Subscriber router

RG-5520G-Wax
RG-5520G-Wax-Z

User manual, firmware version 1.4.0

IP address: 192.168.1.1

User name: admin

Password: password

CONTENTS

1 Introduction

1.1 Abstract

RG-5520G-Wax, RG-5520G-Wax-Z are Wi-Fi access points with integrated routers. The main purpose of these routers is installation inside buildings as access points to various interactive services via wired and wireless data networks.

The devices are aimed at home users and small offices.

This user manual describes intended use, specifications, design, installation, initial setup, configuration, monitoring and firmware update guidelines for the subscriber routers RG-5520G-Wax, RG-5520G-Wax-Z.

1.2 Document conventions

Hints, notes, and warnings

Hints contain important information or recommendations on device operation or setup.

Notes contain additional information on device operation or setup.

Warnings are used to inform the user about situations that may harm the device or a person, lead to malfunction or data loss.

2 Device description

2.1 Purpose

The RG-5520G-Wax and RG-5520G-Wax-Z subscriber routers (hereinafter "devices") are single access points to modern interactive services using wired and wireless data transmission networks: the Internet and Full HD IPTV. The devices are connected to a wired network using a 10/100/1000/2500M Ethernet interface and create wireless access for devices that support Wi-Fi technology in the 2.4 GHz (IEEE 802.11b/g/n/ax) and 5 GHz (IEEE 802.11a/n/ac/ax) bands.

Up to four wired devices can be connected to the routers. The USB connector is used to connect external storage devices.

The devices also have advanced features for stable operation of IPTV over wireless network: software ensures smooth and continuous video playback. The routers have the ability to simultaneously broadcast video streams and transmit data.

The devices support modern requirements for the quality of services and allow one to transfer the most important traffic in higher priority queues than usual. Prioritization is ensured by basic QoS technologies.

The devices include a smart home hub that supports working with sensors and devices using the Z-Wave[1] protocol.

2.2 Device characteristics

The device is powered via an external 220 V AC adapter.

Interfaces:

- LAN × 4 RJ-45 10/100/1000BASE-T Ethernet ports;
- WAN × 1 RJ-45 10/100/1000/2500BASE-T Ethernet port;
- WLAN × IEEE 802.11b/g/n/ax 2.4 GHz and11a/n/ac/ax 5 GHz;
- USB × 1 USB 2.0 port;
- Built-in Z-Wave Smart Home control interface[1].

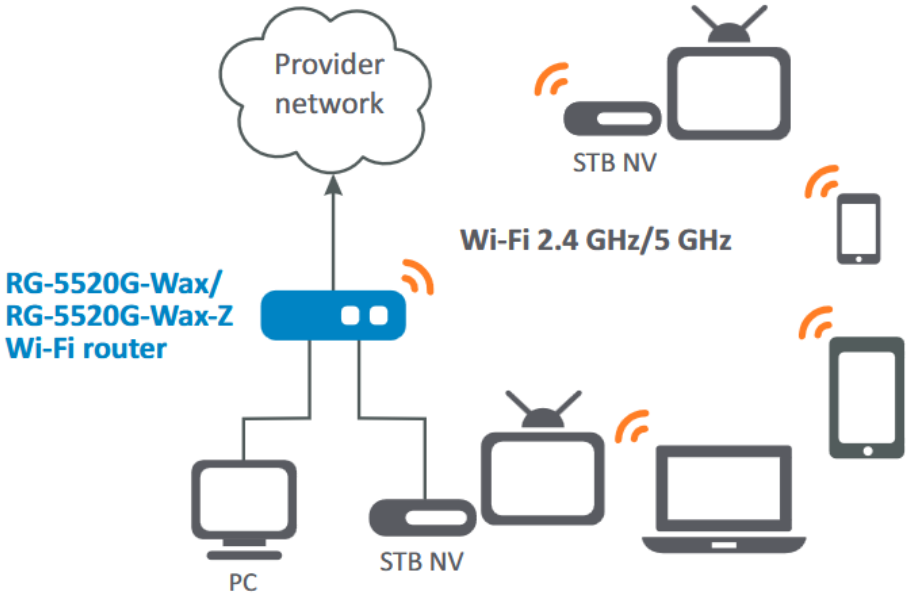
[1] Built-in Z-Wave module is supported for RG-5520G-Wax-Z only.

Functions:

- Network functions:
  - MultiWAN (multiservice model: separate configuration of network parameters for each service: Internet, TR-069, IPTV);
  - QoS;
  - NAT;
  - Port forwarding;
  - DMZ;
  - ALG (FTP, TFTP, H323, SIP, PPTP);
  - IP Passthrough;
  - operation in router and bridge modes;
  - PPPoE (PAP-, CHAP-, MSCHAP-, MSCHAPV2- and EAP-authorization, PPPoE-compression);
  - L2TP;
  - PPTP;
  - WireGuard;
  - 6rd;
  - static address and DHCP (a DHCP client on the WAN side, a DHCP server on the LAN side);
  - DNS;

  - UPnP;
  - IGMP Snooping and MLD Snooping;
  - Firewall;
  - SPI;
  - cloning of the MAC address on the WAN interface;
  - NTP;
  - STP;
  - QoS mechanisms;
  - virtual servers (port forwarding);
  - static and dynamic routing;
  - RIPv1, RIPv2;
  - Dynamic DNS;
  - Restriction of the access to the device via WAN and LAN;
- IPTV functions (IGMP proxy, MLD proxy, UDP-to-HTTP Proxy);
- FTP, Samba, DLNA;
- Software update via the web interface, TR-069;
- TR-069;
- 3G/4G modem;
- Jumbo Frame (up to 9200 bytes);
- EasyMesh;
- Remote monitoring, configuration: web interface, TR-069, Telnet and SSH;
- Control of Z-Wave compatible devices (for RG-5520G-Wax-Z only).

Use case of RG-5520G-Wax, RG-5520G-Wax-Z:



2.3 Main specifications

General parameters	
Clock frequency	1.15 GHz
RAM DDR	256 MB
ROM	128 MB
Operating system	Linux 4.4
Ethernet WAN interface	
Number of interfaces	1
Connector type	RJ-45
Data rate	10/100/1000/2500 Mbps
Standard	BASE-T
Ethernet LAN interface	
Number of interfaces	4
Connector type	RJ-45
Data rate	10/100/1000 Mbps
Standard	BASE-T
Wireless interface	
Number of antennas	2
Antennas type	internal
Antenna gain	2.4 GHz: 2×3 dBi 5 GHz: 2×4 dBi
Standards	802.11a/b/g/n/ac/ax
Frequency range	2402-2482 MHz, 5170-5330 MHz, 5650-5835 MHz
MIMO	MU MIMO 2.4 GHz 2×2 MU MIMO 5 GHz 2×2
Modulation	2.4 GHz: DSSS, CCK, BPSK, QPSK, 16QAM, 64QAM, 256QAM, 1024QAM 5 GHz: BPSK, QPSK, 16QAM, 64QAM, 256QAM, 1024QAM

Data rate	802.11b up to 11 Mbps 802.11a up to 54 Mbps 802.11g up to 54 Mbps 802.11n (HT20) up to 144 Mbps 802.11ax (HE40_MCS11) up to 573.5 Mbps 802.11ac (VHT80_MCS9) up to 866.7 Mbps 802.11ax (HE80_MCS11) up to 1201 Mbps
Maximum output power of the transmitter[1]	2.4 GHz: up to 21 dBm 5 GHz: up to 22 dBm
Receiver sensitivity	2.4 GHz: 802.11n (MCS0): -94 dBm 5 GHz: 802.11n (MCS0): -95 dBm
Safety	WEP, WPA (TKIP+AES), WPA2 (TKIP+AES), WPA/WPA2 (TKIP+AES), WPA3, WPA2/WPA3
Smart Home	
Z-Wave signal at frequency[2]	869 MHz
Management	
Remote control	web interface, TR-069, SSH, Telnet
Access restrictions	by password, by IP addresses, by MAC addresses, by protocol
Physical specifications	
Power supply	external power adapter 12 V DC, 2 A
Maximum power consumption	16 W
Operating temperature range	from +5 to +40 °C
Relative humidity at 25 °C	up to 80 %
Dimensions (W × H × D)	RG-5520G-Wax/RG-5520G-Wax-Z — 234 × 36 × 135 mm RG-5520G-Wax rev.B/RG-5520G-Wax-Z rev.B — 230 × 35 × 138 mm
Weight	RG-5520G-Wax/RG-5520G-Wax-Z — 0.355 kg RG-5520G-Wax rev.B/RG-5520G-Wax-Z rev.B — 0.359 kg
Lifetime	no less than 5 years

[1] The number of channels and the maximum output power will vary according to the rules of radio frequency regulation in your country.
[2] Built-in Z-Wave module is available for RG-5520G-Wax-Z only.

2.4 Design

The RG-5520G-Wax and RG-5520G-Wax-Z devices are enclosed in plastic cases.

2.4.1 Top panel of the device. Description of light indication

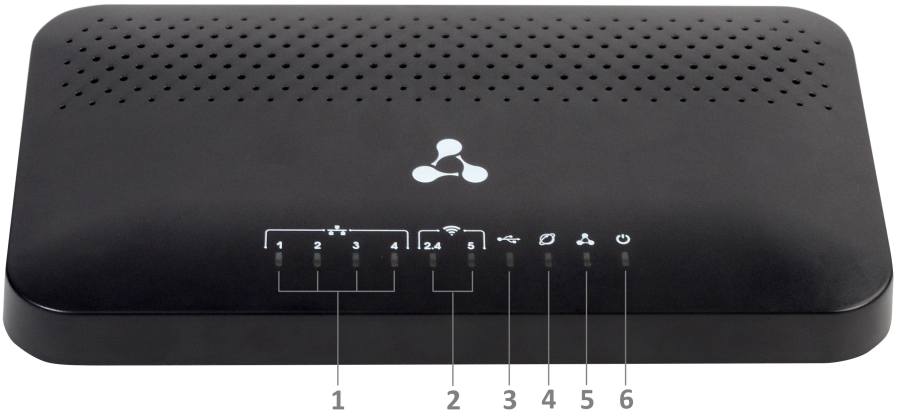
The top panel of RG-5520G-Wax rev.B, RG-5520G-Wax-Z rev.B of size 230 × 35 × 138 mm:

Description of the device top panel indicators:

