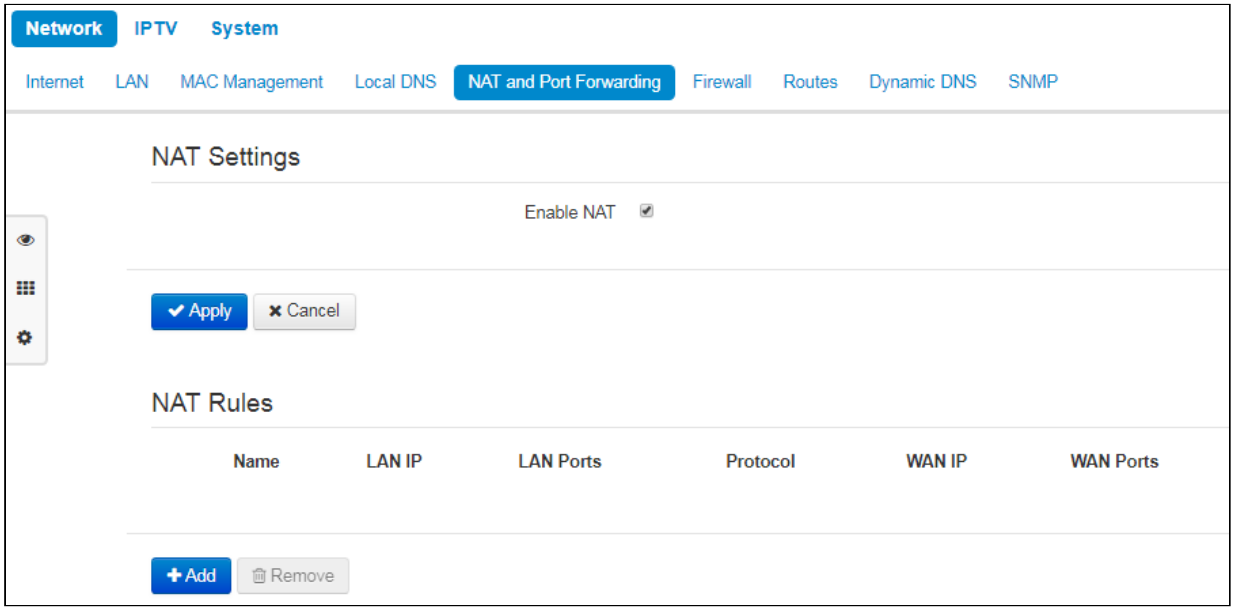
5.6.2.7 «NAT and Port Forwarding» submenu

NAT and Port Forwarding submenu is available only for router mode.

You may configure Port Forwarding from WAN interface to LAN interface in NAT and Port Forwarding submenu.

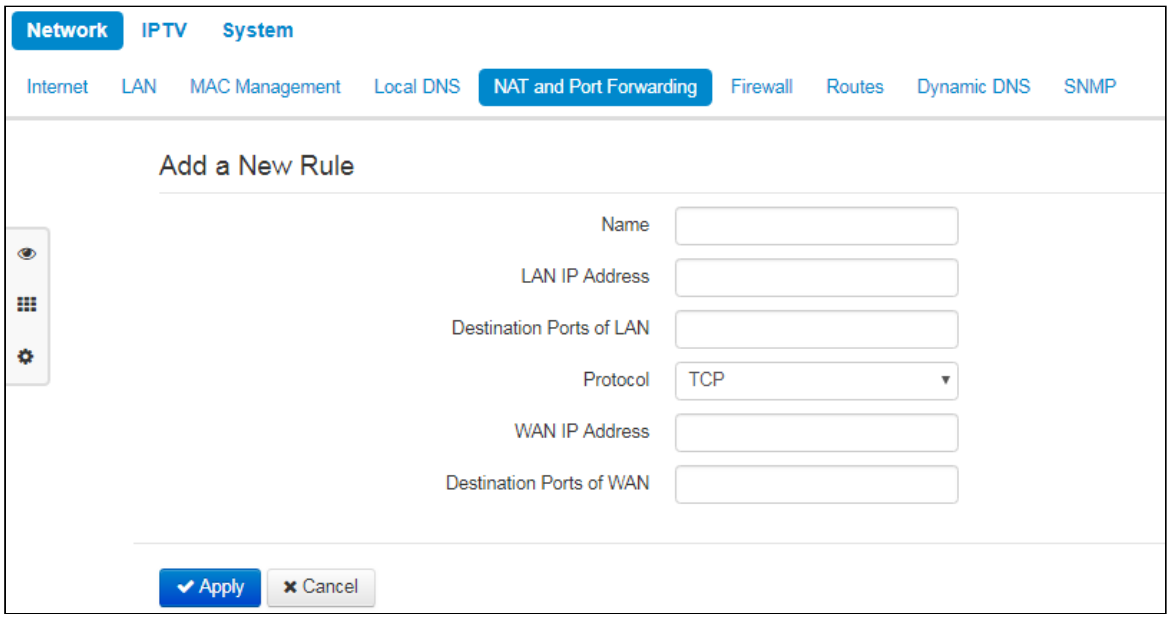
NAT (Network Address Translation) mode allows to modify IP addresses and network ports of IP packets. Port forwarding is necessary when TCP/UDP connection with local PC (connected to LAN interface) is established via external network. The settings menu allows to set rules which permit packets transmission from external network to specified address in a local network, i.e. to establish connection.

Port forwarding is also necessary when using torrent and p2p services. To implement the configuration, find TCP/UDP ports used by torrent or p2p clients in settings and set them for corresponding port forwarding rules to a PC IP address.



NAT rules

To add a new NAT rule, press «Add» and fill the following fields:



- *Name* – name of the rule (it is obligitory to fill the field);
- *LAN IP Address* – IP address of host in local network. Packets translated to this host will follow the rule;
- *Destination ports of LAN* – receiver TCP/UDP ports, via which packets are translated to local network (you may assign either single port or range of ports using dash);
- *Protocol* – select packet protocol for the rule: TCP, UDP, TCP/UDP;
- *WAN IP address* – source IP address in external network which will be under the rule;

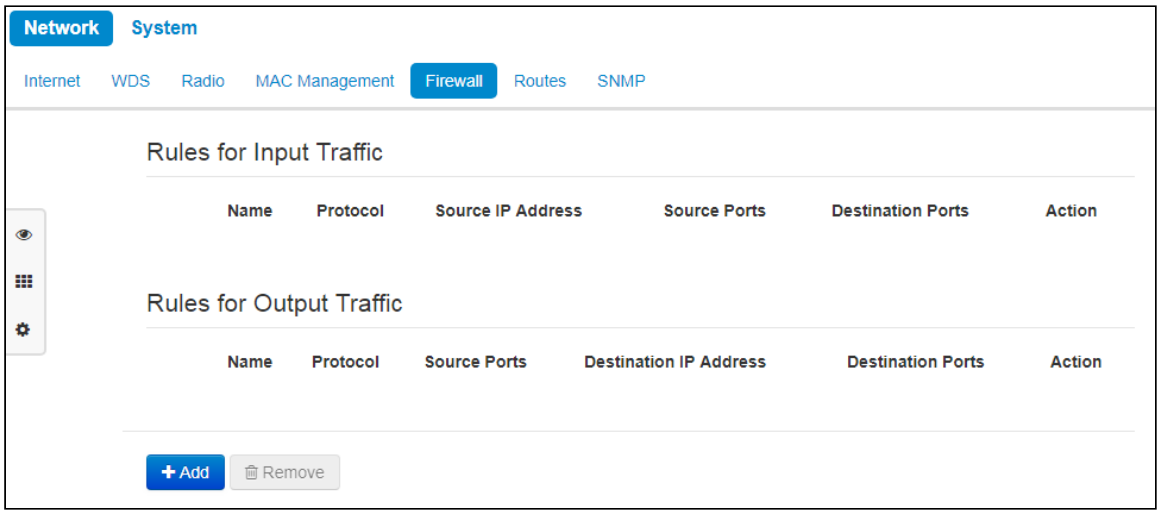
- *Destination Ports of WAN* – destination TCP/UDP ports in external network, packets from which will follow the rule (you may assign either single port or range of ports using dash).

The port forwarding rule is implemented as follows: a packet received via «Protocol» on a port defined in «Destination Ports of WAN» field and having source address defined in «WAN IP address» field (if the field is empty, source IP does not consider) undergoes address and Destination port substitute with the parameters defined in «LAN IP Address» and «Destination Ports of LAN» fields respectively.

Press «Apply» to create concordance IP adrress – domain name. To discard changes, press «Cancel». To delete an entry from the list, select corresponding checkbox and press «Remove».

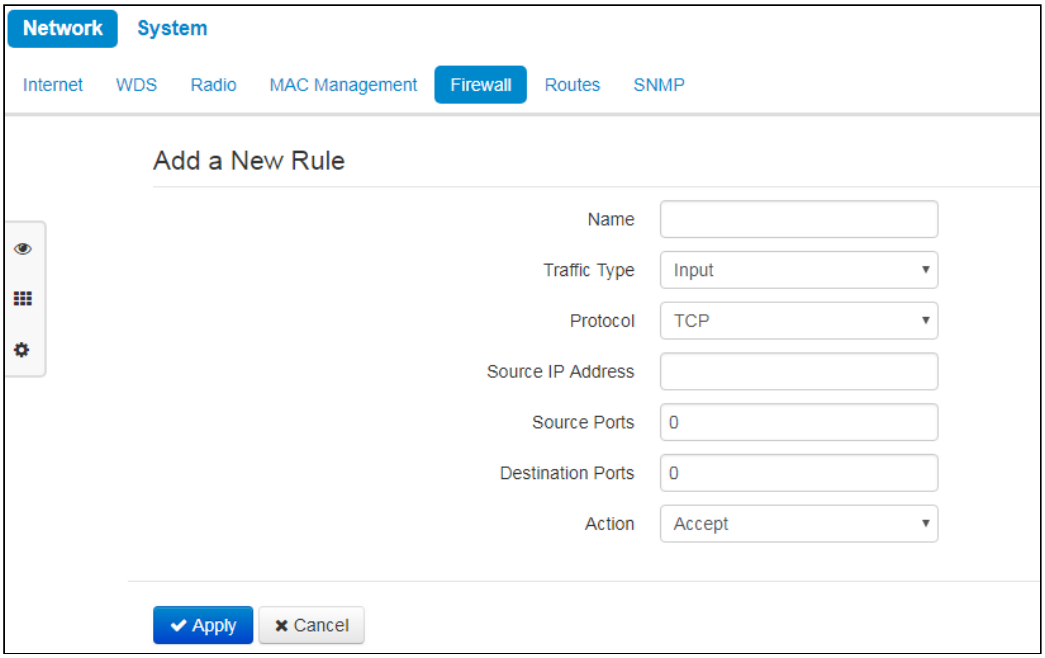
5.6.2.8 «Firewall» submenu

The rules for incoming, outcoming and transit traffic transmission are set in Firewall submenu. There is an opportunity to limit transmission of different types of traffic (incoming, outgoing, transit) depending on protocol type, source and destination IP, TCP/UDP source and destination ports, type of ICMP message.



Configuring firewall rules

To add a new firewall rule, press «Add» button and fill the following fields:



- *Name* – a name of the rule;
- *Traffic Type* – select traffic type for which you create the rule:
  - *Input* – incoming traffic (the receiver is one of the network interfaces of the device). When selected, the following traffic types are available for editing:
    - *Source IP address* – a source IP address. You may set subnet mask after «/» character. The subnet mask should be set in the following formats: xxx.xxx.xxx.xxx or xx, e.g. 192.168.16.0/24 or 192.168.16.0/255.255.255.0 to set addresses range (the subnet mask entry /24 coincides with /255.255.255.0 entry);
  - *Output* – outgoing traffic (traffic which is generated by the device locally from a network interface). If the parameter is selected, the following field will be displayed:
    - *Destination IP address* – set destination IP address. You may set subnet mask after «/» character. The subnet mask should be set in the following formats: xxx.xxx.xxx.xxx or xx, e.g. 192.168.16.0/24 or 192.168.16.0/255.255.255.0 to set addresses range (the subnet mask entry /24 coincides with /255.255.255.0 entry);
- *Protocol* – a protocol of the packets, which will follow the rule: TCP, UDP, TCP/UDP, ICMP, any.
- *Action* – an action for packets to undergo (accept/drop).

When TCP, UDP, TCP/UDP protocols are selected, the following settings will be available to configure:

- *Source ports* – the list of source ports, packets from which will follow the rule (it is acceptable to specify one port or port range with the help of «–» sign). To specify all the source ports, enter «0–65535»;
- *Destination ports* – the list of destination ports, packets from which will follow the rule (it is acceptable to specify one port or port range with the help of «–» sign). To specify all the source ports, enter «0–65535».

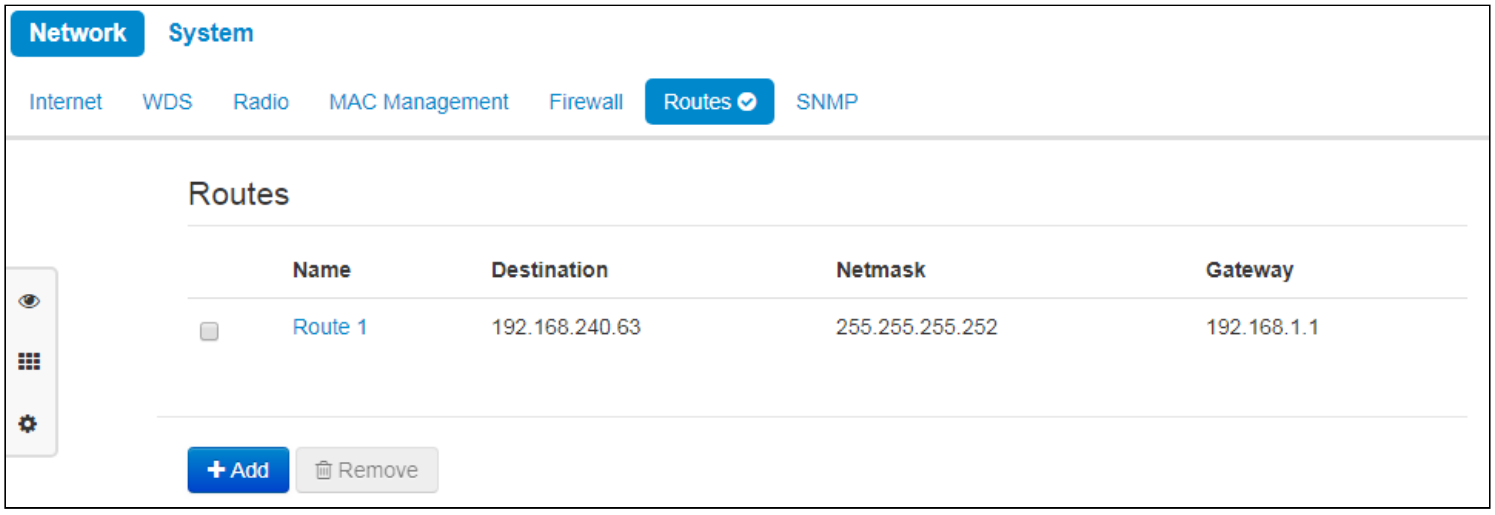
When ICMP is selected, the following settings will be available for editting:

- *Type of ICMP Message* – you may create a rule for a certain ICMP messages type or for all types.