	Indicator	Indicator state	Device state
1	**Power**	solid red	power is on, device is booting
		solid green	power is on, device is operating normally
		off	power is off
2	**Status**	flashing green	no internet connection
		solid green	active internet connection
3	**USB**	solid green	USB flash or USB modem is connected and the 4G LTE WAN interface is enabled
		off	USB device is not connected or USB modem is connected, but the 4G LTE WAN interface is turned off
4	**Wi-Fi**	solid green	Wi-Fi network is active in this band: 2.4 GHz and/or 5 GHz
		flashing green	process of data transmission over a wireless network in this band: 2.4 GHz and/or 5 GHz
		slowly flashing green	WPS device addition mode is enabled in this band: 2.4 GHz and/or 5 GHz
		off	Wi-Fi access point of this band is disabled: 2.4 GHz and/or 5 GHz

	Indicator	Indicator state	Device state
5	**WAN**	solid green	connection has been established with a connected network device at a rate of 10/100 Mbps
		flashing green	process of packet data transmission over the WAN interface at a rate of 10/100 Mbps
		solid orange	connection has been established with a connected network device at a rate of 1000/2500 Mbps
		flashing orange	process of packet data transmission over the WAN interface at a rate of 1000/2500 Mbps
		off	WAN cable is not connected
6	**LAN**	solid green	connection has been established with a connected network device at a rate of 10/100 Mbps
		flashing green	process of packet data transmission over the LAN interface at a rate of 10/100 Mbps
		solid orange	connection has been established with a connected network device at a rate of 1000 Mbps
		flashing orange	process of packet data transmission over the LAN interface at a rate of 1000 Mbps
		off	LAN cable is not connected

The top panel of RG-5520G-Wax, RG-5520G-Wax-Z of size 234 × 36 × 135 mm:



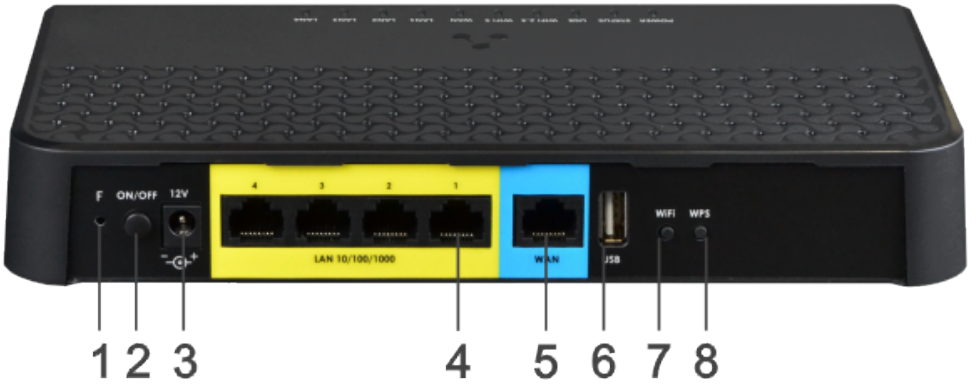
Description of the device top panel indicators:

	Icon	Indicator	Indicator state	Device state
1		**LAN**	solid green	connection has been established with a connected network device at a rate of 10/100 Mbps
			flashing green	process of packet data transmission over the LAN interface at a rate of 10/100 Mbps
			solid orange	connection has been established with a connected network device at a rate of 1000 Mbps
			flashing orange	process of packet data transmission over the LAN interface at a rate of 1000 Mbps
			off	LAN cable is not connected
2		**WLAN**	solid green	Wi-Fi network is active in this band: 2.4 GHz and/or 5 GHz
			flashing green	process of transmitting data over a wireless network in this band: 2.4 GHz and/or 5 GHz
			slowly flashing green	WPS device addition mode is enabled in this range: 2.4 GHz and/or 5 GHz
			off	Wi-Fi access point of this band is disabled: 2.4 GHz and/or 5 GHz
3		**USB**	solid green	USB device is connected
			off	USB device is not connected
4		**WAN**	solid green	connection has been established with a connected network device at a rate of 10/100 Mbps

	Icon	Indicator	Indicator state	Device state
			flashing green	process of packet data transmission over the WAN interface at a rate of 10/100 Mbps
			solid orange	connection has been established with a connected network device at a rate of 1000/2500 Mbps
			flashing orange	process of packet data transmission over the WAN interface at a rate of 1000/2500 Mbps
			off	WAN cable is not connected
5		**Status**	flashing green	no internet connection
			solid green	active internet connection
6		**Power**	solid red	power is on, device is booting
			solid green	power is on, device is operating normally
			off	power is off

2.4.2 Rear panel of the device. Description of ports and connectors

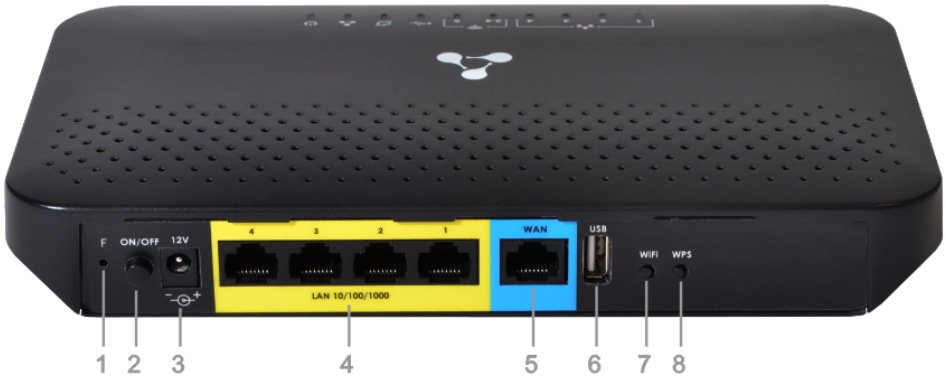
The rear panel of RG-5520G-Wax rev.B, RG-5520G-Wax-Z rev.B:



Description of the ports and connectors of the rear panel of the device:

	Rear panel element	Description
1	F	reset to default settings button
2	ON/OFF	power on/off button
3	12V	connector for power adapter
4	LAN 10/100/1000	4 × 10/100/1000BASE-T Ethernet ports (RJ-45 connector) for connecting network devices
5	WAN	10/100/1000/2500BASE-T port (RJ-45 connector) for connecting to an external network
6	USB	USB port for connecting an external USB device (USB flash, hard disk)
7	Wi-Fi	Wi-Fi on/off button
8	WPS	button for connecting the client via the WPS protocol

The rear panel of RG-5520G-Wax, RG-5520G-Wax-Z:



Description of the ports and connectors of the rear panel of the device:

	Rear panel element	Description
1	F	reset to default settings button
2	ON/OFF	power on/off button
3	12V	connector for power adapter
4	LAN 10/100/1000	4 × 10/100/1000BASE-T Ethernet ports (RJ-45 connector) for connecting network devices
5	WAN	10/100/1000/2500BASE-T port (RJ-45 connector) for connecting to an external network
6	USB	USB port for connecting an external USB device (USB flash, hard disk)
7	Wi-Fi	Wi-Fi on/off button
8	WPS	button for connecting the client via the WPS protocol

2.5 Delivery packet

The standard delivery package includes:

- RG-5520G-Wax(-Z) Wi-Fi router;
- 220/12 V, 2 A power adapter;
- Installation and initial configuration guide.

3 Installation and connection

3.1 Operating conditions

- Do not install the device near heat sources.
- Install the device in a place protected from direct sunlight.
- Do not expose the device to smoke, dust, water, or other liquids. Avoid mechanical damage to the device.
- Do not open the device case. There are no user-serviceable parts inside the device.
- Equipment disposal should be performed separately from household waste.

Do not place objects on the surface of the equipment in order to prevent overheating and malfunction of the device and its components.

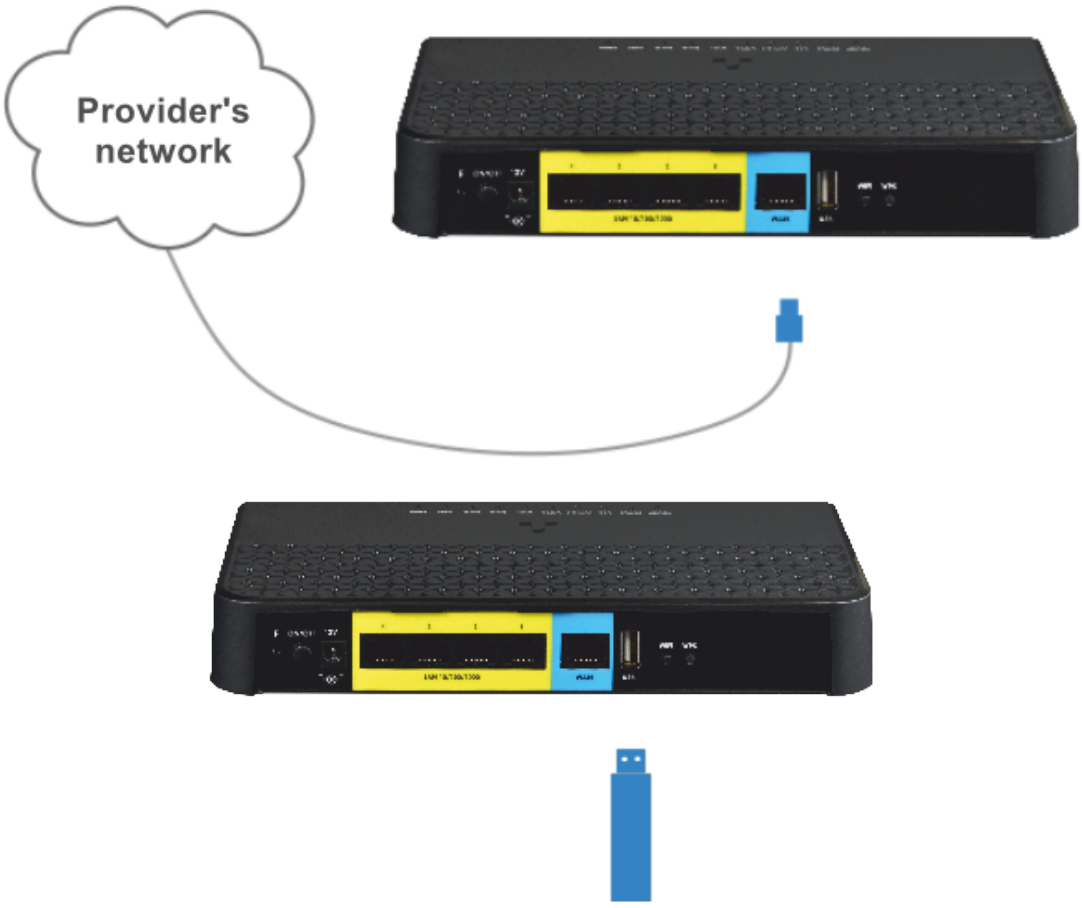
3.2 Installation recommendations

1. Before installing and turning on the device, it is necessary to check the device for visible mechanical damage. In case of any damage, stop installing the device, draw up an appropriate report and contact the supplier.
2. If the device has been at a low temperature for a long time, it must be kept at room temperature for at least two hours before starting work.
3. If the device has been exposed to high humidity for a long time, it must be kept under normal conditions for at least 12 hours before switching on.
4. The device is installed in a horizontal position, following the safety instructions.
5. To ensure the best-performing Wi-Fi network coverage, consider the following guidelines when placing a device:
    - Minimize the number of obstacles (walls, ceilings, furniture, etc.) between the router and other wireless network devices;
    - Do not install the device near (about 2 m) electrical or radio devices;
    - It is not recommended to use radiotelephones and other equipment operating at 4 GHz or 5 GHz within the range of a wireless Wi-Fi network;
    - Obstacles in the form of glass/metal structures, brick/concrete walls, as well as water tanks and mirrors can significantly reduce the range of a Wi-Fi network.

3.3 Connecting the Wi-Fi router

1. Connect the Wi-Fi router to a 220 V network via a power adapter. As soon as the **Status** indicator starts flashing, the device is available for connection to the provider's network and further configuration.

2. Connect the Ethernet cable provided by the Internet service provider to the WAN connector or the 4G modem to the USB port of the router. As soon as the **Status** indicator stops flashing and lights constantly, the connection to the provider's network is established.



3. Make sure that the following indicators are always on: **Power, Wi-Fi (WLAN), WAN, Status**. This means that the device is connected correctly and running.

For the modem connection to work, the Ethernet cable must be disconnected from the WAN port.

3.4 Connecting devices to a Wi-Fi router

3.4.1 Wired connection

Connect devices (computers, printers, etc.) using an Ethernet cable to the LAN ports of the router.

3.4.2 Wireless connection

Connect devices (laptop, smartphone, etc.) to the router's network. To do this:

1. Enable wireless network detection on the user's device.
2. In the list of available networks, find the network with the name (SSID) that matches the name indicated on the bottom panel of the router.
3. Select this network and enter the password specified on the bottom panel of the router.

One can also connect one's smartphone using a QR code in two ways:

- **Scan the QR code on the bottom panel of the device;**
- **Log into the router's web interface, go to the "Wi-Fi" menu of the Advanced Mode and then to the "Basic Settings" submenu for the appropriate Wi-Fi range (2.4 GHz or 5 GHz). Click the**  **button and scan the QR code.**

3.4.3 WPS connection

The device supports connecting the client to the router's Wi-Fi network according to the WPS standard.

Connection procedure:

1. Select the WPS connection method on the client device.
2. Press and hold the WPS button on the rear panel of the Wi-Fi router for one second.

The client will connect to the Wi-Fi router automatically.

Connecting the client device to the router takes no more than two minutes. If one couldn't connect the device the first time, try again and make sure that the WPS function on the client device was enabled no later than 2 minutes after enabling the WPS function on the Wi-Fi router.

The WPS feature is enabled by default. One can disable the feature in the web interface in the "Wi-Fi" menu of the Advanced Mode, in the "WPS" submenu (2.4 GHz or 5 GHz).

3.5 Connecting the Wi-Fi router as an additional router

To connect a Wi-Fi router only as an additional router to an existing network, follow these steps:

Using an Ethernet cable, connect the WAN port of the Wi-Fi router to the LAN port of an already connected third-party router that organizes one's Wi-Fi network. The Ethernet cable is not included in the delivery packet of the device. Choose the cable according to your network environment.

If the third-party router uses the 192.168.1.0/24 subnet, then when connecting RG-5520G-Wax/Wax-Z its LAN address will automatically change to 192.168.2.1.

3.6 Interaction with the smart home system

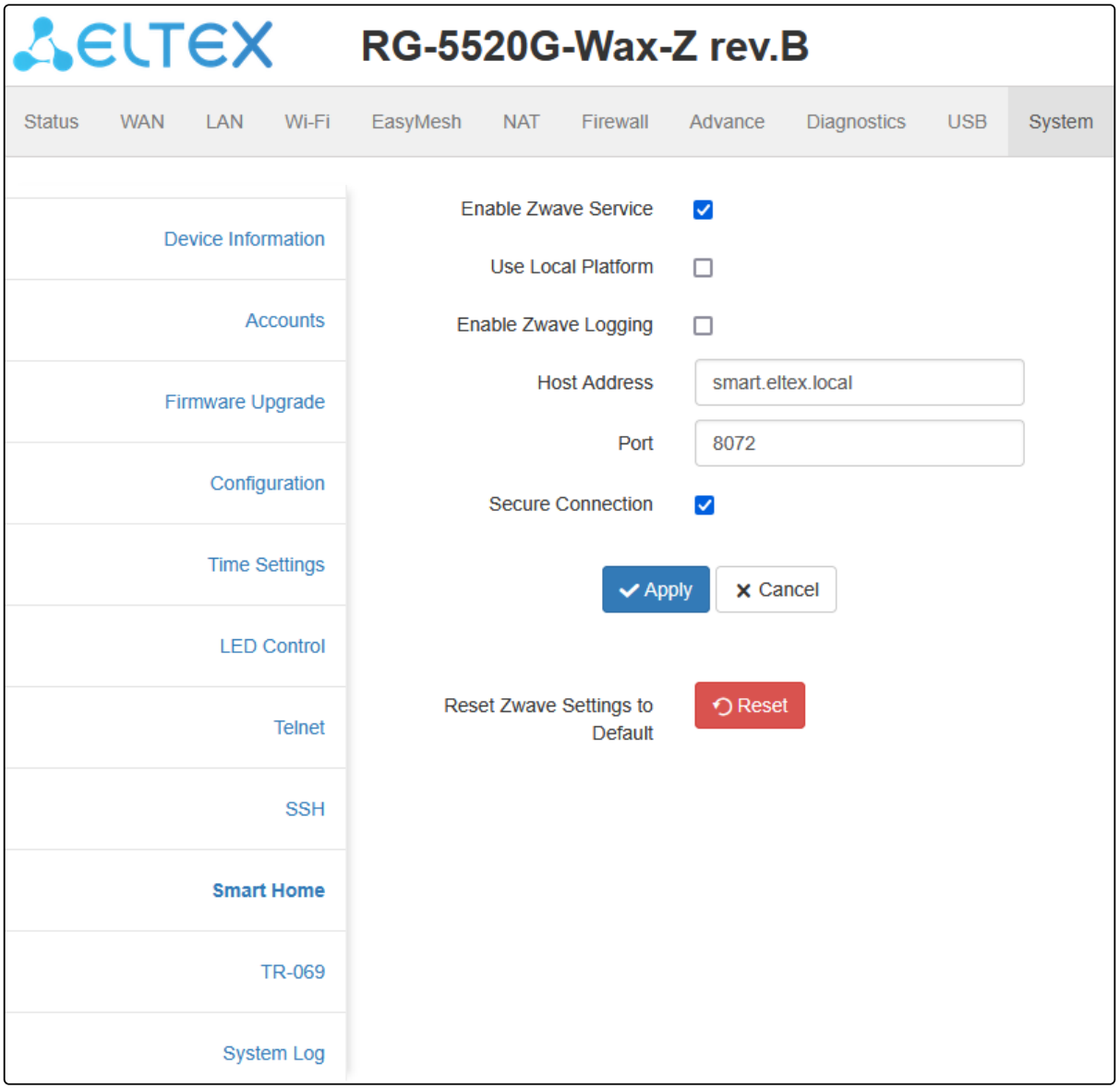
The RG-5520G-Wax-Z router includes a smart home hub that supports operation with sensors and devices using the Z-Wave[1]. To connect Wi-Fi and Z-Wave devices[1], download the Eltex Home mobile app on the Play Market or App Store.

[1] **Built-in Z-Wave module is supported for RG-5520G-Wax-Z only.**

	By the link	Through the search	By QR code
Google Play	Eltex Home	By the name "Eltex Home"	
App Store	Eltex Home		

After downloading the application, enter the platform address, register, and log in. To connect the router, follow the application guidelines.

Before adding a router to the Eltex Home platform, check whether the service Smart home is enabled via the device web interface: go to the "System" menu of the Advanced Mode, than to the "Smart Home" submenu.



Enable Zwave Service[1] — when the flag is set, the Z-Wave hub function is enabled. This feature is enabled by default.

Use Local Platform — when the flag is set, the local platform connected to the device will be used. The default value is smart.eltex.local.

Enable Zwave Logging — when the flag is set, events with the Z-Wave device are saved to the system log.

Host Address — address of the Eltex Smart Control (Eltex SC) server. The default value is smart.eltex.local.

Port — port for communication with the "Eltex Smart Control" platform. The default port is 8072.

Secure Connection — when the flag is set, the SSL encryption protocol is used. Enabled by default.

Reset Zwave Settings to Default — restarting the hub and deleting all connected devices using the Z-Wave protocol.

3.7 Reset the device to factory settings

There is a reset function "F" button on the rear panel of the devices, which allows one to reboot the devices or reset them to factory settings. Use the "F" button when the Wi-Fi router is turned on and ready to work: the "Power" indicator is on green, the "Status" indicator is on/flashing green. To reset the device to factory

settings, press and hold the "F" button for more than 5 seconds until the "Status" indicator slowly flashes green. The device will reboot automatically.

At factory settings, the DHCP client is running on the WAN interface, and the DHCP server is running on the LAN interface.

- **The device address on the LAN interface is *168.1.1*, the subnet mask is *255.255.255.0*;**
- **For access via the web interface under the *User account:* username — *user,* password — *password*;**
- **For access via the web interface with elevated privileges under the *Admin account:* username — *admin,* password — *password*.**

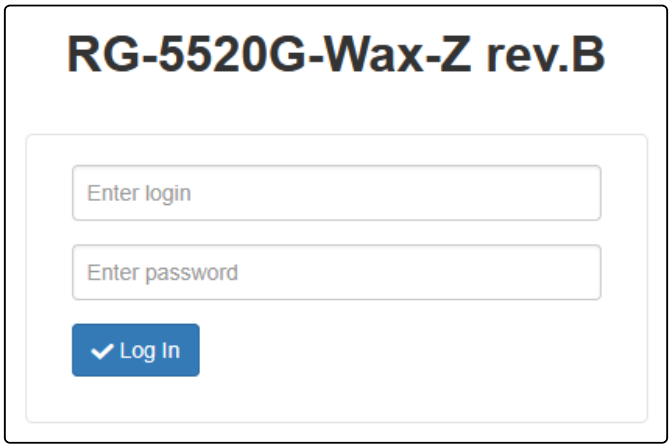
4 Managing via web interface

4.1 Getting started

1. Open a web browser and enter the device IP address in the browser address bar.

Default IP address: *192.168.1.1*, subnet mask: *255.255.255.0*.