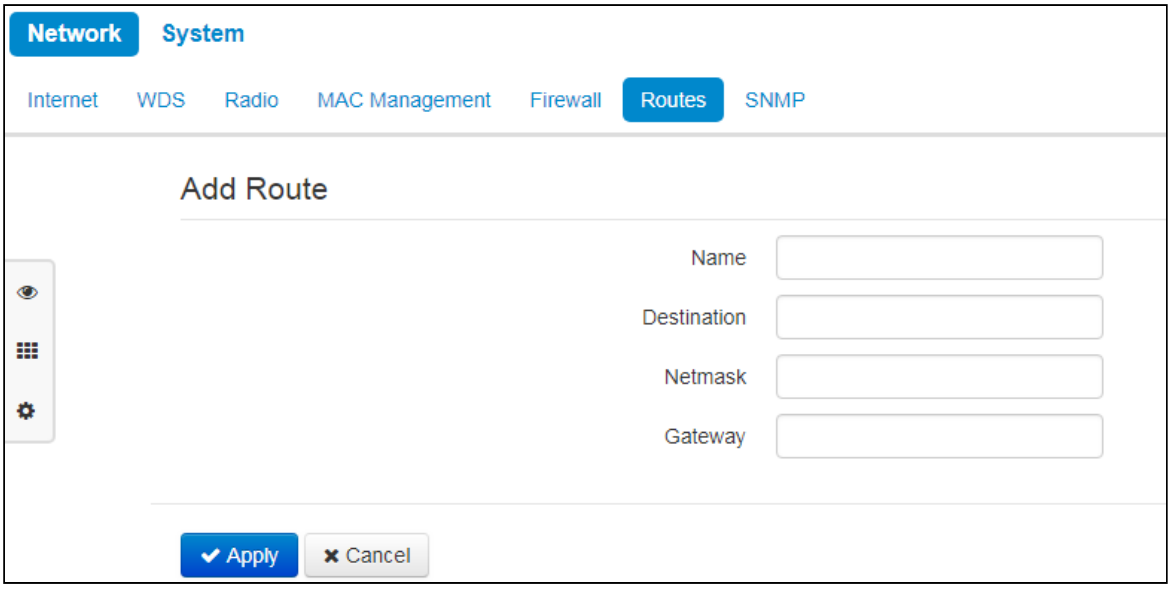
Press «Apply» button to add a new rule. Press «Cancel» to discard the changes. To delete a created rule, check the box next to the rule and press «Remove».

5.6.2.9 «Routes» submenu

You may set static routes in Routes submenu.



Press «Add» button to add a new route. Fill the following fields:



- *Name* – route name.
- *Destination* – destination host or subnet IP address, to which the route will be set.
- *Netmask* – a subnet mask. A subnet mask for a host is set to 255.255.255.255 value, for a subnet — depending on its size.
- *Gateway* – IP address of the gateway through which the device may access Destination.

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

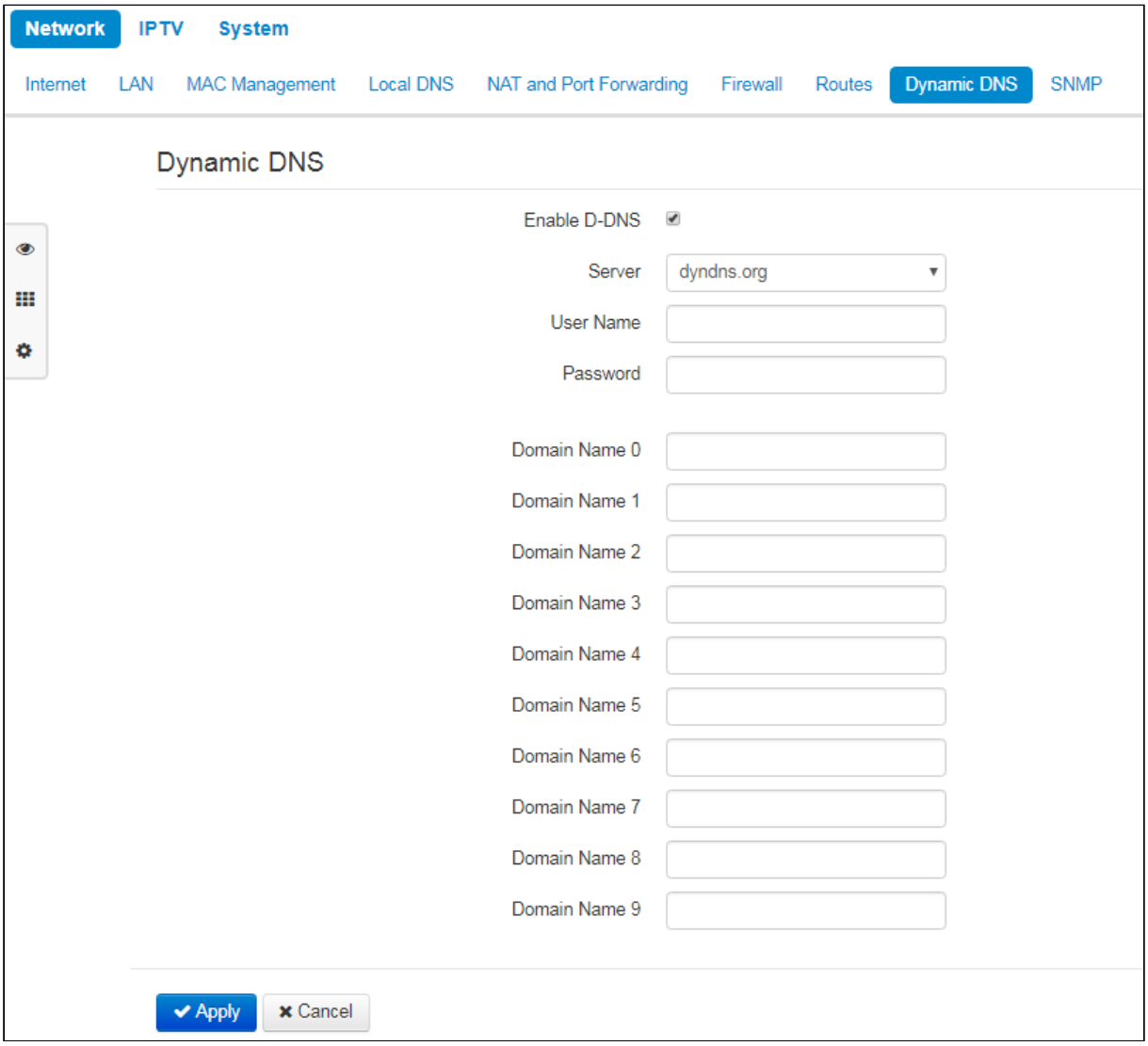
5.6.2.10 «Dynamic DNS» submenu

Dynamic DNS submenu is available only in router mode.

In dynamic DNS submenu, you may configure the coresponding service.

Dynamic DNS (D-DNS) provides information on DNS server update in real time or automatically, if necessary. It is used to assign a permanent domain name to a device (PC, router) with dynamic IP address.

Dynamic DNS is often used in local networks, where clients obtain IP addresses via DHCP, and then register their names on local DNS server.

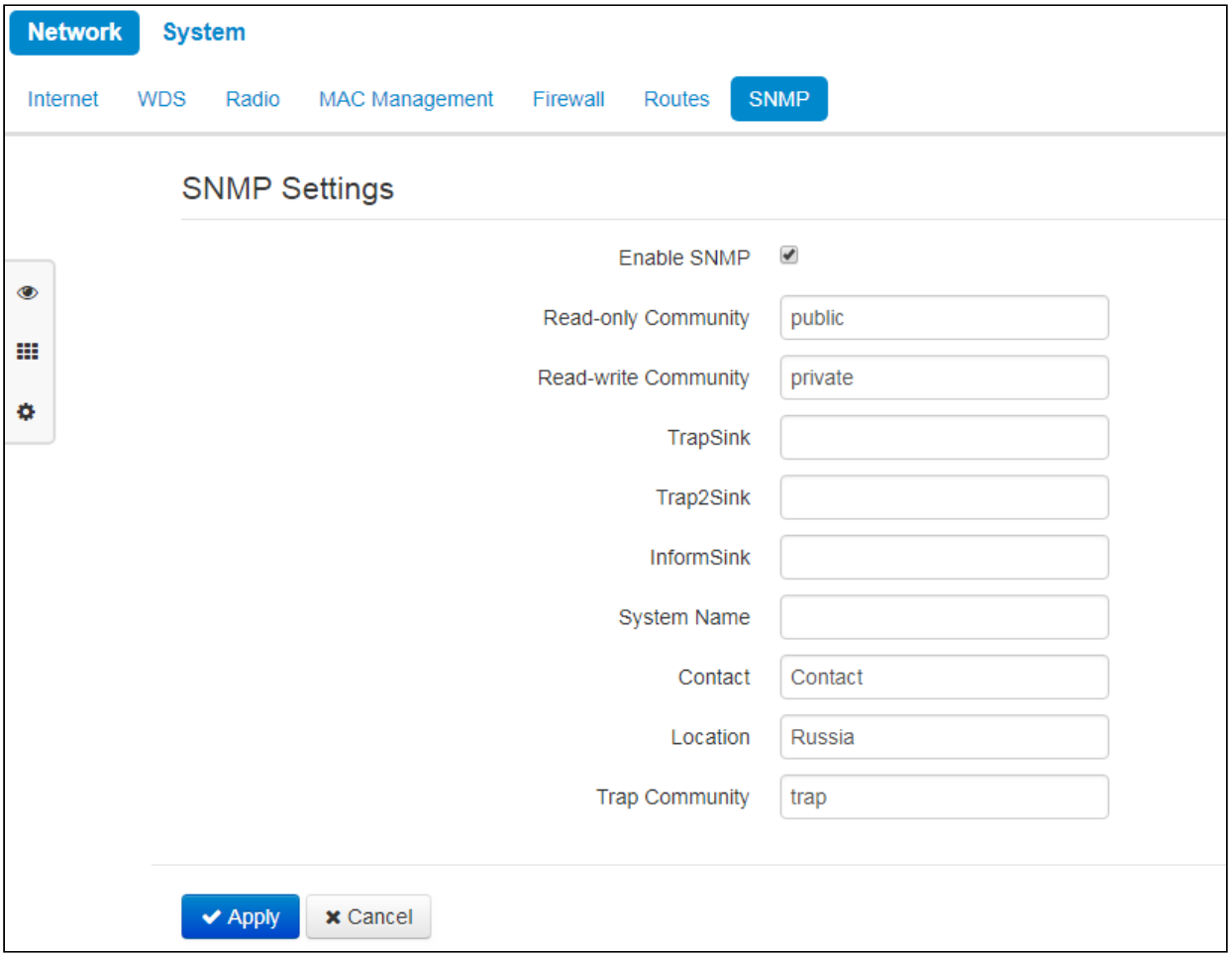


- *Enable D-DNS* – when checked, D-DNS service is enabled. The following fields are available:
  - *Server* – D-DNS provider name – select one of the available providers;
  - *User Name* – a user name for access to D-DNS service account;
  - *Password* – a password for access to D-DNS service account;
  - *Domain name (0..9)* – you may register up to 10 domain names (usually only one is required). The update of data on IP address of the device is implemented once in 60 seconds on a provider server.

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

5.6.2.11 «SNMP» submenu

The software of WB-2P-LR5 allows to monitor device state and its sensors via SNMP. In SNMP submenu, you may configure SNMP agent parameters. The device supports SNMPv1, SNMPv2, SNMPv3.



- *Enable SNMP* – when checked, SNMP is enabled;
- *Read-only Community* – a password to read the parameters (by default: *public*);
- *Read-write Community* – a password to configure (write) parameters (by default: *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* – an IP address or domain name of Inform messages receiver in HOST [COMMUNITY [PORT]] format;
- *System Name* – device name;
- *Contact* – the manufacturer contact;
- *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

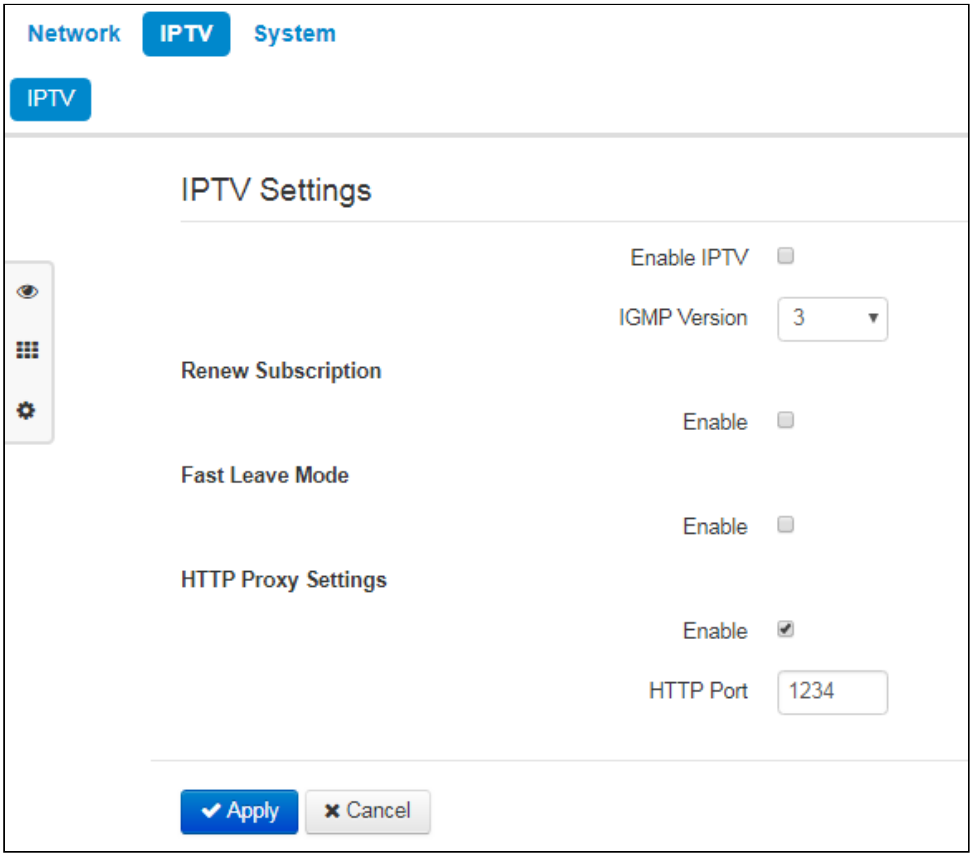
where Enterprise – 1.3.6.1.4.1.35265.1.56 is Eltex Enterprise identifier.

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

5.6.3 «IPTV» settings

The menu is available only in router mode.

You may configure IPTV service in IPTV settings menu.



- *Enable IPTV* – when checked, IPTV signals transmission via WAN interface (from provider network) to the devices connected to the LAN interface is enabled;
- *IGMP version* – IGMP protocol verion for IGMP messages transmission via WAN interface (messages of activation or deactivation of subscribtion to IPTV channels). Versions 2 and 3 are supported.

Renew subscription

- *Enable* – when checked, messages with data on the list of active IPTV channels are periodically transmitted to a higher server which implements IPTV signals translation. Enabling of the function is necessary if a higher server disables IPTV channels translation in a certain period of time.
- *Renew Subscription Interval, s* – a period of messages transmission with data on active IPTV channels list, specified in seconds. Set the value of interval less than interval (timeout) of higher server signals translation disabling.

Fast leave mode

- *Enable* – when checked, the option for fast exit from the multicast group is enabled. The function is not recommended when more than one multicast traffic receiver is used.

HTTP Proxy Settings

- *Enable* – when checked, HTTP Proxy function is enabled. HTTP Proxy implements modification of UDP stream to HTTP stream using TCP (transmission control protocol), that allows to improve quality of

transmitted image in case of poor communication channel quality in a local network. The function is useful when IPTV is watched via wireless Wi-Fi channel.
- *HTTP Port* – a number of HTTP Proxy port, from which video stream will be translated. Use this port to connect IPTV streams translated by the device.

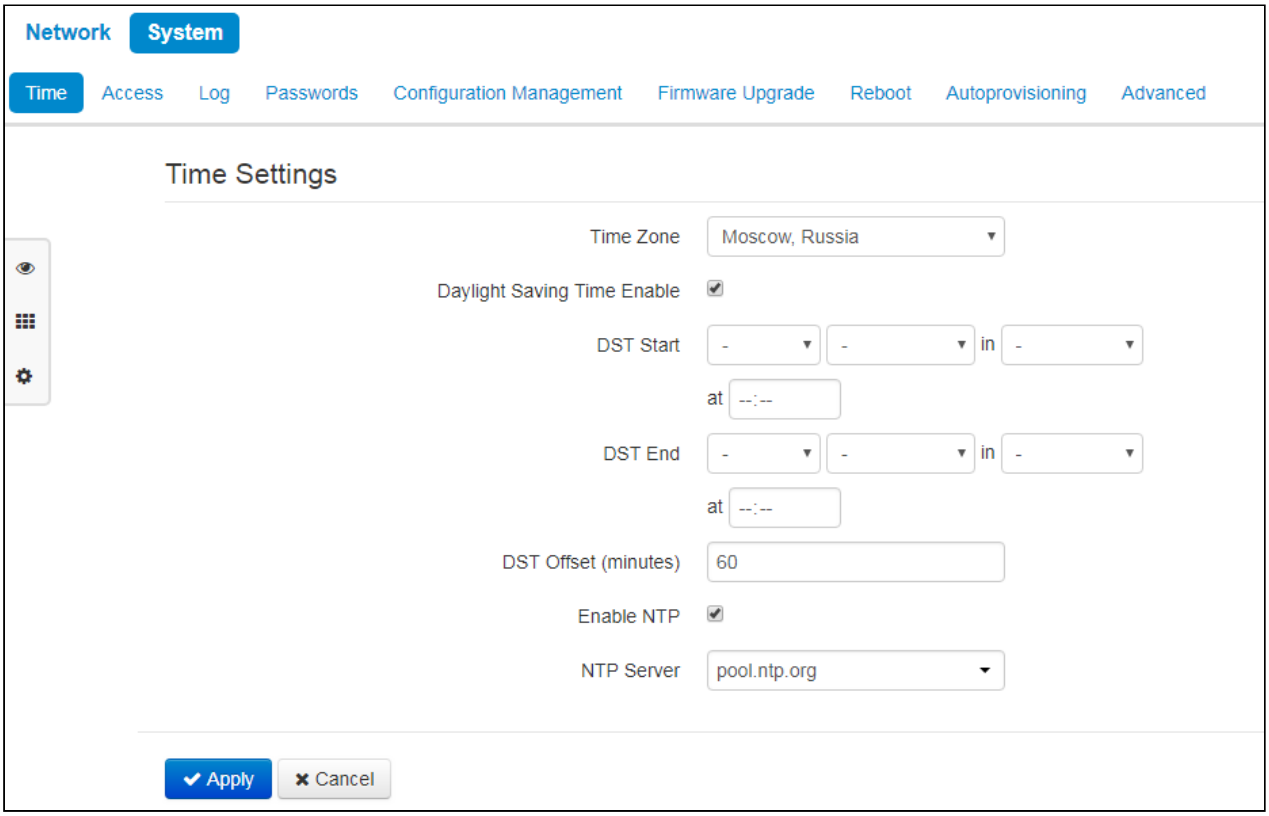
For instance, if the device has the following address of LAN interface 192.168.0.1, port of Proxy server is 2345, and it is necessary to playback the channel 227.50.50.100, translated on UDP port 1234 – you should assign the stream address for VLC programm as follows: http://@192.168.0.1:2345/udp/227.50.50.100:1234.
To apply a new configuration and save setting to non-volatile memory, press «Apply». Press «Cancel» to discard the changes.

5.6.4 «System» menu

In system submenu, you may configure system parameters: time, access via different protocols, change password, update software.

5.6.4.1 «Time» submenu

The configuration of time synchronization protocol (NTP) is implemented in time submenu.



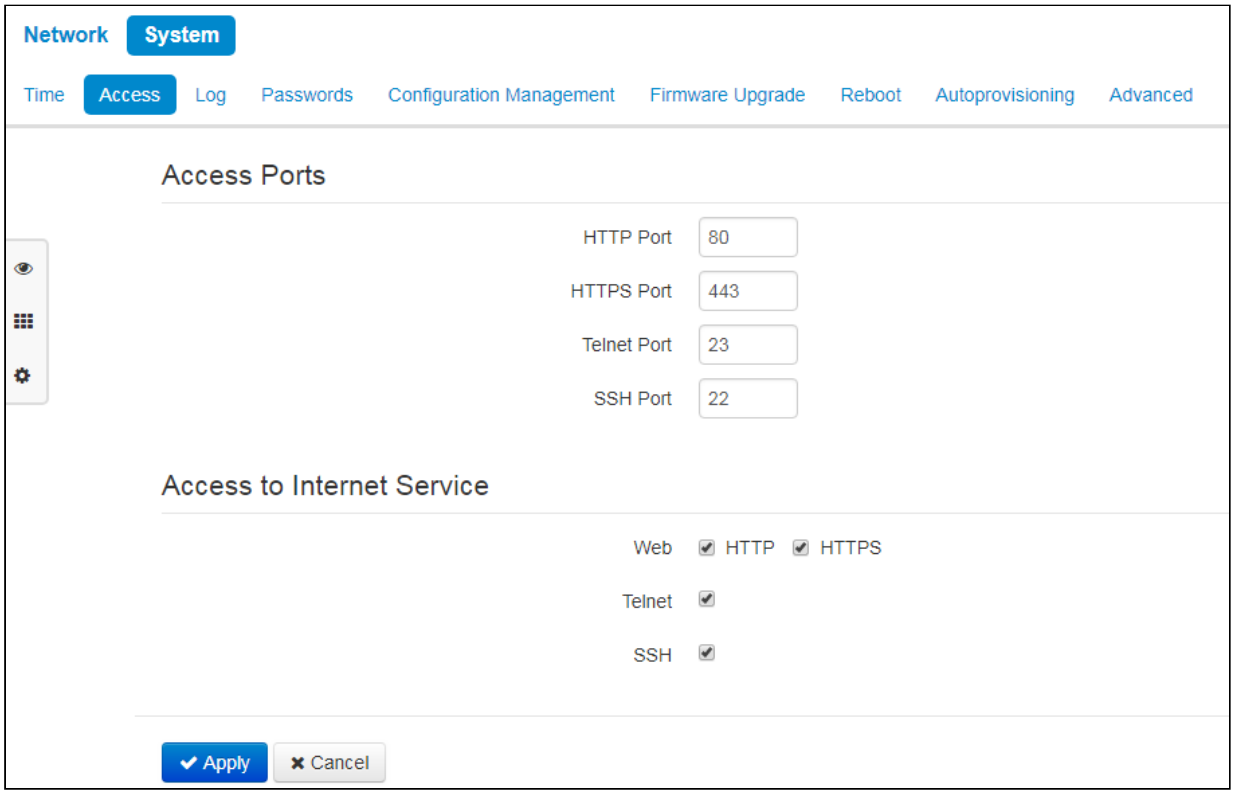
Time Settings

- *Time Zone* – allows you to set a timezone from the list according to the nearest city in your region;
- *Daylight Saving Time Enable* – when selected, automatic daylight saving change will be performed automatically within the defined time period:
  - *DST Start* – daylight saving change starting day;
  - *DST End* – daylight saving change ending day;
  - *DST Offset (minutes)* – time shift in minutes.
- *Enable NTP* – check to enable device system time synchronization with the particular NTP server;
- *NTP Server* – time synchronization server IP address/domain name.

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

5.6.4.2 «Access» submenu

In access submenu, you may configure access to the device via web interface, Telnet and SSH.



Access Ports

In this section you may configure TCP ports for the device access to HTTP, HTTPS, Telnet , and SSH services via LAN port.

- *HTTP port* – number of the port for access to the device web interface via HTTP, default value is 80.
- *HTTPS port* – number of the port for access to the device web interface via *HTTPS* (*HTTP Secure* – secure connection), default value is 443;
- *Telnet port* – number of the port for access to the device web interface via *Telnet*, default value is 23;
- *SSH port* – number of the port for access to the device web interface via *SSH*, default value is 22.

You may use Telnet and SSH protocols in order to access the command line (Linux console).

Access to Internet service

To get access via Internet service interfaces (router mode), set the following permissions:

Web:

- *HTTP* – when checked, connection to the device web configurator through WAN port via HTTP is enabled (insecure connection);
- *HTTPS* – when checked, connection to the device web configurator through WAN port via HTTP is enabled HTTPS (secure connection).

Telnet:

Telnet – a protocol that allows you to establish mechanisms for control over the network. It allows you to remotely connect to the gateway from a computer for configuration and management purposes. To enable the device access via Telnet protocol, select the corresponding checkbox.

SSH:

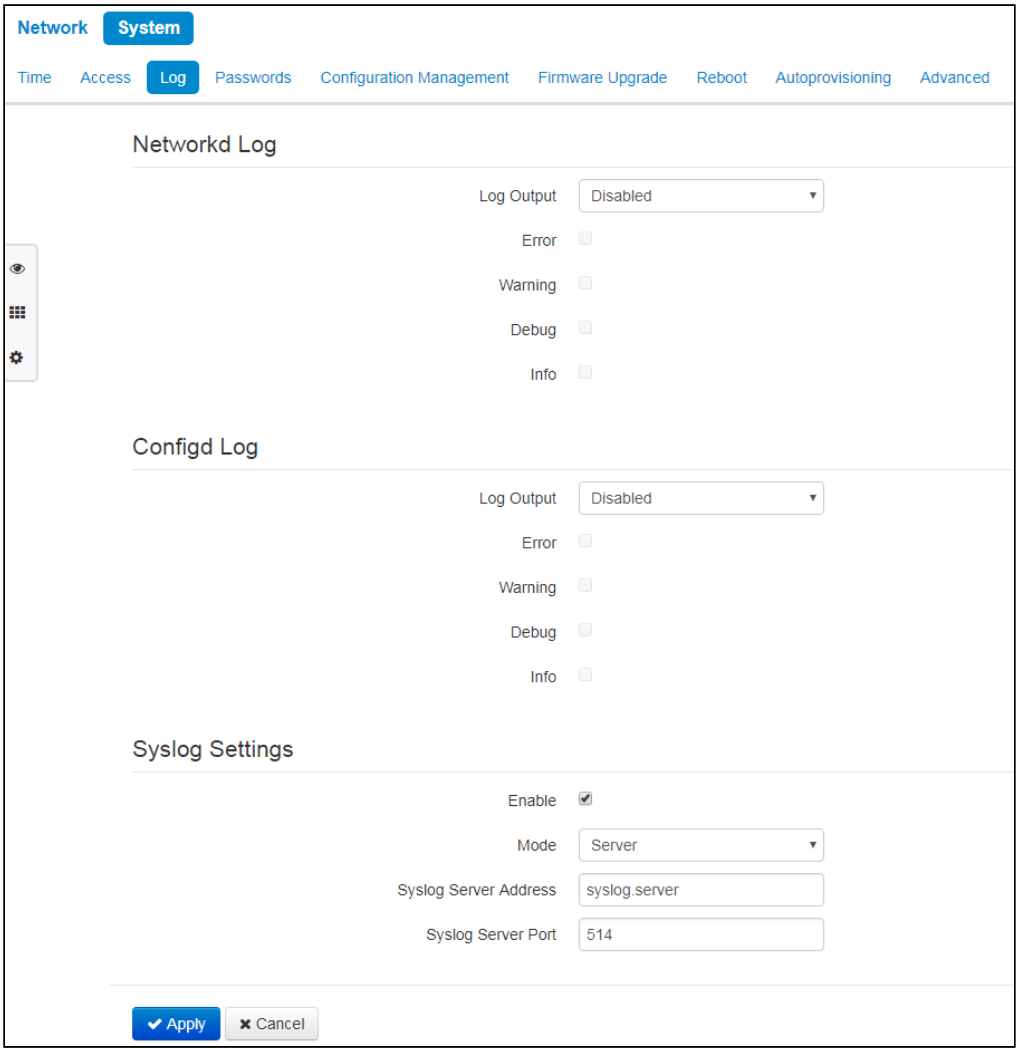
SSH – is a secure device remote control protocol. As opposed to Telnet, SSH encrypts all traffic being transferred including passwords. To enable the device access via SSH protocol, select the corresponding checkbox.

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

5.6.4.3 «Log» submenu

In Log submenu you may configure output for various debug messages intended for device troubleshooting. Debug information is provided by the following device firmware modules:

- Networkd Log – deals with the device configuration according to the configuration file.
- Configd Log – deals with the configuration file operations (config file reads and writes from various sources) and the device monitoring data collection.



Networkd Log

- *Log output* – log messages output direction:
  - *Disabled* – the log is disabled;
  - *Syslog* – messages are output to remote server or local file via syslog protocol (for protocol configuration, see below);
  - *Console* – messages are output to the device console (requires connection via COM port adapter);
  - *Telnet* – messages are output to the telnet session; create telnet protocol connection first.

Select types of messages to be output in Networkd Log:

- *Error* – check to collect «Error» type messages;
- *Warnings* – check to collect «Warning» type messages;
- *Debug* – check to collect debug messages;
- *Info* – check to collect information messages.

Configd Log

- *Log output* – log message output direction:
  - *Disabled* – the log is disabled;
  - *Syslog* – messages are output to remote server or local file via syslog protocol (for protocol configuration, see below);
  - *Console* – messages are output to the device console (requires connection via COM port adapter);
  - *Telnet* – messages are output to the telnet session; create telnet protocol connection first.

Select types of messages to be output in Configd Log:

- *Error* – check to collect «Error» type messages;
- *Warnings* – check to collect «Warning» type messages;
- *Debug* – check to collect debug messages;
- *Info* – check to collect information messages.

Syslog settings

If there is at least a single log (Networkd Log or Configd Log) configured for Syslog output, you should enable Syslog agent that will intercept debug messages and send them to a remote server or save them to a local file in Syslog format.

- *Enable* – when selected, user Syslog agent is launched;
- *Mode* – Syslog agent operation mode:
  - *Server* – log information will be sent to a remote Syslog server (it is also called 'remote log' mode);
  - *Local file* – log information will be saved to a local file;
  - *Server and file* – log information will be sent to a remote Syslog server and saved to a local file.