When the device is successfully detected, web interface login and password request page will be shown in the browser window:



Web interface authorization page

2. Enter username and password.

For the *User account*: username — *user*, password — *password*.
For the *Admin account*: username — *admin*, password — *password*.

3. Click the "Log in" button. The Home page will open in the browser window.

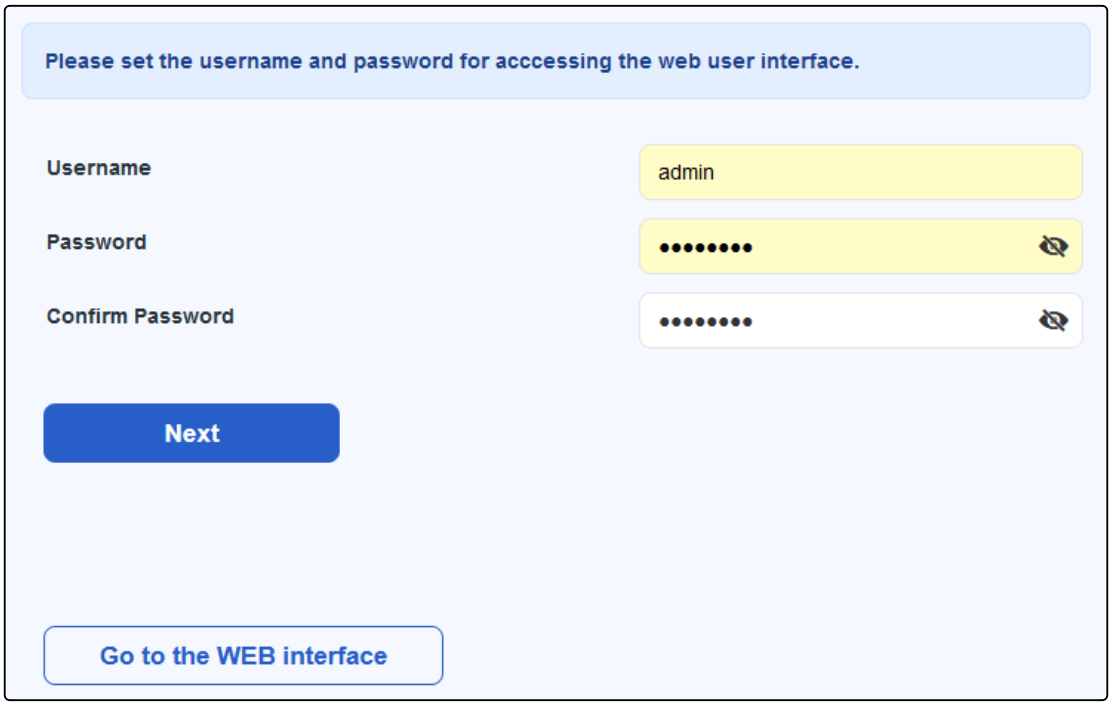
4.2 Setup Wizard

Setup Wizard allows one to configure the basic device parameters.

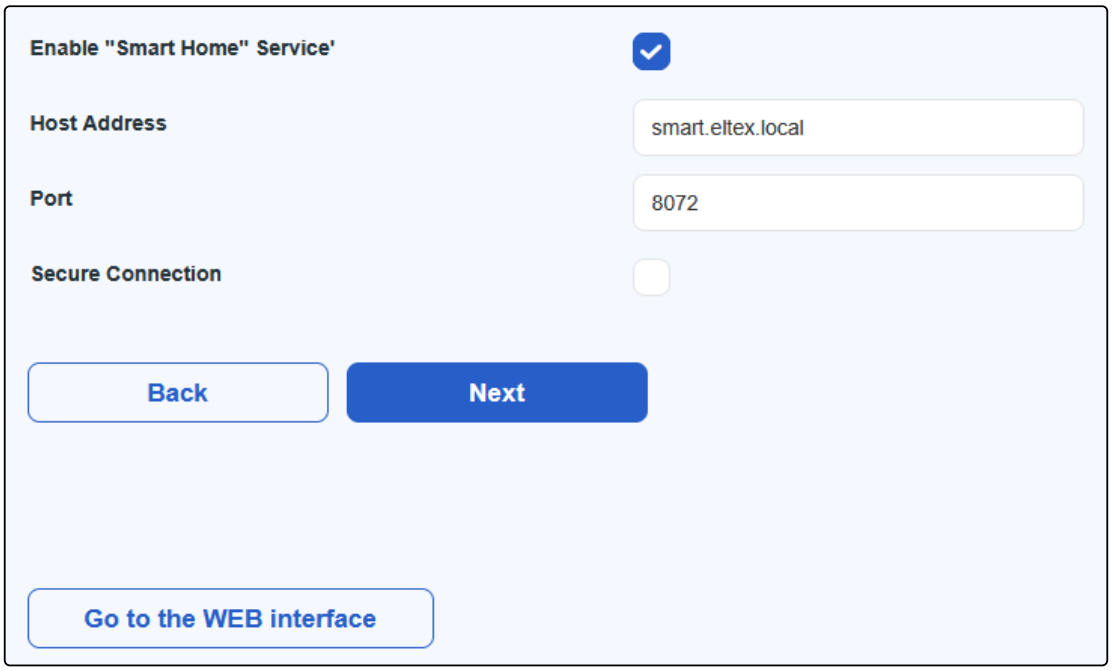
To access the Setup Wizard, connect the cable to the device's WAN interface and click the "Start Wizard" button.

Follow the steps in Setup Wizard to complete the device configuration. Or select the manual setting by clicking the "Manual Config" button.

1. Enter username and password for logging into the web interface.



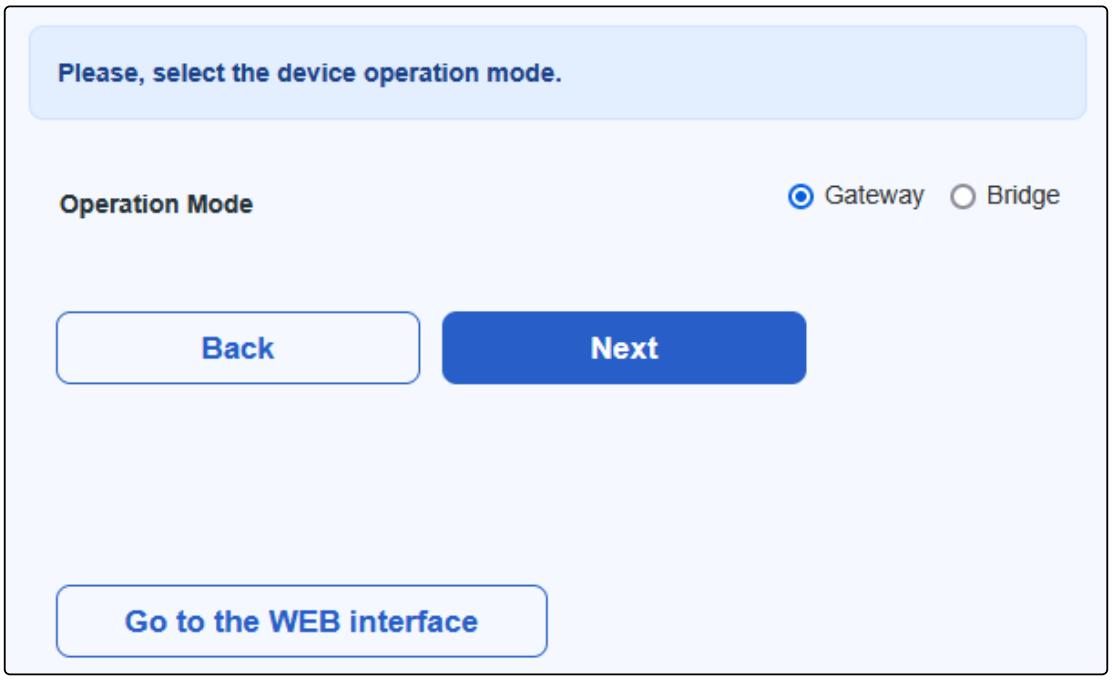
2. Configure the Smart Home service (for RG-5520G-Wax-Z only) or leave default settings.



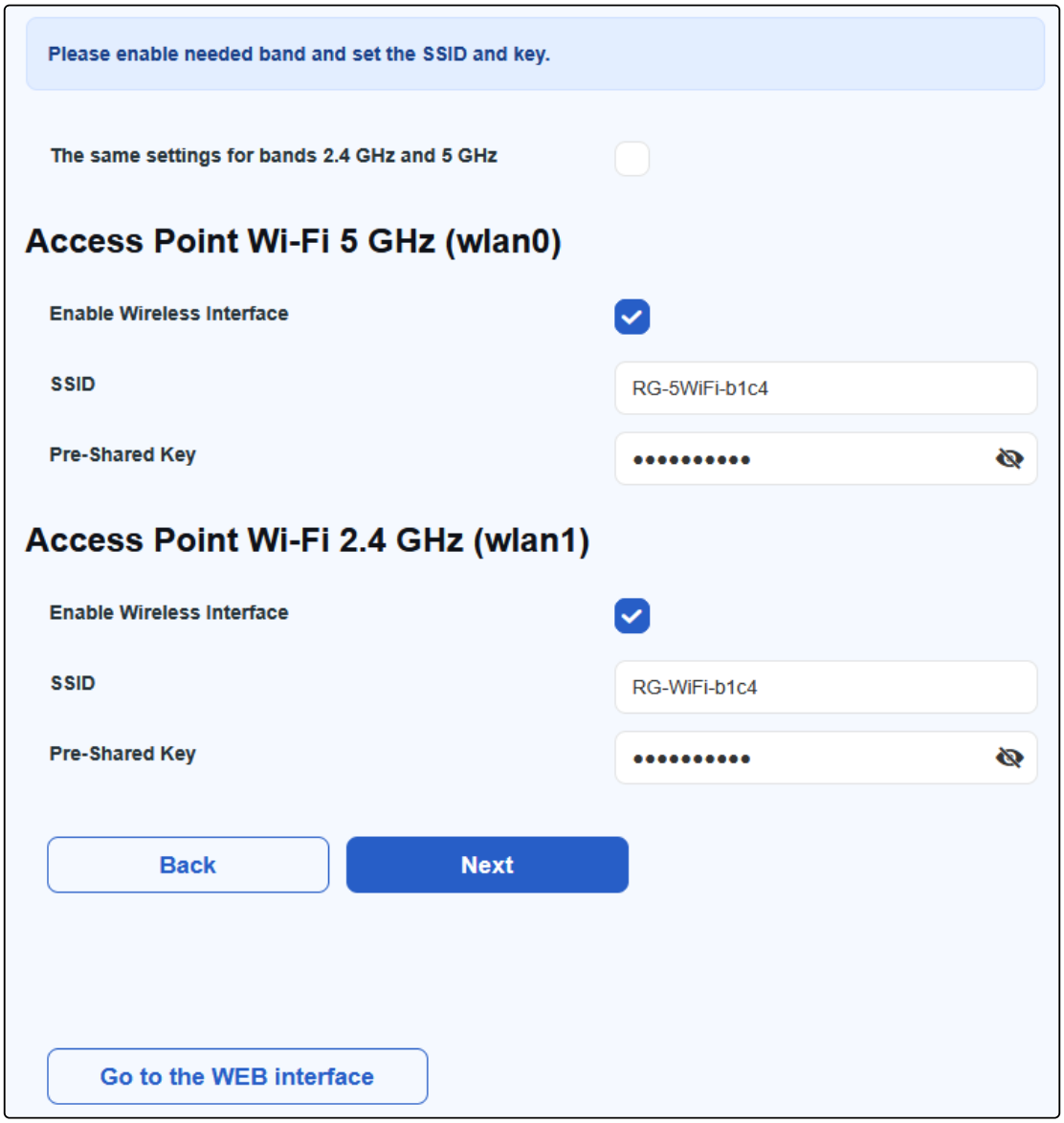
3. Select the device operation mode.

Operation Mode — select the device operation mode:

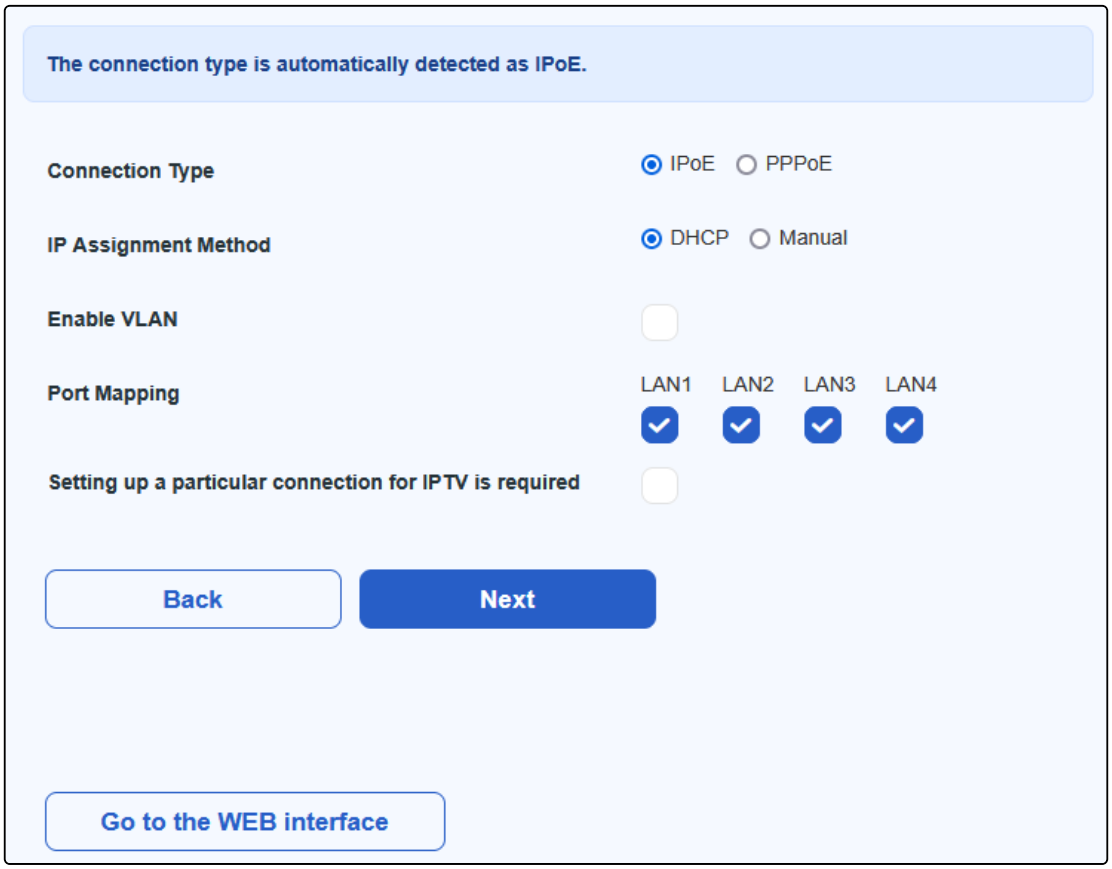
- *Gateway* — Wi-Fi router mode (enables NAT on the WAN interface and transmits traffic from the local network via the IP address of the device WAN interface);
- *Bridge* — adds a WAN interface to the device local bridge.



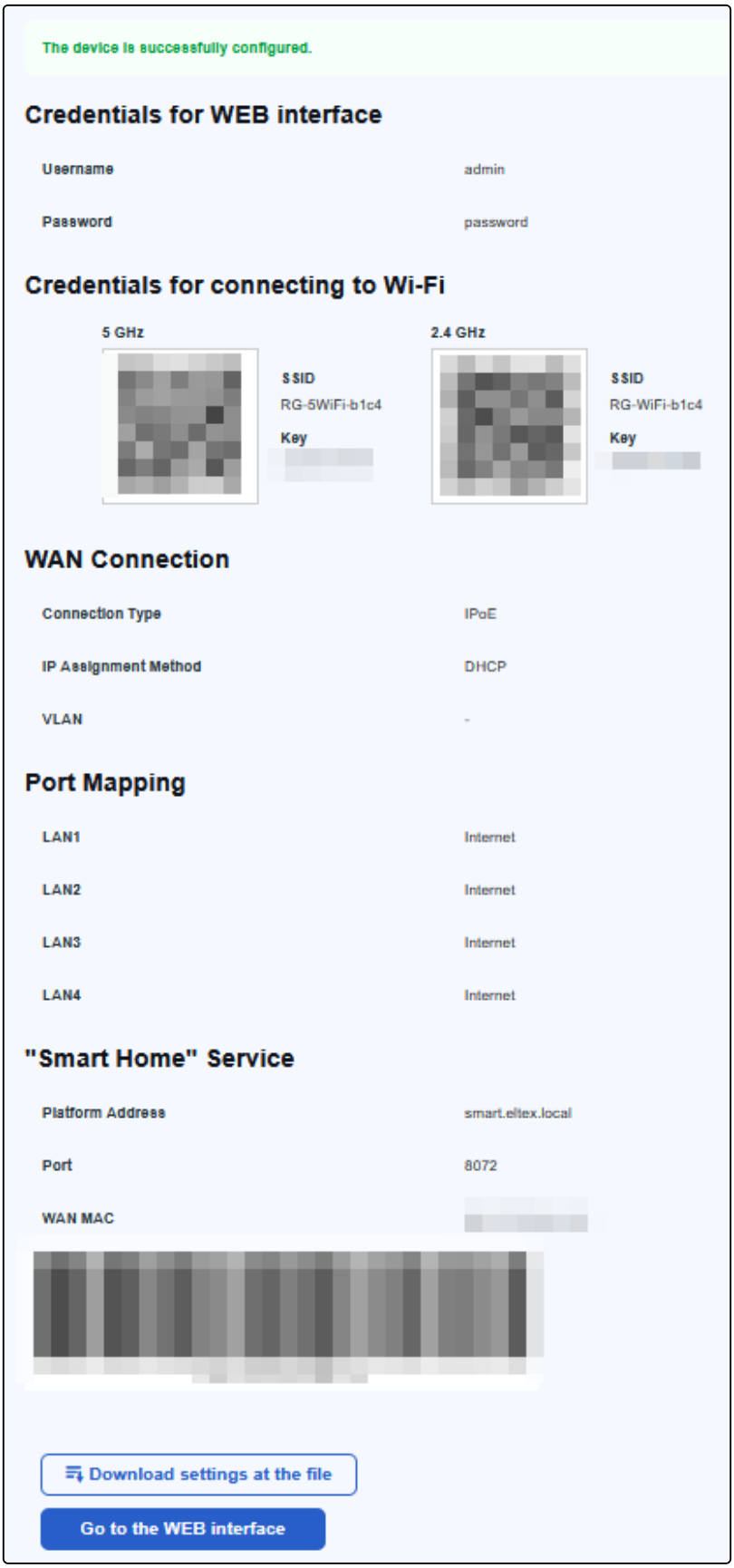
4. Configure the Wi-Fi network.



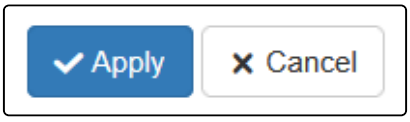
5. Configure the device network and select the LAN ports for Internet access and for the IPTV service (if the IPTV service uses a bridge connection).



After Setup Wizard configuration is completed, a screen with information about the configured device parameters will be displayed.



4.3 Applying configuration and canceling changes



Click the "Apply" button to apply settings. Some settings will take effect only after the device is rebooted. The system will warn about this when one presses the button.

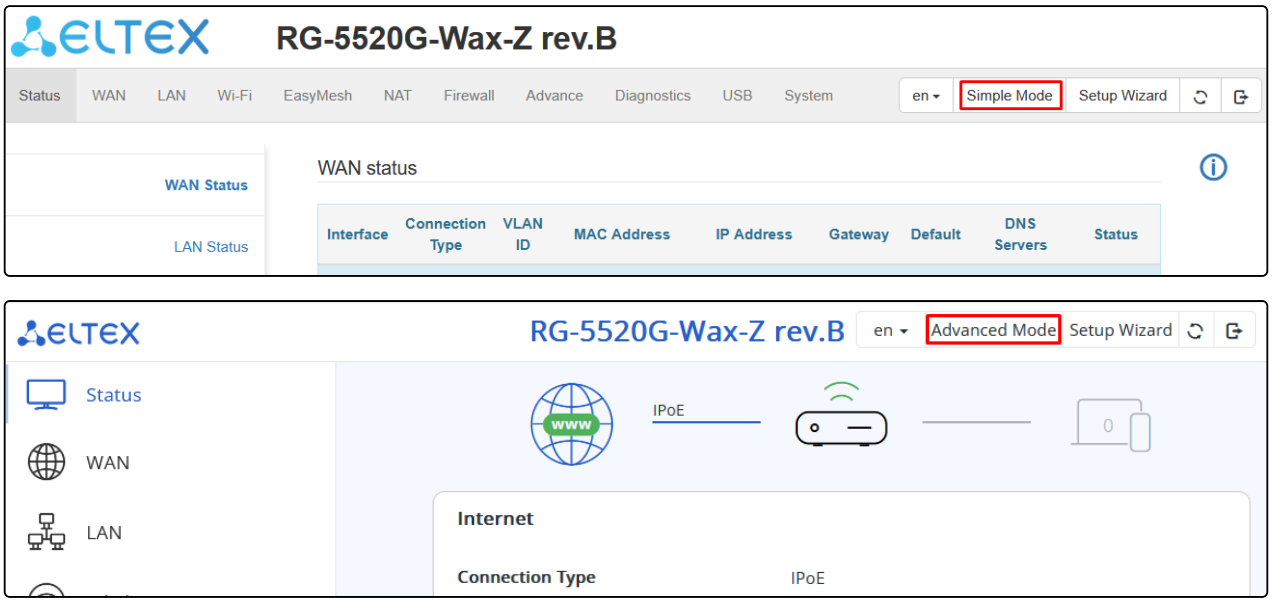
The changes are canceled only before clicking on the "Apply" button. In this case, the parameters changed on the page will be updated with the current values stored in the device memory. After clicking on the "Apply" button, it will not be possible to return to the previous settings.