According to Syslog agent mode, the following settings might be avaliable:

- *Syslog server address* – Syslog server IP address or domain name (required for 'Server' mode);
- *Syslog server port* – port for Syslog server incoming messages (default value is 514; required for 'Server' mode).
- *File name* – name of the file to store log in Syslog format (required for 'File' mode);
- *File size, KB* – maximum log file size (required for 'File' mode).

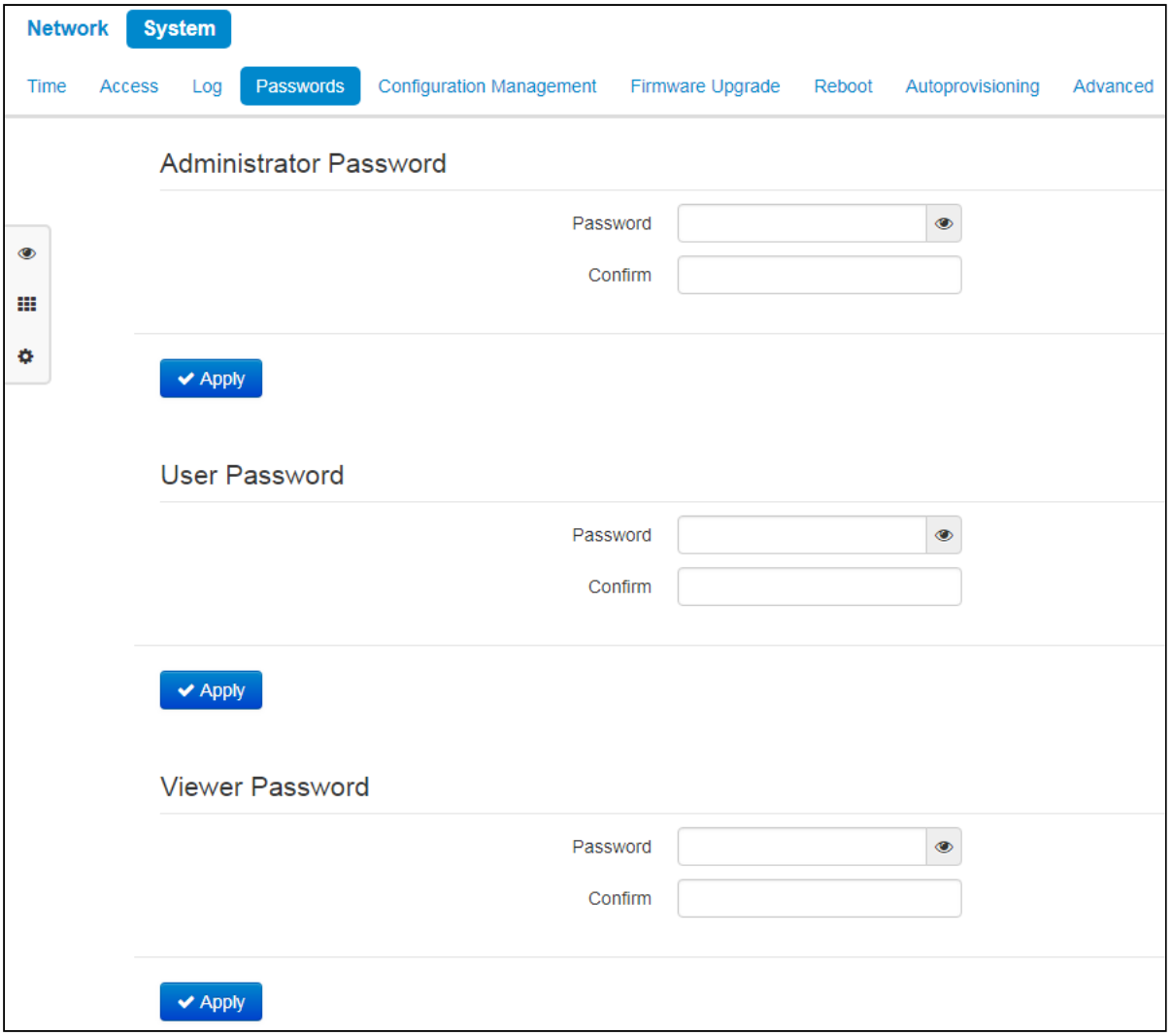
5.6.4.4 «Passwords» submenu

In the 'Passwords' submenu you may define passwords for administrator, non-privileged user, and viewer access.

The set passwords are used for access to the device via web interface, Telnet and SSH.

When signing into web interface, administrator (default password: password) has the full access to the device: read/write any settings, full device status monitoring. Unpriviledge user (password: **user**) has rights to implement network settings (except Internet connection settings) and Wi-Fi settings, to monitor device state. A viewer (password by default: **viewer**) has rights to view configuration and device monitoring data. Viewer is not permitted to change settings.

Admin login: admin
Unpriviledge user login: user
Viewer login: viewer

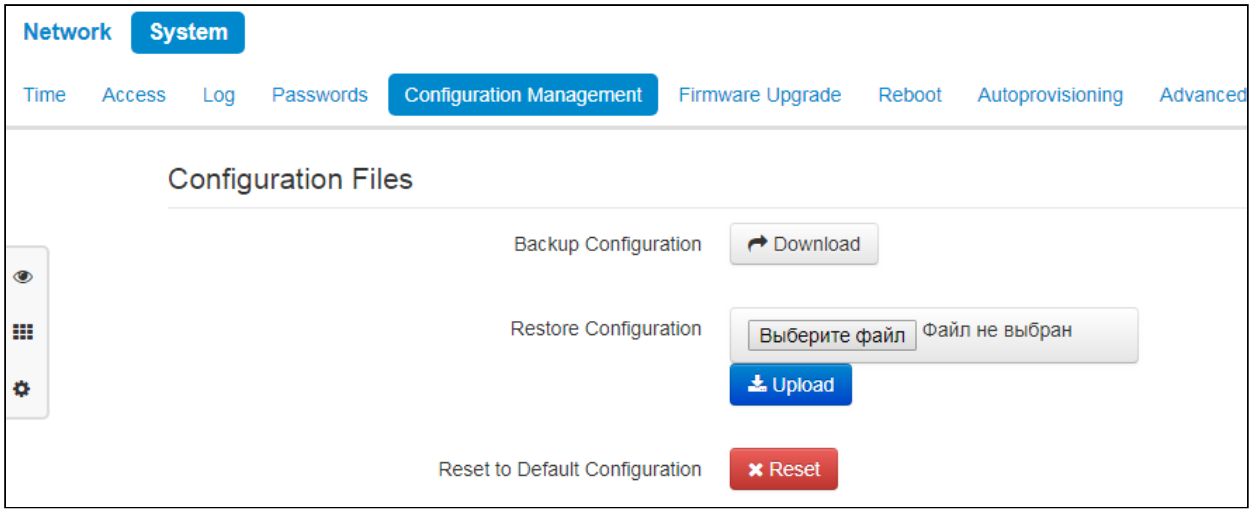


- *Administrator password* – enter administrator password in the corresponding field and confirm it;
- *User password* – enter user password in the corresponding field and confirm it;
- *Viewer password* – enter user password in the corresponding field and confirm it.

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

5.6.4.5 «Configuration management» submenu

In the «Configuration management» submenu you may save and update the current configuration.



Backup Configuration

To save the current device configuration to a local PC, click «Download» button.

Restore Configuration

- *Upload* – to upload configuration from a PC, press «Выберите файл» (Select a file), select a configuration file stored on a local PC (in .tar.gz. format) and press «Upload» button. Uploaded configuration will be applied automatically and does not require device reboot.

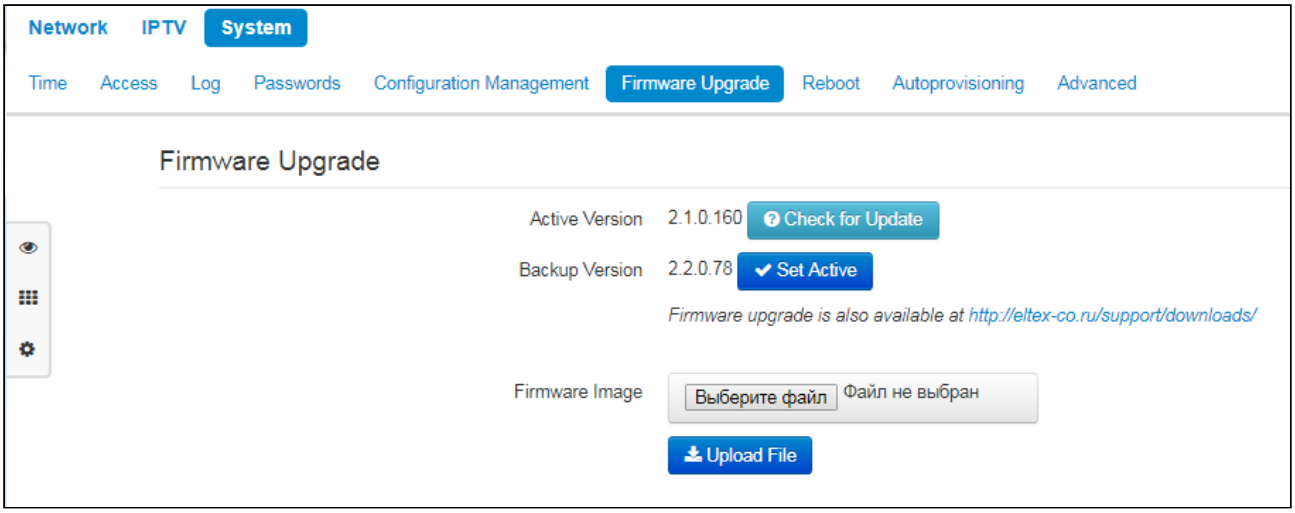
Note that all the passwords of configuration are encrypted with a key depending on device MAC address. Before loading a configuration from one device to another, you should reset all passwords or change them after loading.

Reset to Default Configuration

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

5.6.4.6 «Firmware Upgrade» submenu

Firmware Upgrade submenu is dedicated to update firmware version of the device.



WB-2P-LR5 firmware upgrade:

- *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;
- *Check for upgrade* – click this button to check the availability of the latest firmware version. With this function, you may quickly check the latest firmware version and update the firmware, if necessary;
- *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 check function requires access to the Internet.

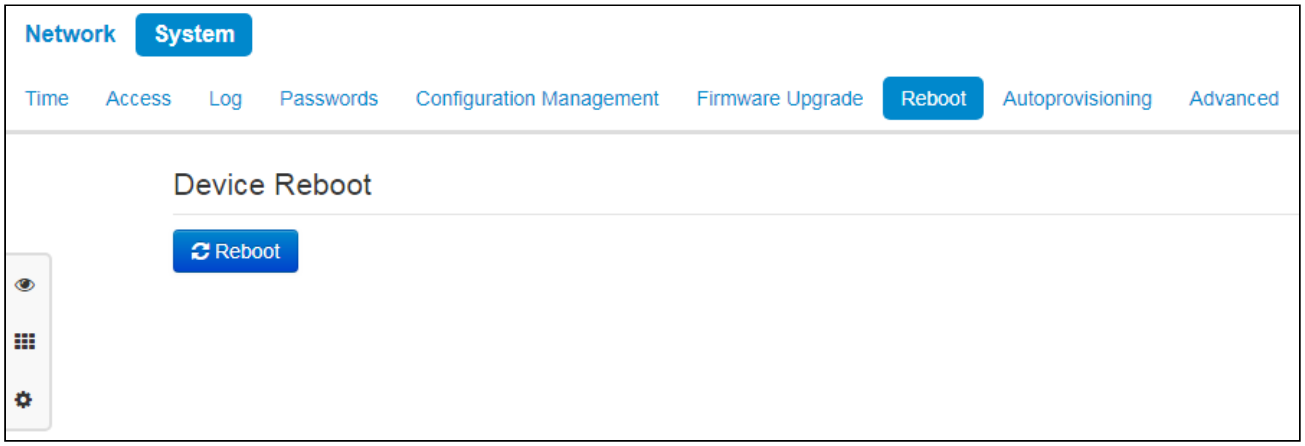
You may update the device firmware manually by downloading the firmware file from the web site http://eltex-co.ru/support/downloads/ and saving it on the computer. To do this, click the 'Select file' button in the *'Firmware update file'* field, and specify path to firmware .tar.gz format file.

To launch the update process, click *'Upload file'* 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 software update. When you update the device from 2.0.0 to 2.1.0 firmware version, you should reset the device to factory settings and configure it once again according your requirements, or preliminary set signal power in Network –> Internet submenu as no more than 16 dBm.

5.6.4.7 «Reboot» submenu

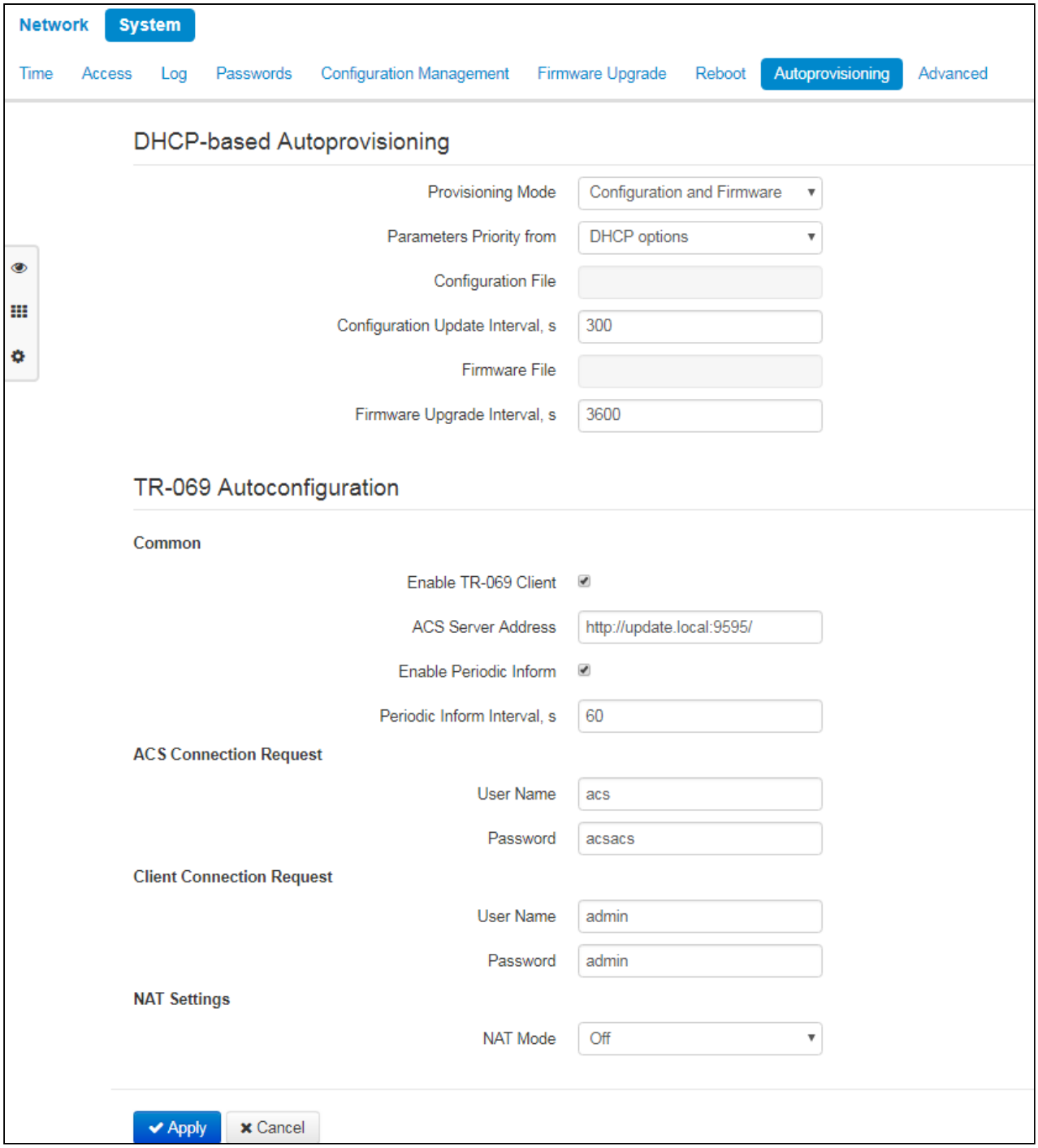
In the «Reboot» submenu you may reboot the device.



Click the «Reboot» button to reboot the device. Device reboot process takes approximately 1 minute to complete.

5.6.4.8 «Autoprovisioning» submenu

In the «Autoprovisioning» submenu you may configure DHCP-based autoprovisioning algorithm and subscriber device automatic configuration protocol TR-069.



DHCP-based Autoprovisioning:

- *Provisioning Mode* – select a mode for automatic device update. The followings are available:
  - *Disabled* – automatic update of configuration and firmware is disabled;
  - *Configuration and Firmware*– periodical configuration and firmware update is permitted;
  - *Configuration only* – only periodical update of configuration is permitted;
  - *Firmware only* – only periodical update of firmware is permitted.
- *Parameters Priority from* – the parameter defines names and locations of configuration and firmware files:
  - *Static settings* – paths to configuration and firmware files are defined by the «*Configuration file*» and «*Firmware file*» settings correspondingly; more detailed information on the algorithm see in section An algorithm of automatic update based on DHCP;
  - *DHCP options* – paths to configuration and firmware files are defined by the DHCP Option 43, 66, and 67 (to do this, you should select DHCP for the Internet service); more detailed information on the algorithm see in section An algorithm of automatic update based on DHCP;

- Configuration File – full path to configuration file – set in URL format (there is an opportunity to load configuration files via TFTP and HTTP):

  tftp://<server address>/<full path to cfg file>
  http://<server address>/<full path to cfg file>
  where < server address > – HTTP- or TFTP server address (domain name or IPv4),
  < full path to cfg file > – full path to configuration file on the server.

- *Configuration Update Interval, s* – time period in seconds that will be used for periodic device configuration update. if 0 is selected, device will be updated only once — immediately after startup.
- *Firmware File* – full path to firmware file – set in URL format (there is an opportunity to load configuration files via TFTP and HTTP):

  tftp://<server address>/<full path to firmware file>
  http://<server address>/<full path to firmware file>
  where < server address > – HTTP- or TFTP server address (domain name or IPv4),
  < full path to firmware file > – full path to configuration file on the server.

- *Firmware Upgrade Interval, s* – a time interval. The firmware update is implemented according to this period. If 0 is set, update of the device will be implemented once, right after reloading of the device.

More detailed information on the algorithm see in section An algorithm of automatic update based on DHCP.

Autoconfiguration via TR-069:

Common:

- *Enable TR-069 Client* – when checked, the operation of embedded TR-069 client is enabled, otherwise it is prohibitted.
- *ACS Server Address* – autoconfiguration server address. The address should be enterred in the following formats http://<address>:<port> or https://<address>:<port> (<address> – IP address or domain name of ACS server, <port> – ACS server port, the default port is 10301). The second format is to use the secure protocol – HTTPS for exchanging data with ACS server.
- *Enable Periodic Inform* – when checked, embedded TR-069 client implements periodic poll of ACS server with interval equal to «Periodic Inform Interval» value in seconds. The poll aim is to detect device configuration changes.

ACS Connection Request :

- *User Name, Password* – user name and password for client to access ACS server.

Client Connection Request :

- *User Name, Password* – user name and password for ACS server to access TR-069 client.

NAT Settings :

If there is modification of network addresses between client and ACS server (NAT – network address translation), ACS server might not have the opportunity to establish connection with the client if certain technologies are not used to avoid it. The techologies help the client to define so called public address (NAT addresses – an address of external gateway, behind which the client is located). When the public address is defined, the client inform the server. Then, the server uses the public address (not the local) to establish connection with the client.

- *NAT mode* – defines how client should obtain public address. The following modes are available:
  - *STUN* – use STUN protocol for defining public address;
  - *Manual* – manual mode, when public address is set manually in the configuration; in this mode, you should add the rule for forwarding of TCP port used by TR-069 client on the device implementing NAT functions.
  - *Off* – do not use NAT – the mode is recommended to be used only when the device is connected to ACS server directly, without network addresses modification. In this case, public address coincides with local one.

When STUN mode is selected you should configure the following settings:

- *STUN Server Address* – IP address or domain name of STUN server;
- *STUN Server Port* – UDP port of STUN server (the value by default is 3478);
- *Minimum Keep Alive Period, s* and *Maximum Keep Alive Period, s* – defines time interval for sending messages to STUN server periodically to detect public address changing.

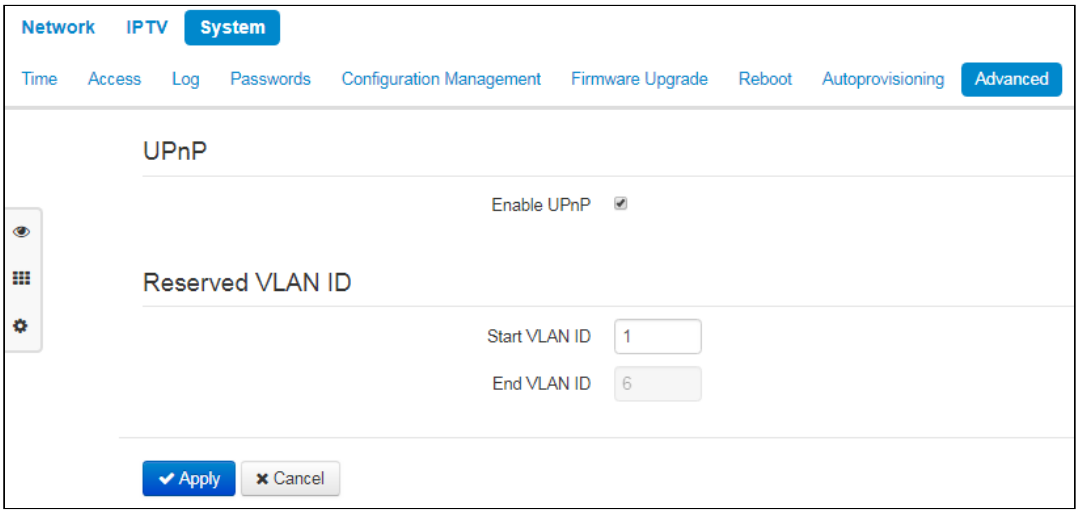
When Manual mode is selected, client address is set manually in *NAT Address* parameter (the address should be set in IPv4 format).

Through TR-069, you may implement main configuration of the device, firmware update and reading the data on the device (firmware version, model, serial number, etc.), uploading/downloading of configuration file, remote reboot (TR-069, TR-098, TR-104 specifications are supported).

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

5.6.4.9 «Advanced» submenu

Use the menu to set reserved VLAN ID and enable UPnP.



UPnP

UPnP is used by some applications (e.g. DC clients such as FlylinkDC++) to create forwarding rules for TCP/UDP ports used by these applications on a higher router. It is recommneded to enable UPnP for operation of file exchange services on a network.

- *Enable UPnP* – when checked, UPnP is enabled, otherwise – disabled.

Reserved VLAN ID

Reserved VLAN ID – the list of service VLANs, which are used for for solving intrasystem tasks.

- *Start VLAN ID* – starting VLAN ID value in the reserved range;
- *EndVLAN ID* – ending VLAN ID value in the reserved range.

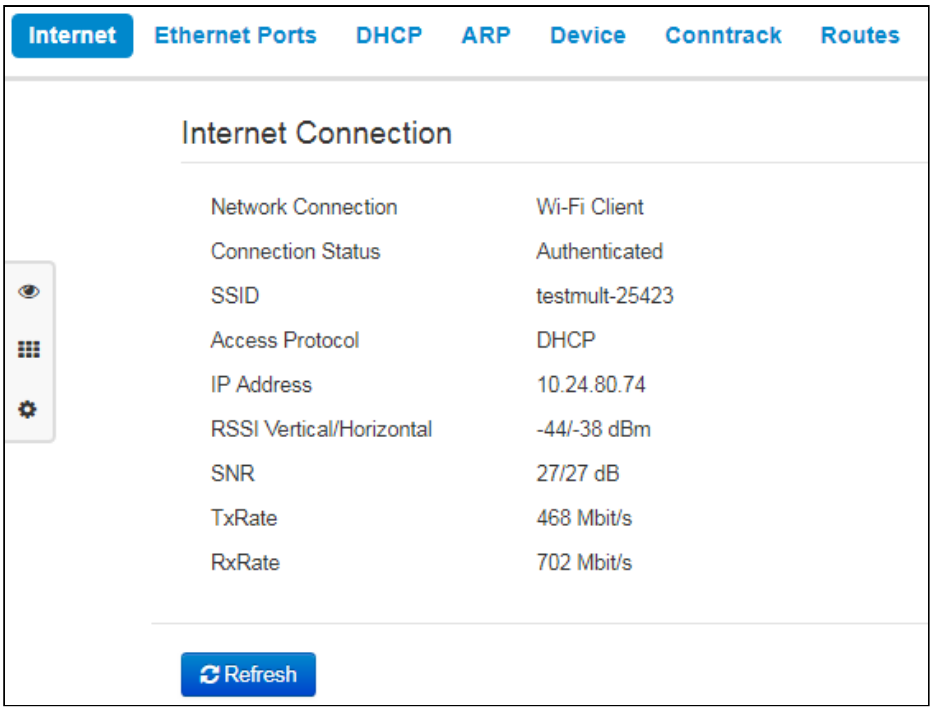
5.7 System monitoring

To move to monitoring mode, select «Monitoring» on the left panel.

Some pages are not updated automatically. To obtain current state of the device, press Refresh.

5.7.1 «Internet» submenu

In the Internet submenu, you may view main network settings of the device.



Internet Connection

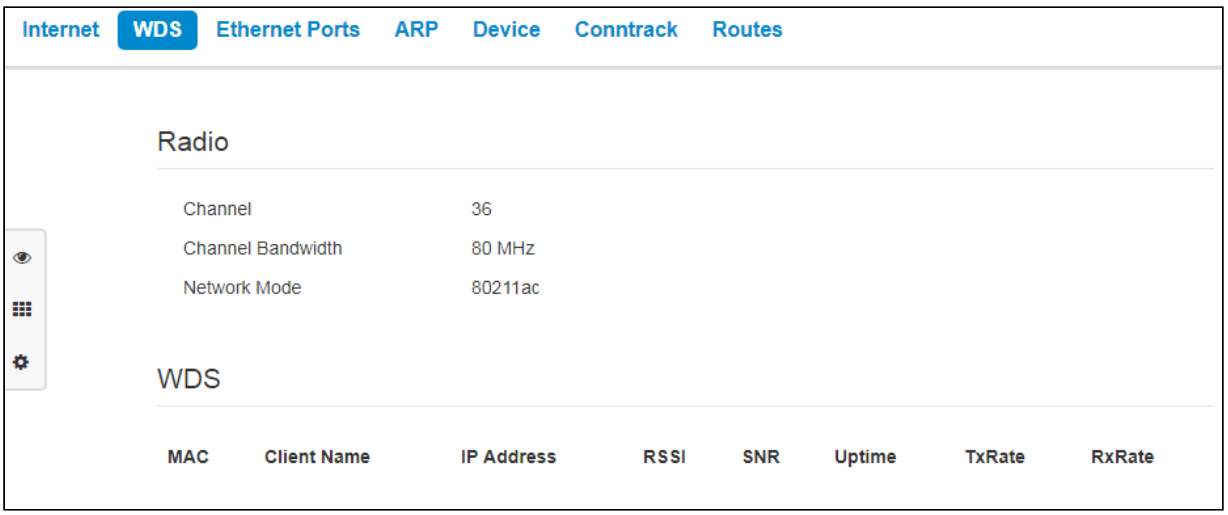
- *Network connection* – the parameter shows the type of connection to the Internet;
- *Connection Status* – the parameter shows state of connection to external Internet network;
- *SSID* – a name of wireless network, to which the device is connected;
- *Access Protocol* – a protocol which is used for access to Internet;
- *IP Address* – device IP address in the external network;
- *RSSI Vertical/Horizontal* – level of signal received from base station, dBm;
- *SNR* – signal/noise ratio, dB;
- *TxRate* – data rate of transmission, Mbps;
- *RxRate* – data receive rate, Mbps.

Press «Refresh» button to update the page.

5.7.2 «WDS» submenu

«WDS» submenu is available only in Wirelees bridge mode.

You may view radiointerface settings and wireless bridge state in WDS submenu.



Radio:

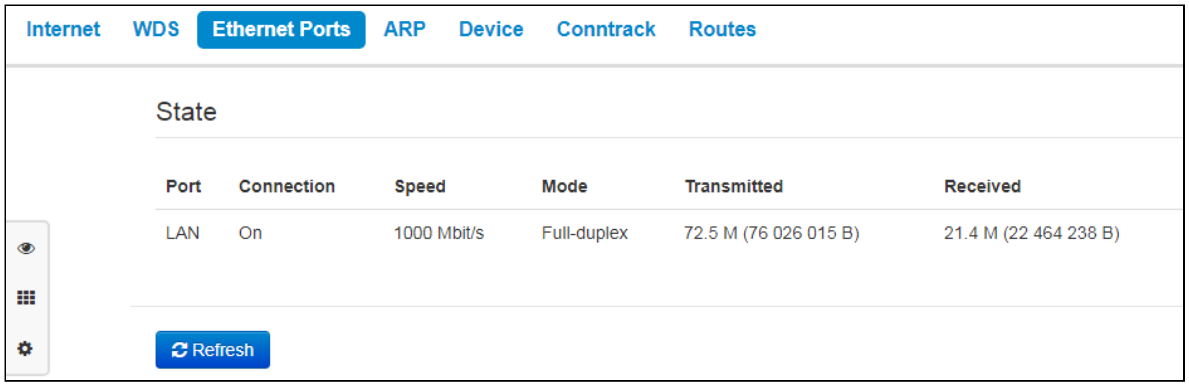
- *Channel* – a channel of wireless bridge;
- *Channel Bandwidth* – channel bandwidth used for wireless bridge;
- *Network mode* – the current network mode of the radiointerface.

WDS:

- *MAC address* – MAC address of the opposite device;
- *Client Name* – network name of the opposite device;
- *IP address* – IP address of the opposite device;
- *RSSI* – level of signal received from the opposite device, dBm;
- *SNR* – signal/noise ratio, dB;
- *Uptime* – time of wireless bridge operation;
- *TxRate* – channel data rate of transmission, Mbps;
- *RxRate* – channel data rate of receiving, Mbps.

5.7.3 «Ethernet ports» submenu

You may view Ethernet ports' state in Ethernet Ports submenu.