4.4 Switching between web interface modes

Two modes are available for controlling and configuring the RG-5520G-Wax, RG-5520G-Wax-Z devices via the web interface:

- Simple mode is a web interface with the configuration of the main device parameters;
- Advanced mode is a web interface with detailed device configuration.

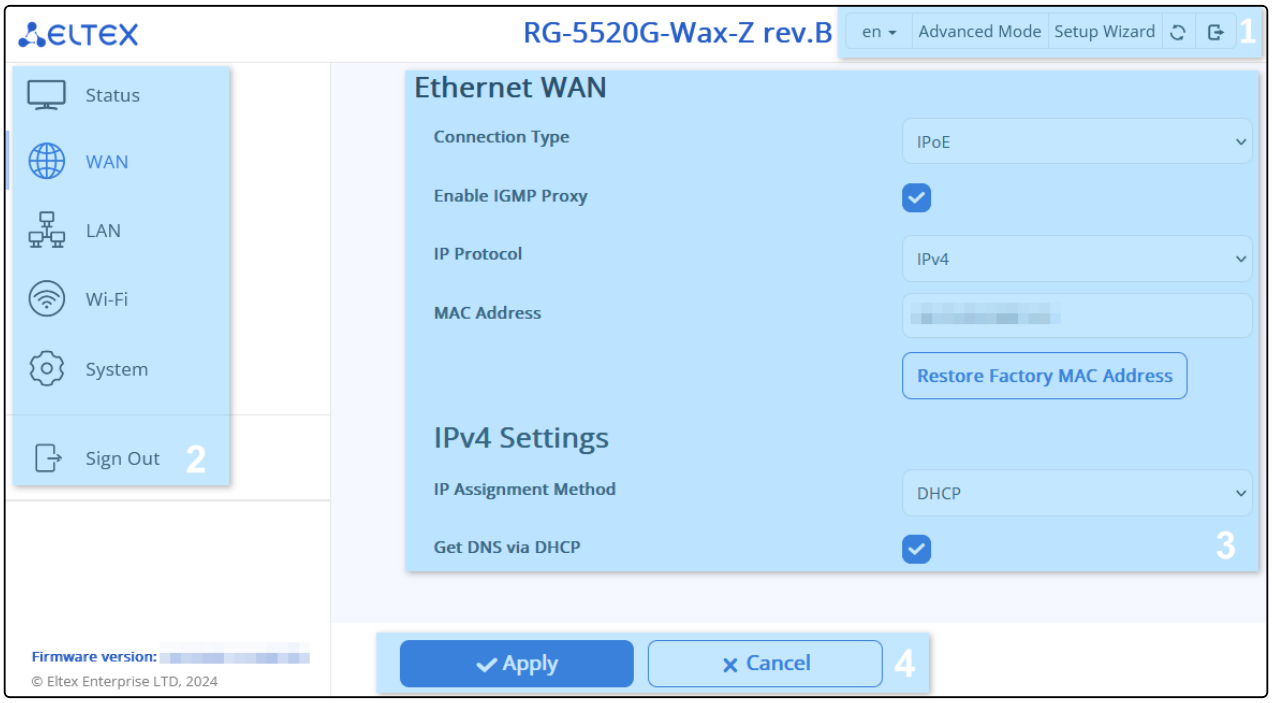
To switch from advanced mode to simple one, click the "Simple Mode" button. To switch from simple mode to advanced mode, press the "Advanced Mode" button. The buttons are located in the upper right part of the window.



4.5 Device control panel in Simple Mode

All device settings changes are performed using the control panel menu located on the left side of the web interface.

4.5.1 Key elements of the Simple Mode web interface



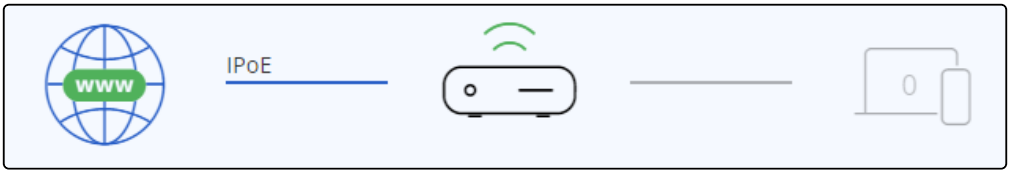
1. Panel for changing the web interface language, mode of the web interface, launching the Setup Wizard, with reboot and log out buttons.
2. Control panel menus.
3. Main device settings field corresponding to the selected tab from field 2.
4. Buttons for applying configuration changes and cancelling to the last saved values.

4.5.2 Status menu

The "Status" menu displays a summary of the device status.

Network map

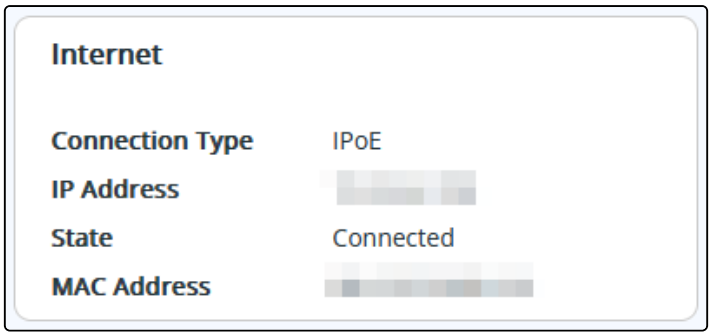
A visual representation of the network operation is available in this section.



Internet icon — upon successful connection, the icon is displayed in green, otherwise the icon is displayed in red.
Router icon — if at least one wireless interface is enabled on the device, the icon is displayed in green, otherwise the icon is displayed in red.
Wireless clients icon displays the wireless interface of the main access point and the number of wireless clients connected to it.

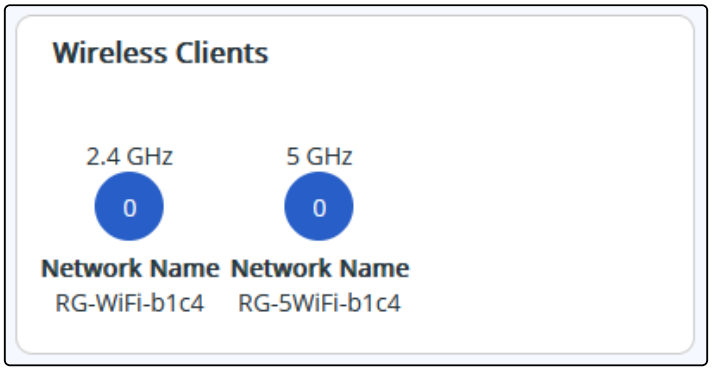
Internet

This section displays information about names of the main access points and the number of clients connected to the main wireless access points.



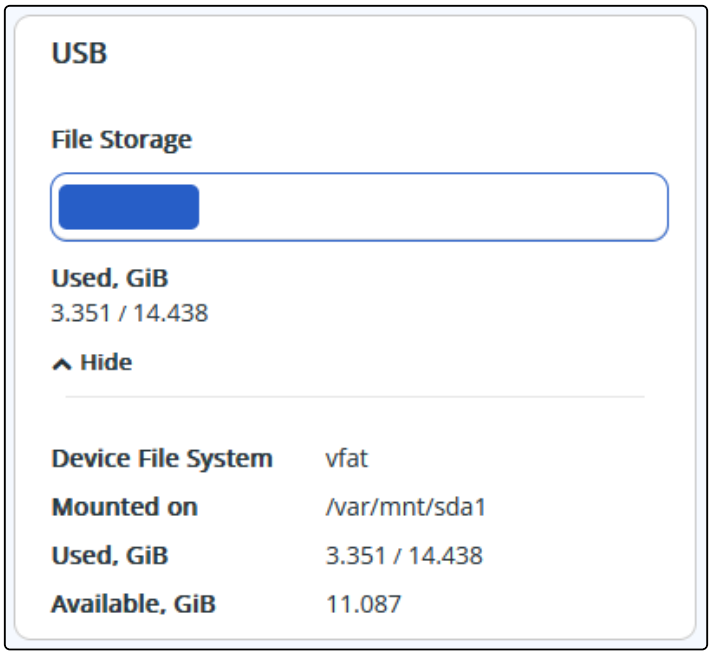
Wireless Clients

This section displays information about names of the main access points and the number of clients connected to the main wireless access points.



USB

This section displays information about connected USB devices.

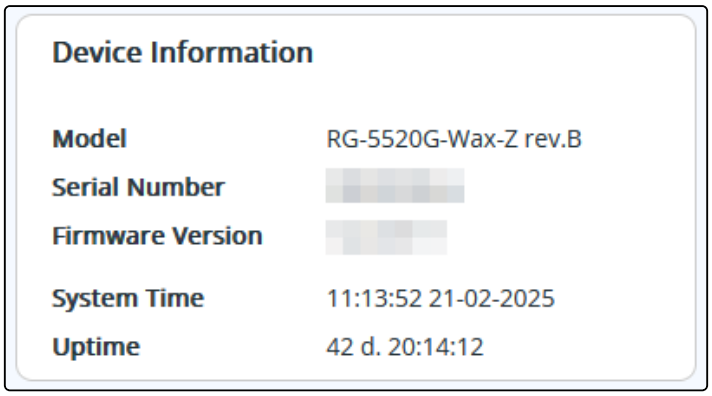


Ports

This section displays the status of the device physical ports.