State

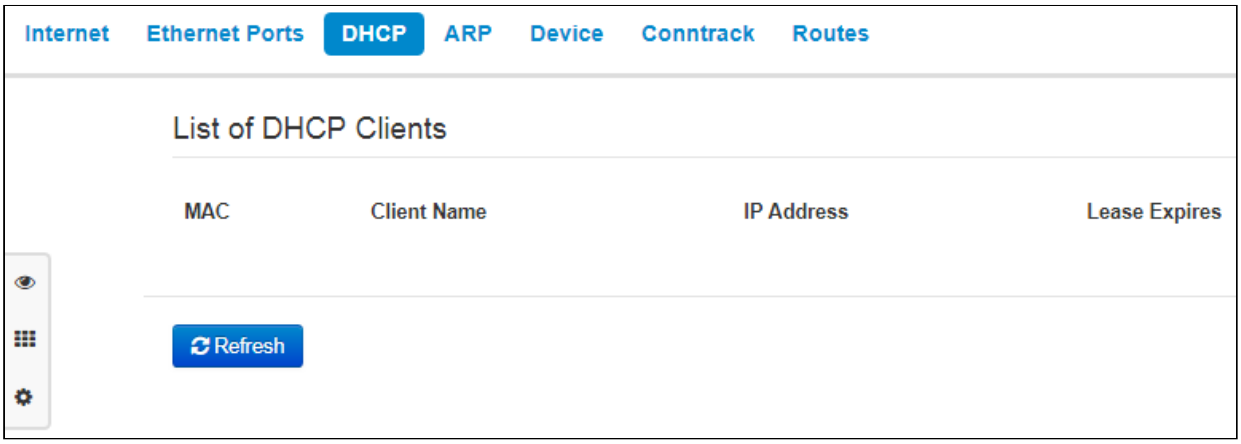
- *Port* – a port name:
  - *LAN* – a local network port.
- *Connection* – port connection state:
  - *On* – network device is connected to the port (connection is active);
  - *Off* – network device is not connected to the port (connection is inactive).

- *Speed* – speed of external network device connection to the port (10/100/1000 Mbps);
- *Mode* – data transmission mode:
  - *Full-duplex* – full-duplex mode;
  - *Half-duplex* – half-duplex mode;
- *Transmitted* – the quantity of bytes transmitted from the port;
- *Received* – the quantity of bytes received by the port.

To obtain current information on Ethernet ports states, press «Refresh» button.

5.7.4 «DHCP» submenu

The list of network devices connected to LAN (WLAN) interface of the device, whose IP addresses were assigned by local DHCP server, is given in DHCP submenu. The expire time of address lease is shown in the table as well.



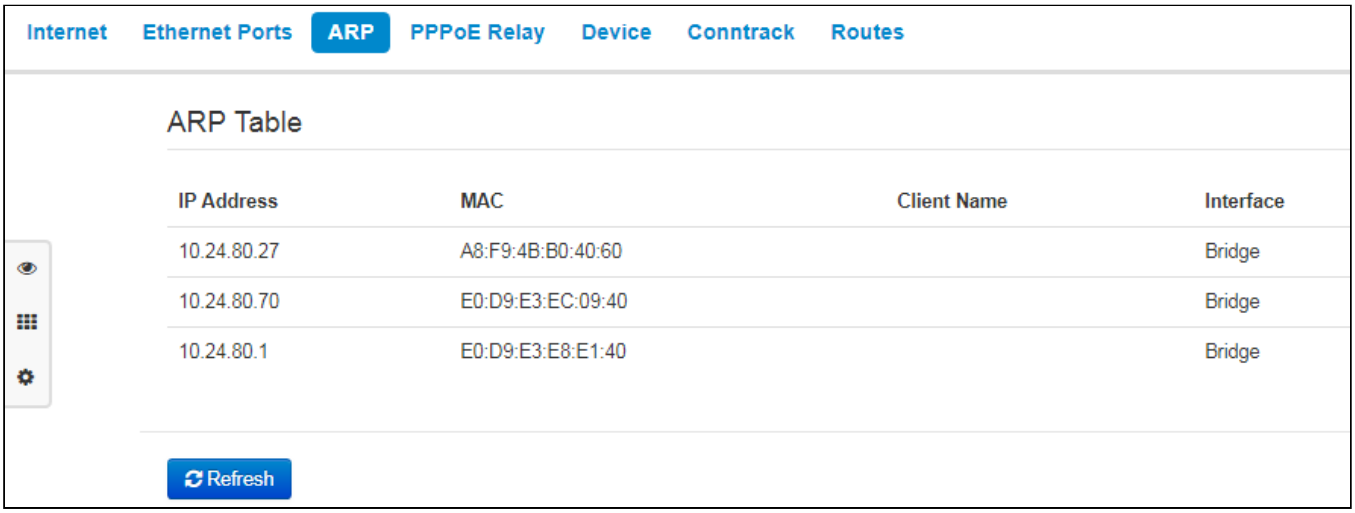
List of DHCP Clients

- *MAC* – MAC address of connected device;
- *Client name* – network name of connected device;
- *IP address* – IP address assigned from adresses pool;
- *Lease Expires* – time range after which the lease of the address expires.

To obtain current information on DHCP clients, press «Refresh» button.

5.7.5 «ARP» submenu

You may view ARP table in ARP submenu. ARP table contain information on IP and MAC addresses mapping.



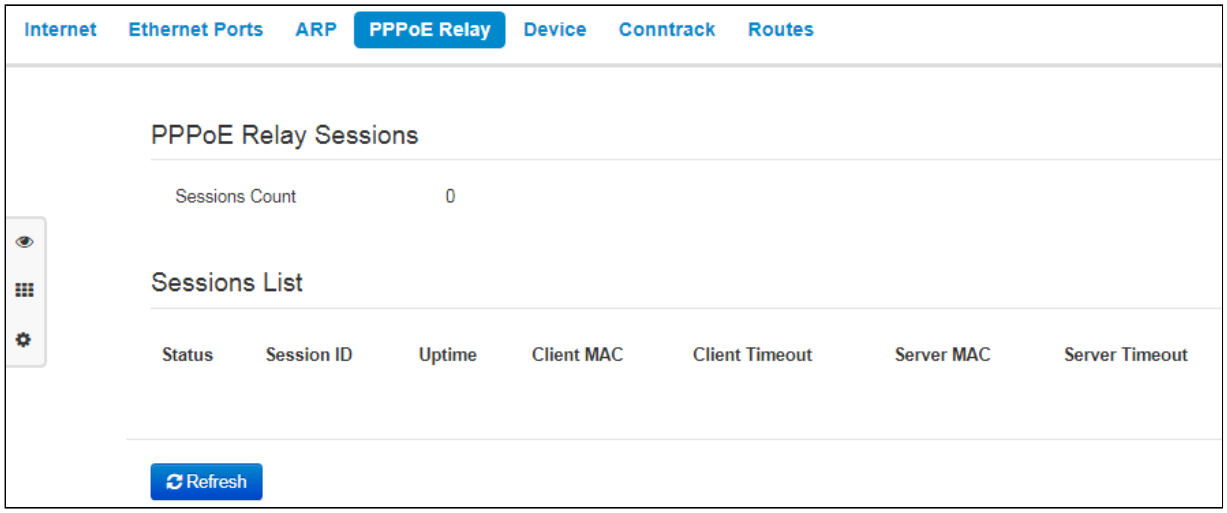
ARP Table

- *IP address* – device IP address;
- *MAC* – device MAC address;
- *Client name* – device hostname (if there is one);
- *Interface* – interface of the device active side: WAN, LAN or Bridge.

To obtain current information on Ethernet ports states, press «Refresh» button.

5.7.6 «PPPoE Relay» submenu

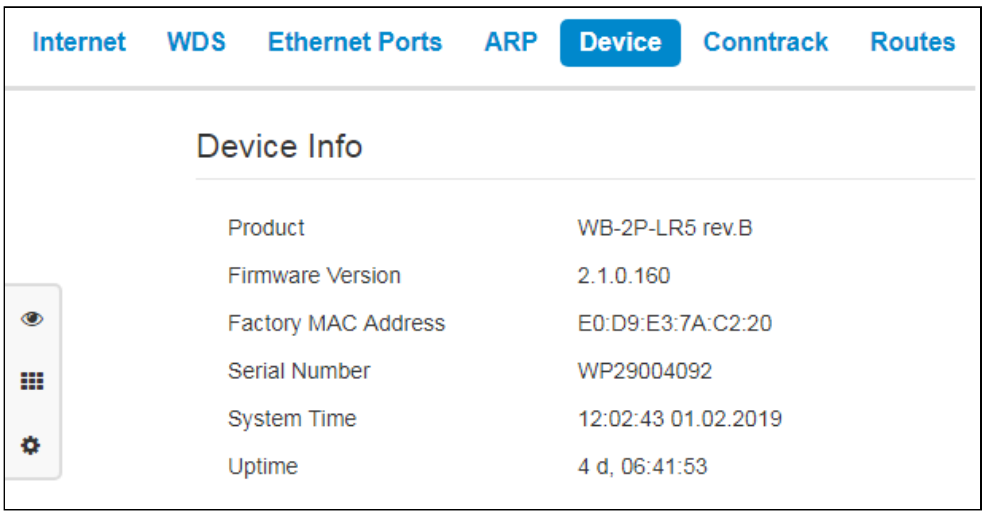
«PPPoE Relay» submenu is available only in Wireless station mode



- *Sessions Count* – the quantity of PPPoE sessions established through the device. The maximum value – 32.
- *Status* – active or inactive session.
- *Session ID* – number of session.
- *Uptime* – session uptime.
- *Client MAC* – MAC address of a client.
- *Client Timeout* – time when the last packet from the client is received.
- *Server MAC* – MAC address of a server.
- *Server Timeout* – time when the last packet from the server is received.

5.7.7 «Device info» submenu

General information on the device is given in Device submenu.

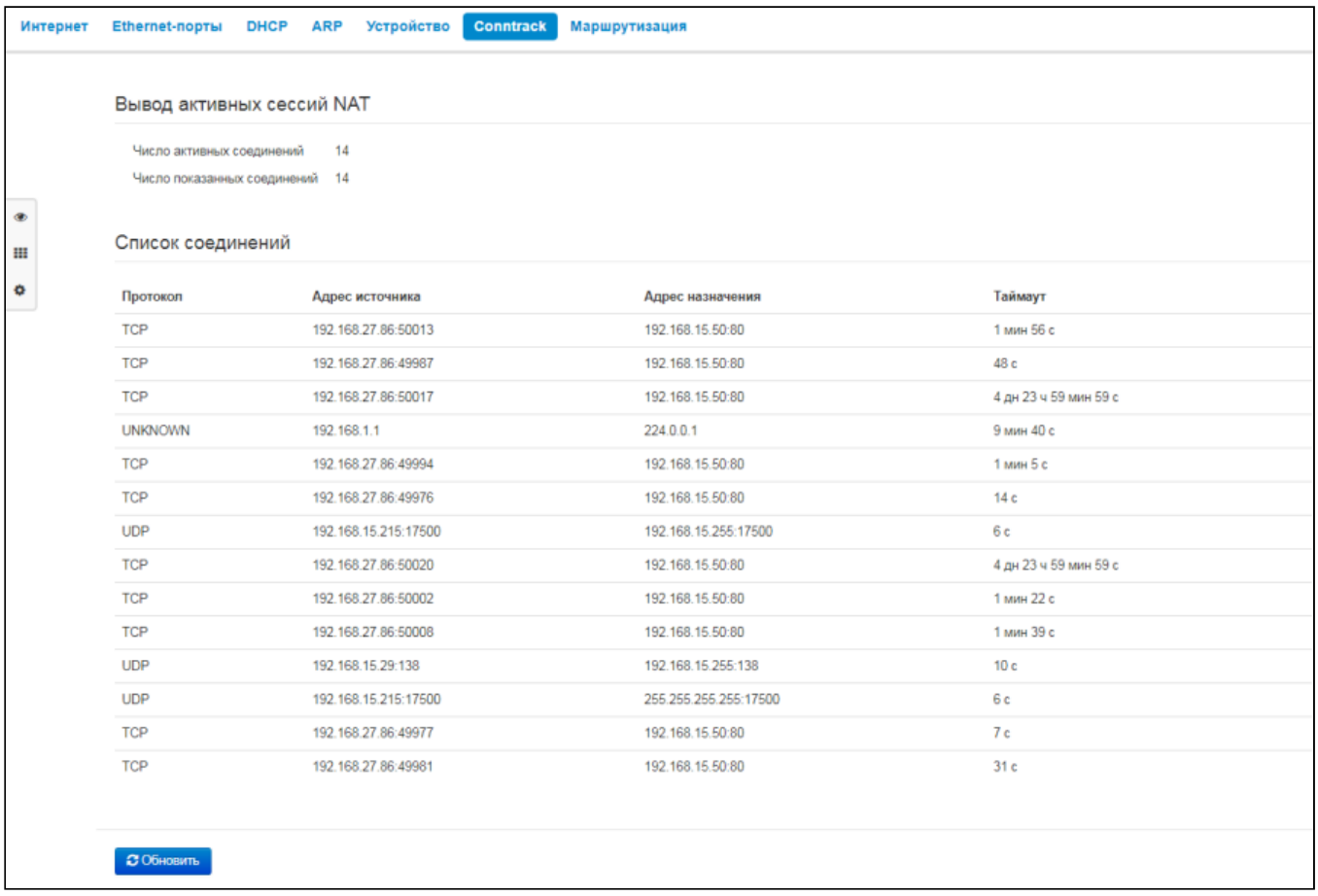


Device info

- *Product* – device model name;
- *Firmware Version* – device firmware version;
- *Factory MAC Address* – MAC address of the device's WAN interface, defined by the manufacturer;
- *Serial number* – device serial number defined by the manufacture;
- *System time* – current time and date set in the system;
- *Uptime* – time of operation since the last startup or reboot of the device.

5.7.8 «Conntrack» submenu

In the «Conntrack» submenu you may find the current active network connections of the device.



Active NAT Session

- *Active Connections* – total number of active network connections;
- *Shown Connections* – number of connections shown in the WEB interface. In order to maintain high performance of the WEB interface, the maximum number of connections shown is limited to 1024. You may view other connections through the device command console.