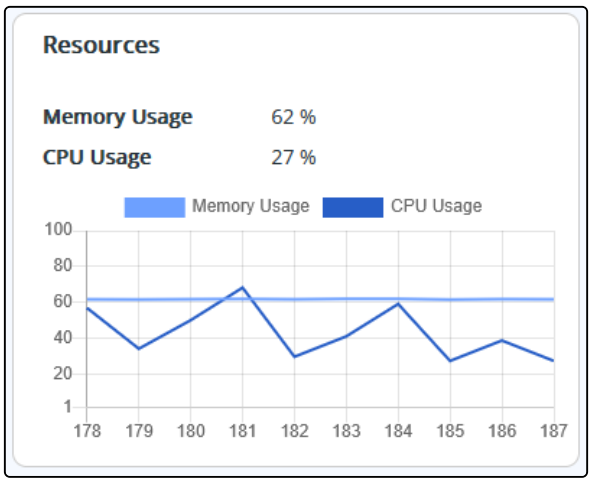
Device Information

This section displays basic information about the device and time settings.



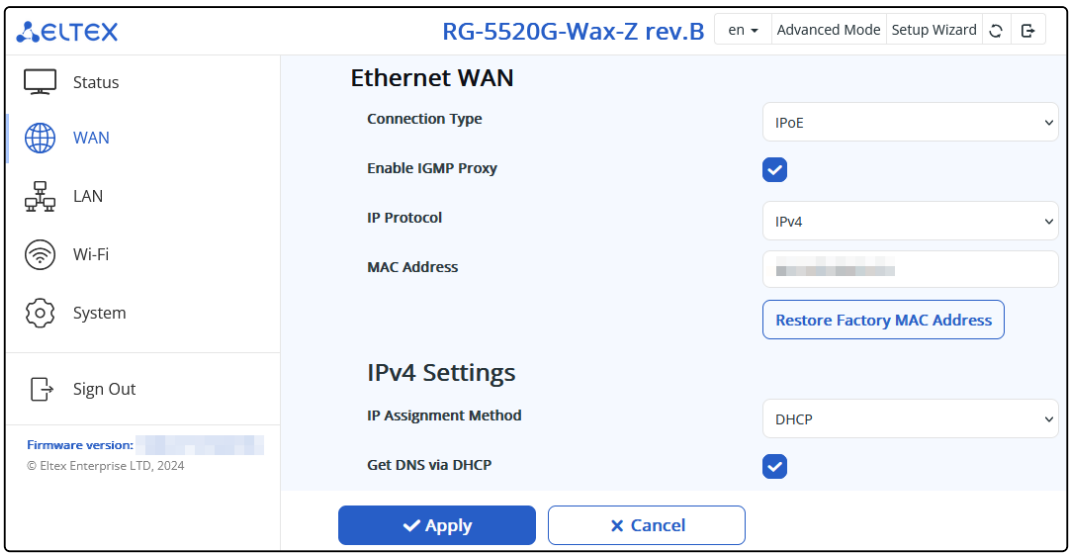
Resources

This section displays the CPU and memory usage of the device.



4.5.3 WAN menu

The basic parameters of the device WAN interface are available for configuring in the "WAN" menu.



Connection Type — selection of protocol used to connect the device WAN interface to the provider's service network:

- *IPoE* — the mode of operation in which the device routes traffic with or without NAT; network settings can be obtained from the DHCPv4 server/DHCPv6 server/RADVD or configured manually;
- *PPPoE* — the mode of operation in which the RPPoE session is reconnected on the WAN interface; network settings can be obtained from the PPPoE server/DHCPv6 server/RADVD.

Enable IGMP Proxy — enabling IGMP Proxy for multicast traffic tracking and broadcasting;

IP Protocol — selection of network protocols used for this WAN:

- *IPv4* — the mode of operation with network access over IPv4 only;
- *IPv6* — the mode of operation with network access over IPv6 only;
- *IPv4/IPv6* is a Dual Stack mode with network access over both IPv4 and IPv6.

MAC Address — the MAC address substitution for a given WAN;

Restore Factory MAC Address — restoring the factory MAC address for a given WAN.

IPoE connection type

IPv4

IP Assignment Method:

- *DHCP* — mode of operation with receiving settings from the DHCP server:
  - *Get DNS via DHCP* — when the flag is set, the DNS settings will be received via DHCP. Without the flag set, the following fields will be displayed:
    - *Preferred DNS Server* — setting the address of the primary DNS server;
    - *Alternative DNS Server* — setting the address of the additional DNS server.
- *Fixed IP* — operating mode with manual setting of the address and network parameters:
  - *IP Address* — IP address of the WAN interface of the device on the provider network.
  - *Gateway* — address of the default gateway to which the packet is sent if no route is found for it in the routing table.
  - *Subnet Mask* — external subnet mask.
  - *Preferred DNS* Server — setting the address of the primary DNS server;
  - *Alternative DNS Server* — setting the address of an additional DNS-server.

IPv6

IP Assignment Method:

- *Autodetection*— a mode of operation with automatic configuration of the address and network settings via ICMPv6/DHCPv6. Gateway is set using ICMPv6. Routing and prefix delegation to the local network are provided:
  - *Get DNS automatically* — when the flag is set, DNS settings will be received via ICMPv6/DHCPv6. Without the flag set, the following fields will be displayed:
    - *Preferred DNS Server* — setting the address of the primary DNS server;
    - *Alternative DNS Server* — setting the address of the additional DNS server.

PPPoE Connection Type

Username — the username for authorization on the PPPoE server.

Password — the password for authorization.

Get DNS automatically — when the flag is set, DNS settings will be received via PPP IPCP. The following fields will be displayed without the flag set:

- *Preferred DNS* Server — setting the address of the primary DNS server;
- *Alternative DNS Server* — setting the address of an additional DNS-server.

IPv6

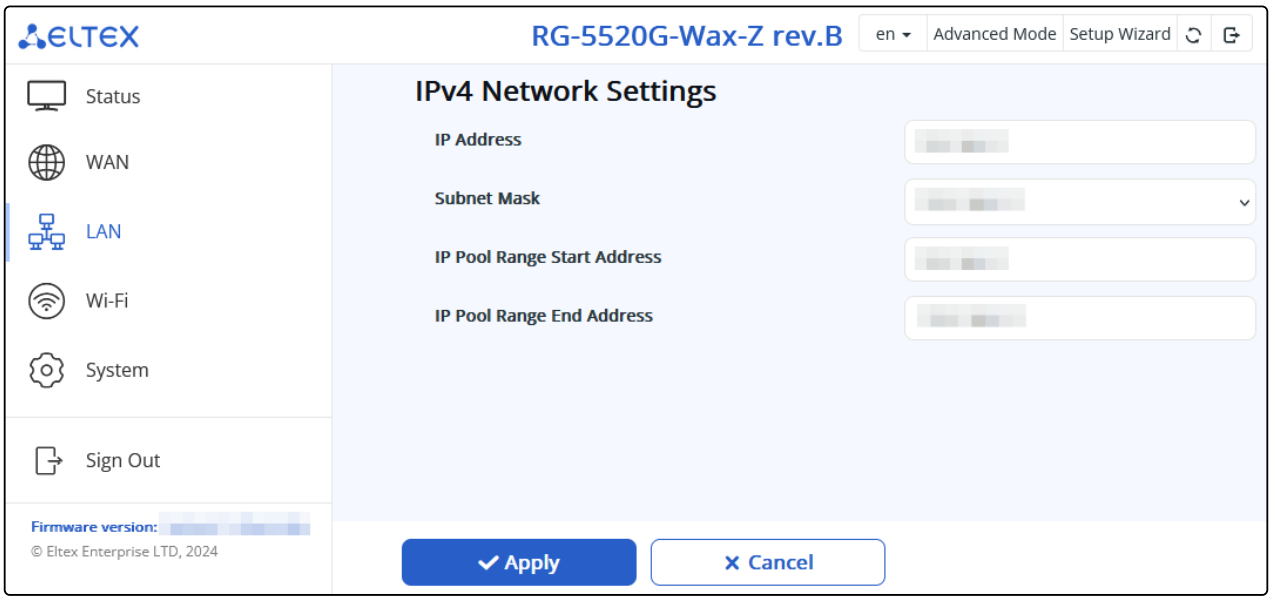
IP Assignment Method:

- *Autodetection* — a mode of operation with automatic configuration of the address and network settings via ICMPv6/DHCPv6. Gateway is set using ICMPv6. Routing and prefix delegation to the local network are provided:
  - *Get DNS automatically* — when the flag is set, DNS settings will be received via ICMPv6/DHCPv6. Without the flag set, the following fields will be displayed:
    - *Preferred DNS Server* — setting the address of the primary DNS server;
    - *Alternative DNS Server* — setting the address of the additional DNS server.

⚠ **In Simple Mode, only one WAN interface (IPoE or PPPoE) can be configured. If several WAN interfaces were previously configured, then after applying the settings, only one will remain. To configure multiple interfaces, switch to Advanced Mode.**

4.5.4 LAN menu

This menu sets up the basic parameters of the local bridge interface over the IPv4 protocol.



IP Address — the local IP address of the device.

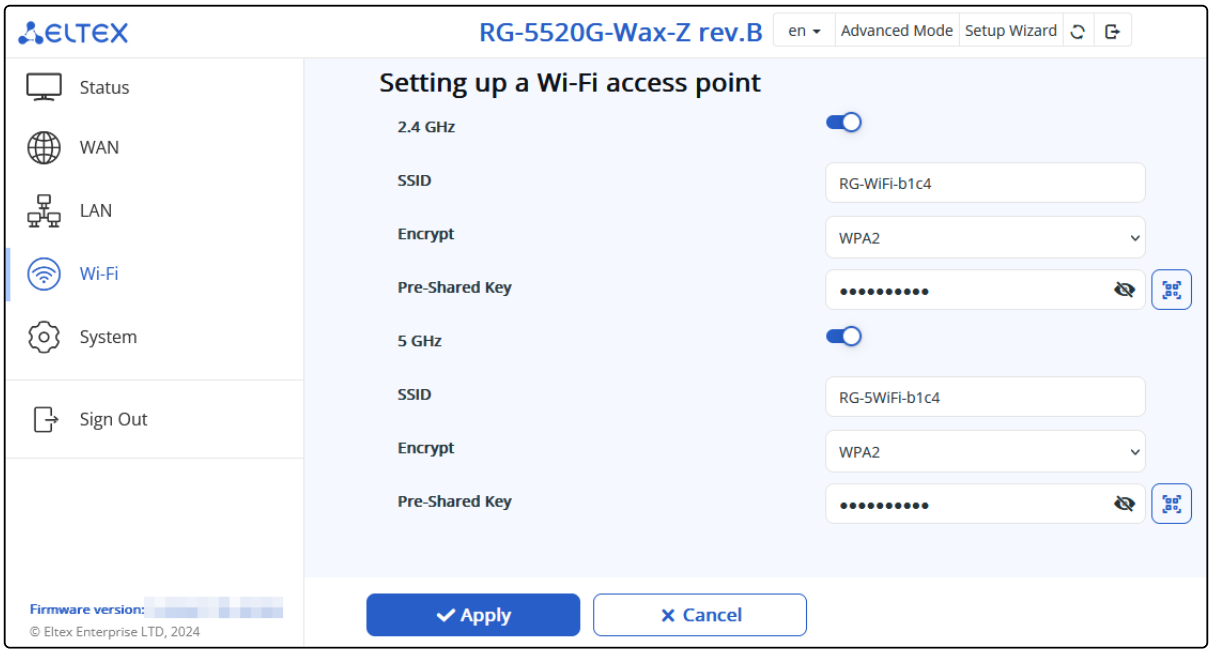
Subnet Mask — the value of the LAN network mask.