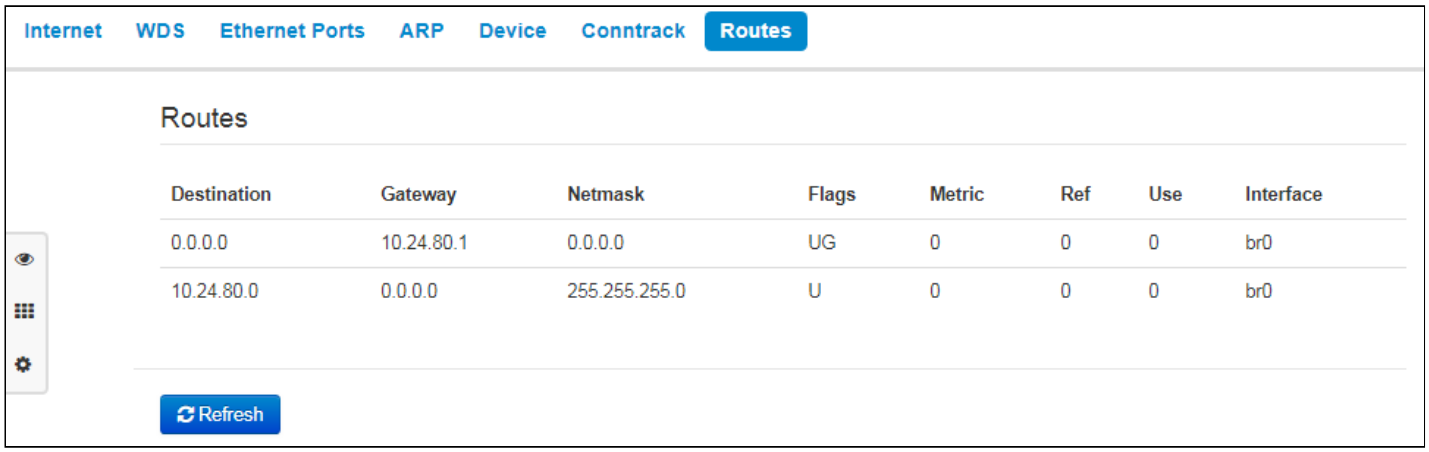
Connections List

- *Protocol* – protocol through which the connection has been established;
- *Source Address* – IP address and port number of the connection initiator;
- *Destination* – destination IP address and port number;
- *Timeout* – time period until the connection termination.

To obtain current information on Ethernet ports states, press «Refresh» button.

5.7.9 «Routes» submenu

In Routes submenu you may view the device route table.

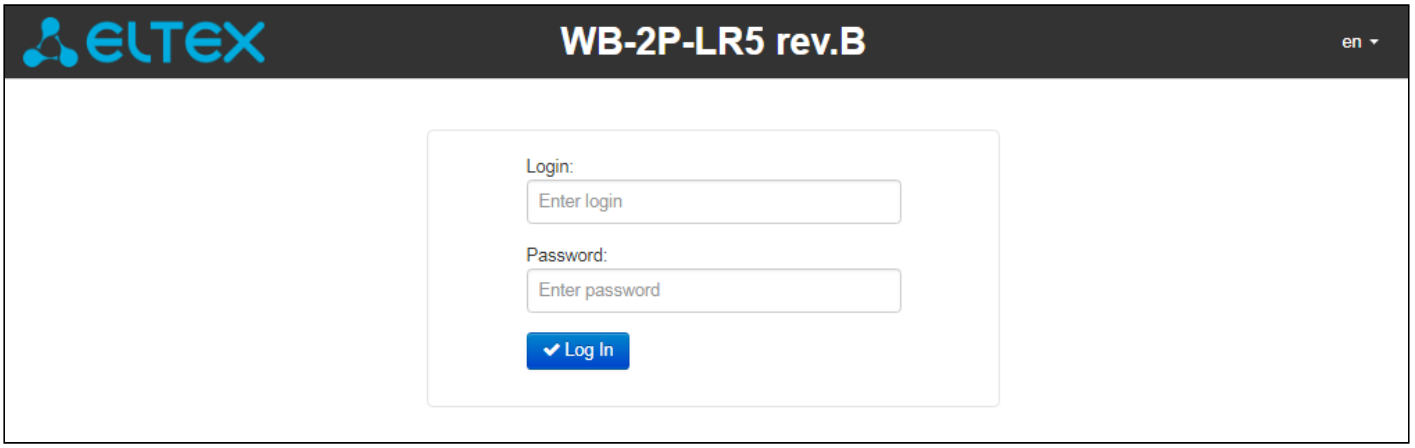


- *Destination* – IP address of destination host or subnet that the route is established to;
- *Gateway* – IP address of the gateway, through which access to the addressee is implemented;
- *Netmask* – subnet mask;
- *Flags* – specific route attributes. The following flag values exist:
  - **U** – means 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.
  - **A** – means buffered route with corresponding record in the ARP table.
  - **C** – 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.
  - **B** – 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.
- *Metric* – defines route cost. Metrics allows you to sort the duplicate routes, if they are exist in the table.
- *Ref* – identified number of references to the route for connection establishment (not used by the system).
- *Use* – number of route detections performed by IP protocol.
- *Interface* – name of the network interface that the route lies through.

To obtain current information on Ethernet ports states, press «Refresh» button.

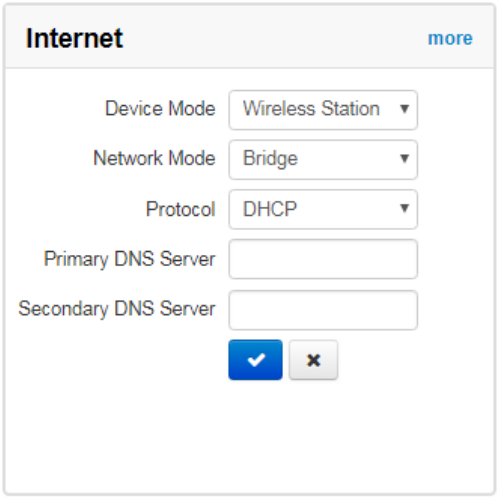
6 Configuration example

1. Connect PC to LAN port of injector;
2. Enter IP address of the device to URL bar of a browser (192.168.1.1 by default, if address was not obtain via DHCP);
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**).



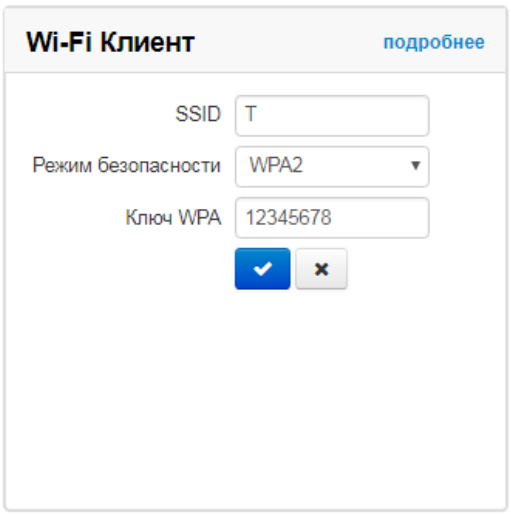
If the window is not displayed, make sure that the PC and the device are in the same network.

4. Implement configuration on Internet tile. In Network Mode field, select the required mode: Bridge or Router. If static settings are used for connection to a provider network, choose «Static» value in «Protocol» field and fill the fields: «IP address», «Netmask», «Default gateway», «Primary DNS Server», «Secondary DNS Server» – the values are given by service provider. Press  to save and apply settings.



To specify additional parameters, move to extended settings mode using «more» link (see section «Internet» submenu)

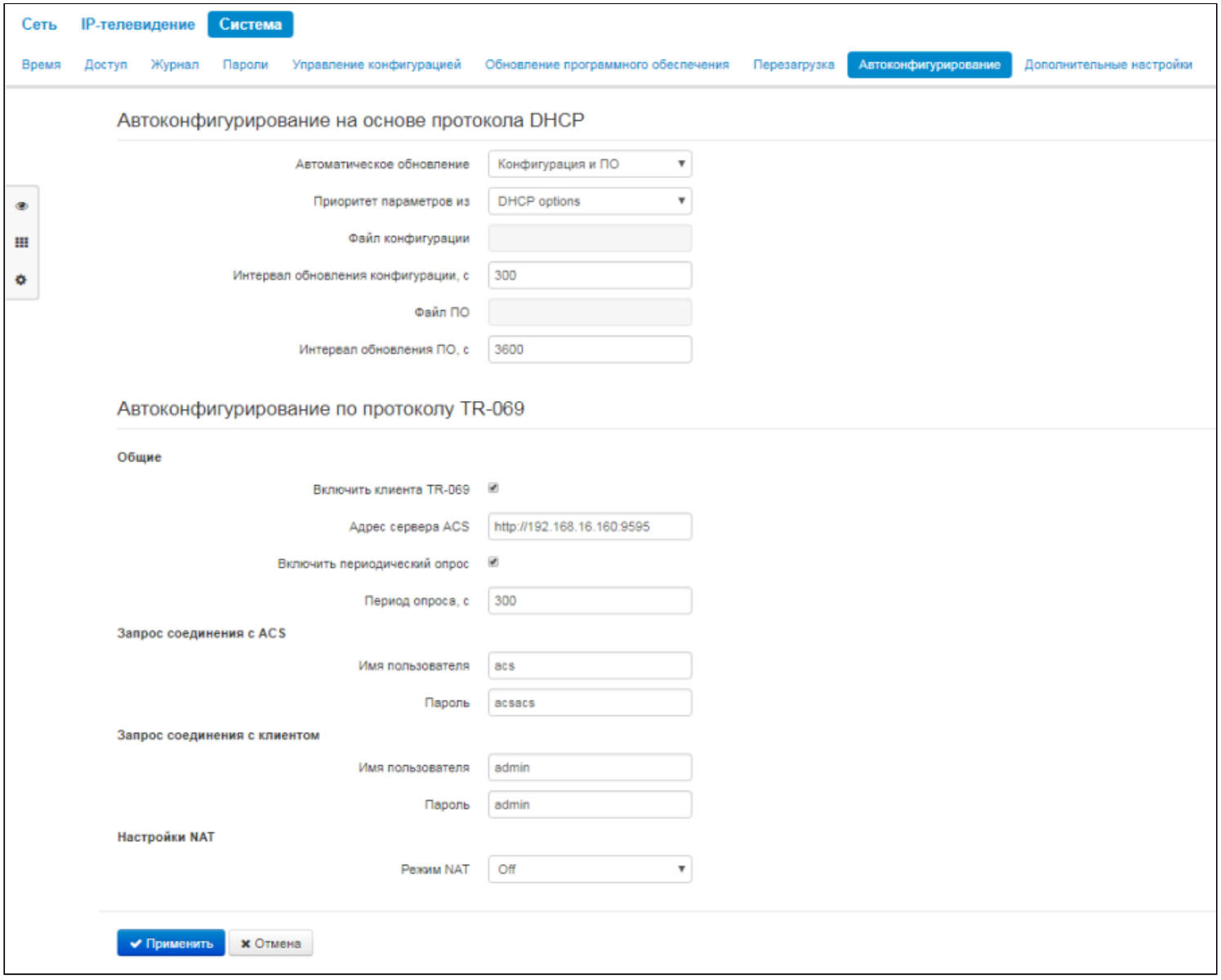
5. Configure conection to a base station. Specify SSID of the wireless network, you want to connect to, in the corresponding field. Select security mode through which authentication of the selected wireless network is implemented.



To set additional parameters and scan environment to find necessary access point, move to extended settings mode using «more» link (see section «Internet» submenu).

Press to save and apply settings.

7 Device automatic update algorithm based on DHCP



Device automatic update algorithm is defined by the «*Parameters Priority from*» value.

1. If the «*Static settings*» value is selected, then the full path (including access protocol and server address) to configuration file and firmware file will be defined by «Configuration file» and «Firmware file» parameters. Full path should be specified in URL format (HTTP and TFTP are supported): <protocol>://<server address>/<path to file>, where

   - <protocol> – protocol used for downloading corresponding files from the server (HTTP and TFTP are supported);
   - <server address> – address of the server with a file to be downloaded (domain name or IPv4);
   - <path to file> – path to file on the server.

   You may use the following macro in URL (reserved words substituted with the specific values):

   - *$MA* – MAC address – the macro is substituted with device's MAC address in file URL;
   - *$SN* – Serial number – the macro is substituted with device's serial number in file URL;
   - *$PN* – Product name – the macro is substituted with device's model name in file URL (e.g., WB-2P-LR5).

For MAC address, serial number and model name, see «Device» section on the monitoring page.
URL examples:

tftp://download.server.loc/firmware.file,

http://192.168.25.34/configs/WB-2P-LR5//my.cfg,

tftp://server.tftp/$PN/config/$SN.cfg,

http://server.http/$PN/firmware/$MA.frm and etc.

Some URL parameters might be omitted. For example, configuration file may be specified in the following format:

http://192.168.18.6
or
config_wb.cfg

If the system is unable to extract the necessary file downloading parameters (protocol, server address or path to file on server) from configuration file or firmware file URL, it will attempt to extract an unknown parameter from DHCP Option 43 (Vendor specific info) or 66 (TFTP server) and 67 (Boot file name), when address obtaining via DHCP is enabled for the Internet service (DHCP option format and analysis will be provided below). If the system is unable to extract missing parameter from DHCP options, default value will be used:

- portocol: tftp;
- server address: update.local;
- configuration file name: wb-2p-lr5.cfg;
- firmware file name: wb-2p-lr5.fw.

Thus, if you leave *'Configuration file'* and *'Firmware file'* fields empty, and Options 43 or 66, 67 with file locations are not obtained via DHCP, configuration file URL will be as follows:

tftp://update.local/wb-2p-lr5.cfg,
and the firmware file URL:
tftp://update.local/wb-2p-lr5.fw.

2. If 'DHCP options' value is selected, configuration file and firmware file URLs will be extracted from DHCP Option 43 (Vendor specific info) or 66 (TFTP server) and 67 (Boot file name), thus, address obtaining via DHCP should be enabled for the Internet service (DHCP option format and analysis will be provided below). If URL parameters are not provided by DHCP options, default parameters values will be used:

- portocol: tftp;
- server address: update.local;
- configuration file name: wb-2p-lr5.cfg;
- firmware file name: wb-2p-lr5.fw.

Option 43 format (Vendor specific info)

1|<acs_url>|2|<pcode>|3|<username>|4|<password>|5|<server_url>|6|<config.file>|7|<firmware.file>|8|<vlan_tag>

1 – TR-069 autoconfiguration server address code;

2 – «Provisioning code» parameter specification code.

3 – code of the username for TR-069 server authorization;

4 – code of the password for TR-069 server authorization;

5 – server address code; server address URL should be specified in the following format: tftp://address or http://address . The first version represents TFTP server address, the second version – HTTP server address;

6 – configuration file name code;

7 – firmware file name code;

8 – a code of VLAN tag for management;

«|» – mandatory separator used between codes and suboption values.

Algorithm of identification for configuration file and firmware file URL parameters from DHCP Options 43 and 66, 67.

1. DHCP exchange initialization
   Device initializes DHCP exchange after the startup.

2. Option 43 analysis
   When Option 43 has been received, suboption 4 is analyzed (vlan_tag):
   - if there is a suboption and it is different from current VLAN tag, DHCP exchange is initiated in new VLAN;
   - if there is no suboption or suboption is not different from current VLAN tag, the analysis of suboptions with codes 1, 2 and 3 to define server address and names of configuration files and firmware files.

3. Option 66 analysis

If Option 43 is not received from DHCP server or it is received but the system fails to extract the server address, Option 66 will be searched. If the system fails to obtain the firmware file name, Option 67 will be searched. They are used for TFTP server address and the firmware file path extraction respectively. Then, configuration and firmware files will be downloaded from Option 66 address via TFTP.

Special aspects of configuration updates

Configuration file should be in **.tar.gz** format (this format is used when configuration is saved from the web interface in the «System» – «Configuration management» tab). Configuration downloaded from the server will be applied automatically and does not require device reboot.

Special aspects of firmware updates

Firmware file should be in **.tar.gz** format. When the firmware file is loaded, the device unpacks it and checks its version (using 'version' file in **tar.gz** archive).

If the current firmware version matches the version of the file obtained via DHCP, firmware will not be updated. Update is performed only when firmware versions are mismatched. When the firmware image is written into the device flash memory, the Power indicator will flash green, orange and red in succession.

Do not power off or reboot the device, when the firmware image is written into the flash memory. These actions will interrupt the firmware update that will lead to the device boot partition corruption. The device will become inoperable. To restore the device operation, use the instruction provided in System recovering after firmware update failure.

8 System recovering after firmware update failure

If while the firmware update (through the web interface or through autoupdate mechanism based on DHCP) a failure occured (e.g. due to power cutoff) and the device does not operate (the «Power» indicator is constantly solid red), use the following algorithm to recover the device:

- Unpack the archive with firmware file.
- Connect PC to the device port. Set the following subnet mask on the network interface: 192.168.1.0/24.
- Launch TFTP client on PC (it is recommended to use Tftpd32 programm for Windows). Set 192.168.1.6 as remote host and select file *linux.bin* from the unpacked archive to transmit.
- Launch the command to transmit the file to remote host (**Put** command). The process of file transmission will be launched.
- If the transmission has started, please, wait for finishing. The device will write the firmware to its memory and launch the system automatically. The time of writing takes approximately 8 minutes. If the process is completed successfully, «Power» indicator will be green or orange. The configuration of the device before failure is saved. If you can not connect the device, reset it to factory settings.
- If the process has not started, make sure that the network settings of PC are correct and try again. If it does not work, sent the device to maintanence service or proceed recovery using the connection via COM port through a special adapter (if available).

9 Application A. Launch user script when starting the system

Sometimes you need the device to implement certain actions when starting, which cannot be implemented through settings in configuration file. In this case you may configure a user script through a configuration file that will be launched when the system starting. You may set any needed commands sequence.

For user script launching, there is a settings section in the configuration file cfg.yaml:

UserScript:
Enable: "0"
URL: ""

Option «*Enable*» permits (if the value is 1) or forbids (if the value is 0) launch of the script, path to which is in *URL* parameter.

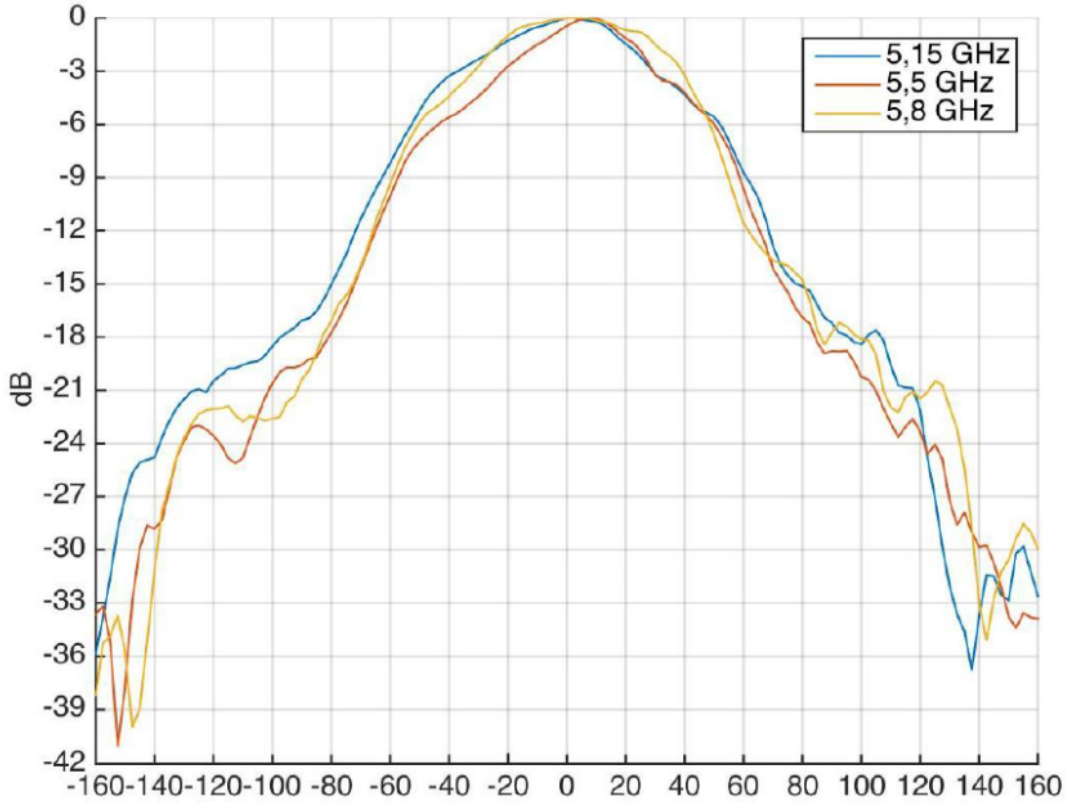
The userscript might be located on remote server as well as on the device. The script is loaded via HTTP or TFTP from remote server. Examples of configuration files for user script launching using different sources are given below:

1. Launch from HTTP server
   To launch a script from HTTP server, enter the entire path to the file in HTTP-URL format to URL parameter:
   URL: " http://192.168.0.250/user-script/script.sh "
   In this case, after the device started, file script.sh, which is kept in the catalogue having 192.168.0.250 address, will be automatically loaded via HTTP from the defined server. Then it will be launched.
2. Launch from TFTP server
   To launch a script from TFTP server, enter the entire path to the file in TFTP-URL format to URL parameter :
   URL: " tftp://192.168.0.250/user-script/script.sh "
   In this case, after the device started, file script.sh, which is kept in the catalogue having 192.168.0.250 address, will be automatically loaded via TFTP from the defined server. Then it will be launched.
3. Local script launch
   Due to the peculiar properties of the file system, a local script should be stored in /etc/config catalogue as the content of the catalogue is saved after device reload. You may create script in /etc/config catalogue through vi editor or load it from TFTP server using *tftp –gl user.sh <TFTP-server address>* command. After creating a script, you should set rights for launching using the following command:
   chmod 777 /etc/config/user.sh
   In configuration file, URL for local script launching should be set as follows:
   URL: " File://etc/config/user.sh "

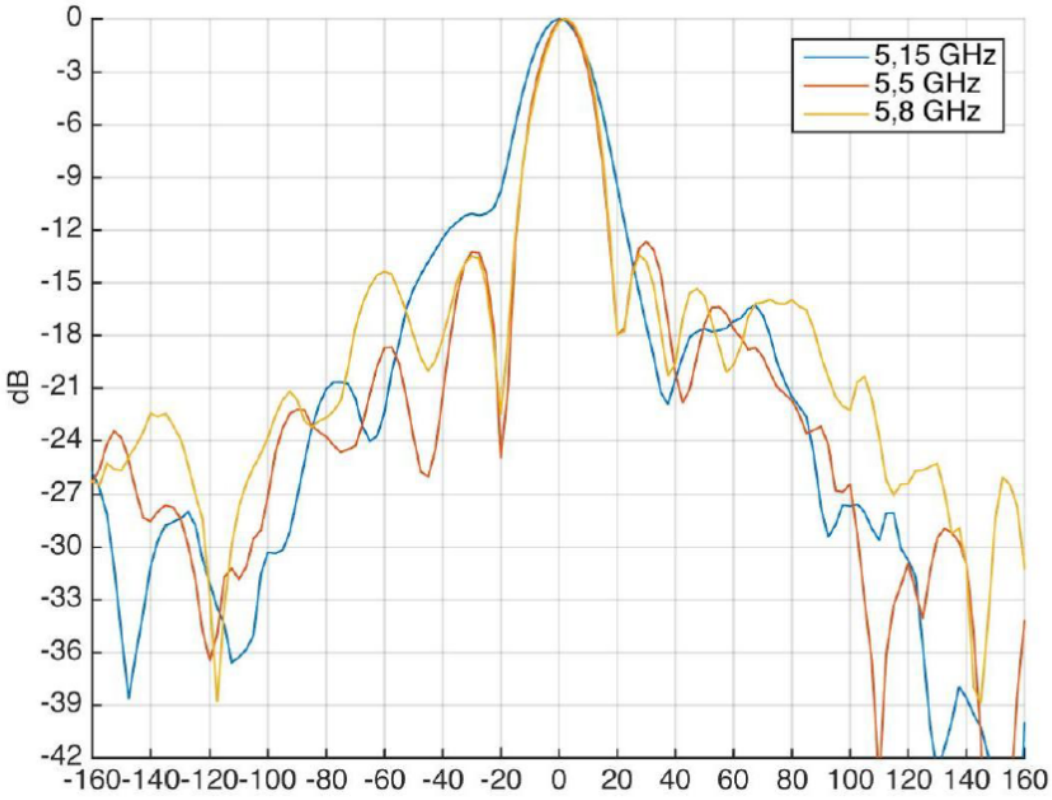
   A user script should start from the *#!/bin/sh* directive.

10 Application B. Antenna patterns

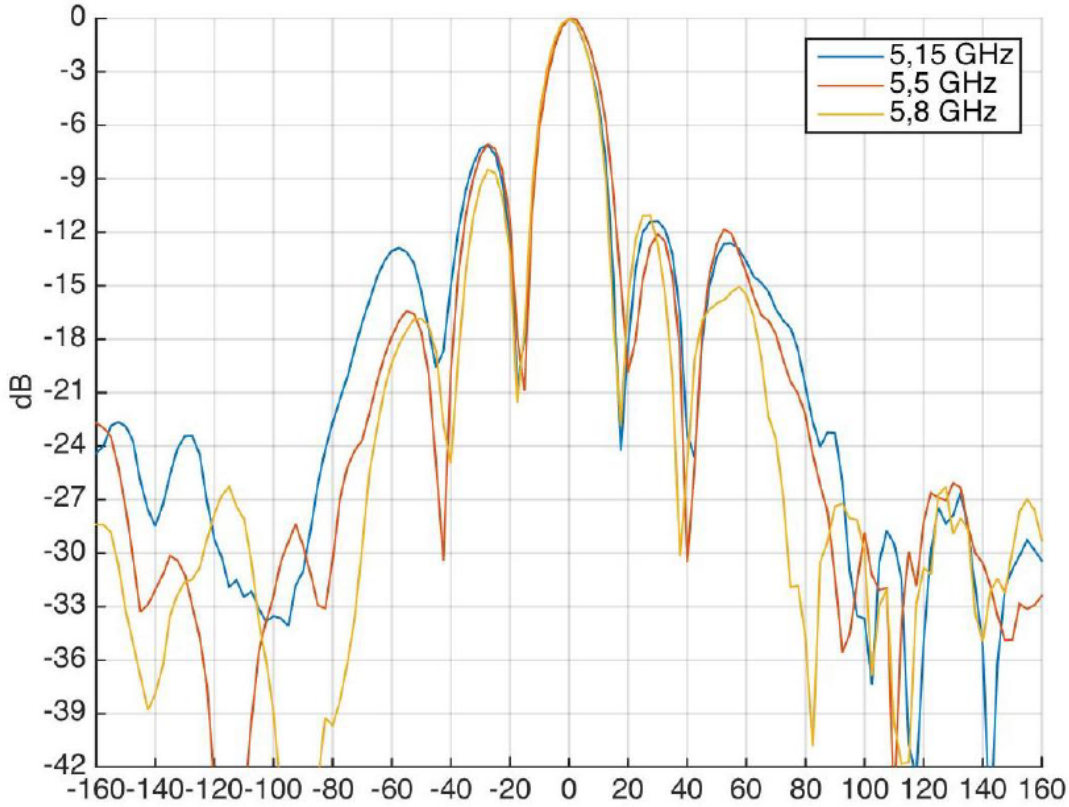
The pattern of vertically-polarized antenna in H-plane:



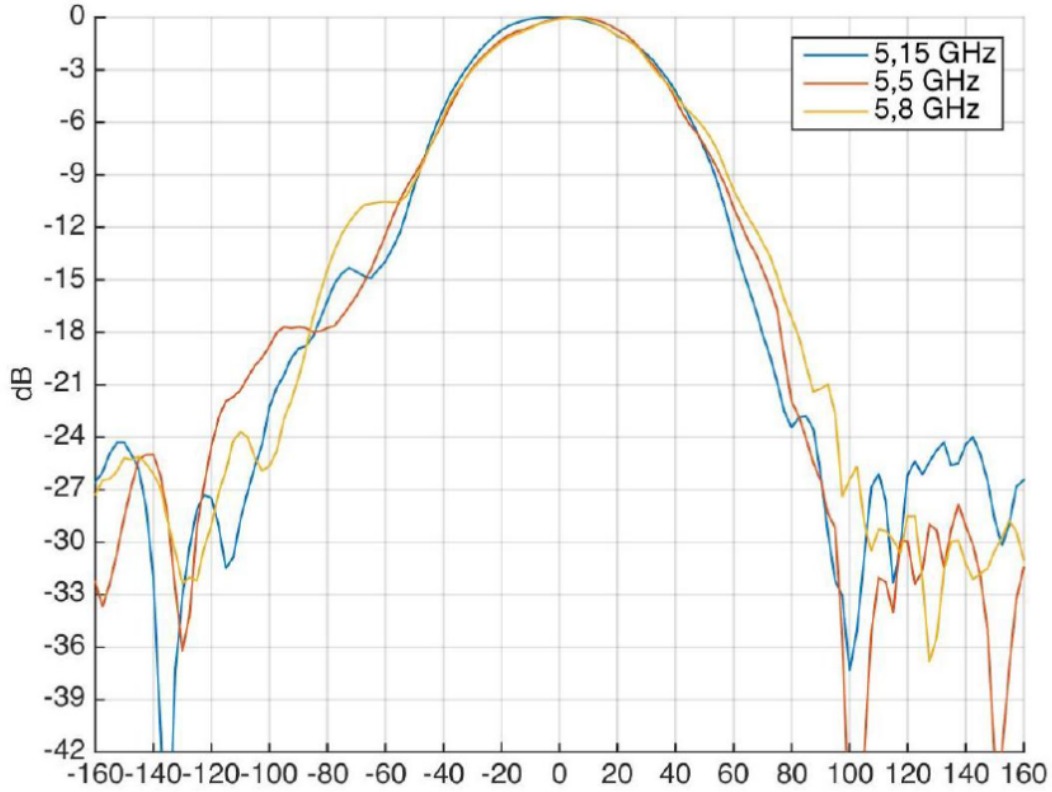
The pattern of vertically-polarized antenna in E-plane:



The pattern of horizontally-polarized antenna in H-plane:



The pattern of horizontally-polarized antenna in E-plane:



The list of changes

Document version	Issue date	Changes
Version 2.0	31.10.2018	Added: 4.5.3 Wireless bridge 4.6.4 «WDS» submenu 4.6.5 «Radiointerface» submenu 4.7.2 «WDS» submenu Changes in chapters: 2.2 Device specifications 4.6.3 «Internet» submenu 4.6.7 «MAC addresses confinuration» submenu
Version 1.0	24.11.2017	First issue
Firmware version 2.1.0		

TECHNICAL SUPPORT

For technical assistance in issues related to handling of ELTEXALATAU Ltd. equipment please address to Service Centre of the company:

Republic of Kazakhstan, 050032, Medeu district, microdistrict Alatau, 9 st. Ibragimova, 9
Phone:
+7(727) 220-76-10
+7(727) 220-76-07
E-mail: post@eltexalatau.kz

In official website of the ELTEXALATAU Ltd. you can find technical documentation and software for products, refer to knowledge base, consult with engineers of Service center in our technical forum:

http://www.eltexalatau.kz/en/