IP Pool Range Start Address — the start IP address from which addresses will be issued to clients. The address must fall within the range of the selected network.

IP Pool Range End Address — the last IP address that the device can issue to a client. Upon reaching it, the pool is considered exhausted until the already occupied address is released. The address must fall within the range of the selected network.

4.5.5 Wi-Fi menu

This menu performs the basic settings of the Wi-Fi network. Settings are made for a 2.4 GHz or 5 GHz Wi-Fi network. The device supports simultaneous operation in two frequency bands.



2.4 GHz/5 GHz toggle button — when on, the 2.4 GHz/5 GHz Wi-Fi radio frequency interface is enabled.

SSID — name of the wireless network used to connect to the device. The maximum length of the name is 32 characters, case-sensitive. This parameter can consist of numbers, Latin letters, spaces, and symbols “-“, “_”, “.”, “!”, “;”, “#”, but the symbols “!”, “;” , “#” and space cannot stand first.

Encrypt — selecting the wireless network security mode:

- *Disabled* — no wireless network encryption, low security level.
- *WEP* — WEP encryption. WEP Pre-Shared Key must consist of hexadecimal digits and be 10 or 26 characters long, or it must be a string (characters a-z, A-Z, 0-9, ~!@#$%^&*()_-+=) and have a length of 5 or 13 characters (by default, 26 characters HEX/13 ASCII characters, to switch to 10 HEX/5 ASCII characters, go to the Advanced Mode, Wi-Fi menu → Advanced Security Settings submenu and specify the Key Length — web64, when WEP Encryption is selected);
- *WPA* — WPA encryption. The key length ranges from 8 to 63 characters. It is allowed to use only the following characters: a-z, A-Z, 0-9, ~!@#$%^&*()_-+=;:\\|/?.,<>”` or a space;
- *WPA2* — WPA2 encryption. The key length ranges from 8 to 63 characters. It is allowed to use only the following characters: a-z, A-Z, 0-9, ~!@#$%^&*()_-+=;:\\|/?.,<>”` or a space;
- *WPA/WPA2* is a mixed encryption mode that supports WPA and The key length ranges from 8 to 63 characters. It is allowed to use only the characters: a-z, A-Z, 0-9, ~!@#$%^&*()_-+=;:\\|/?.,<>”` or a space;
- *WPA3* — WPA3 encryption, has a higher level of security compared to WPA2. The key length ranges from 8 to 63 characters. It is allowed to use only the following characters: a-z, A-Z, 0-9, ~!@#$%^&*()_-+=;:\\|/?.,<>”` or a space.
- *WPA2/WPA3* — mixed encryption mode that supports WPA2 and The key length ranges from 8 to 63 characters. It is allowed to use only the characters: a-z, A-Z, 0-9, ~!@#$%^&*()_-+=;:\\|/?.,<>”` or a space.

Pre-Shared Key — the encryption key that will provide access to the network.

In the Simple Mode, the device is configured only in the "Access Point" mode. To set up a different operating mode, switch to Advanced Mode.

4.5.6 System menu

This menu contains configuration and firmware update options.

4.5.6.1 Firmware Update submenu

This submenu is designed to update the device's control firmware.

Active Firmware Version — the version of the firmware installed on the device.

In case of damage to the main firmware, the backup is automatically loaded.

If the firmware update is successful, the firmware backup process starts after 10 minutes.

To start the firmware update process, click the "Start Upgrading" button.

To start checking for updates, click the "Check For Update" button.

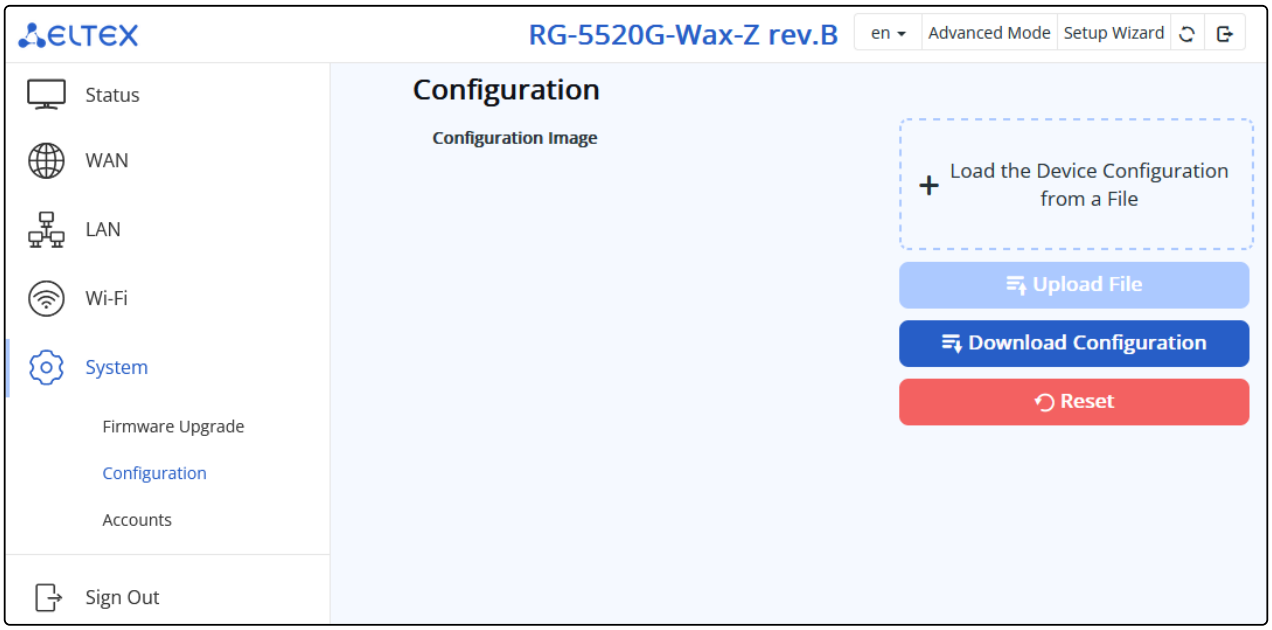
Do not turn off the device or reboot it during the firmware update process.

4.5.6.2 Configuration submenu

In the "Configuration" submenu, the current configuration is saved and updated.

If one is not sure about any settings, it is recommended to save the configuration file of the current installations to restore the configuration in an emergency.

Also, if necessary, one can reset all the settings to factory settings and then configure the device again.



Configuration Image — selection of the configuration file saved on the local computer. To update the device configuration, click the "Load the Device Configuration from a File" button, select the file (in .cfg format) and click the "Upload File" button.

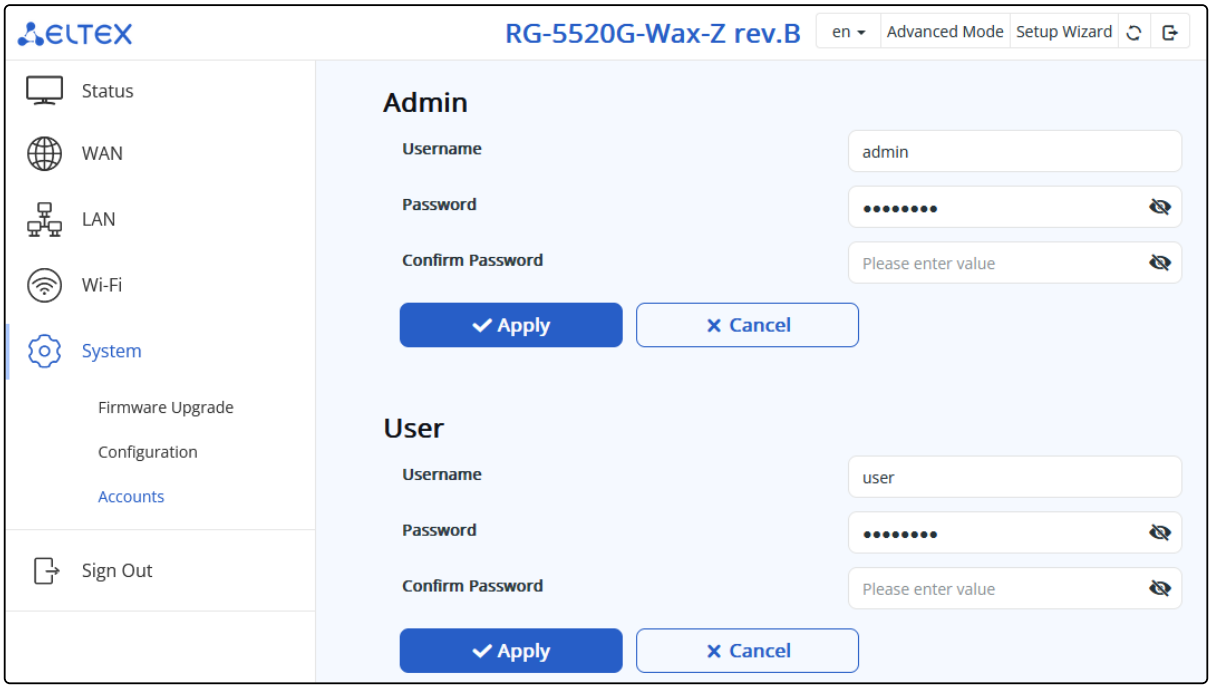
"Download Configuration" — click the button to save the current device configuration to the local computer.

"Reset" — click the button to reset all device settings to the default factory settings.

4.5.6.3 Accounts submenu

In the "Accounts" submenu, the user name and password for accessing the device web interface for the Admin and User accounts are set.

The Admin account is available for viewing and editing only when logged in under this account. The User account only allows one to change one's own account.



Admin

Username — a field for changing the user name.

Password — the input field for changing the device password.

Confirm Password — a field for re-entering a new password in order to confirm it.

User

Username — a field for changing the user name.

Password — the input field for changing the device password.

Confirm Password — a field for re-entering a new password in order to confirm it.

4.5.7 Sign out menu

The menu for logging out of the current account.

4.6 Device control panel in Advanced Mode

All device settings changes are performed using the control panel menulocated on the left side of the web interface

4.6.1 Key elements of the Advanced Mode web interface

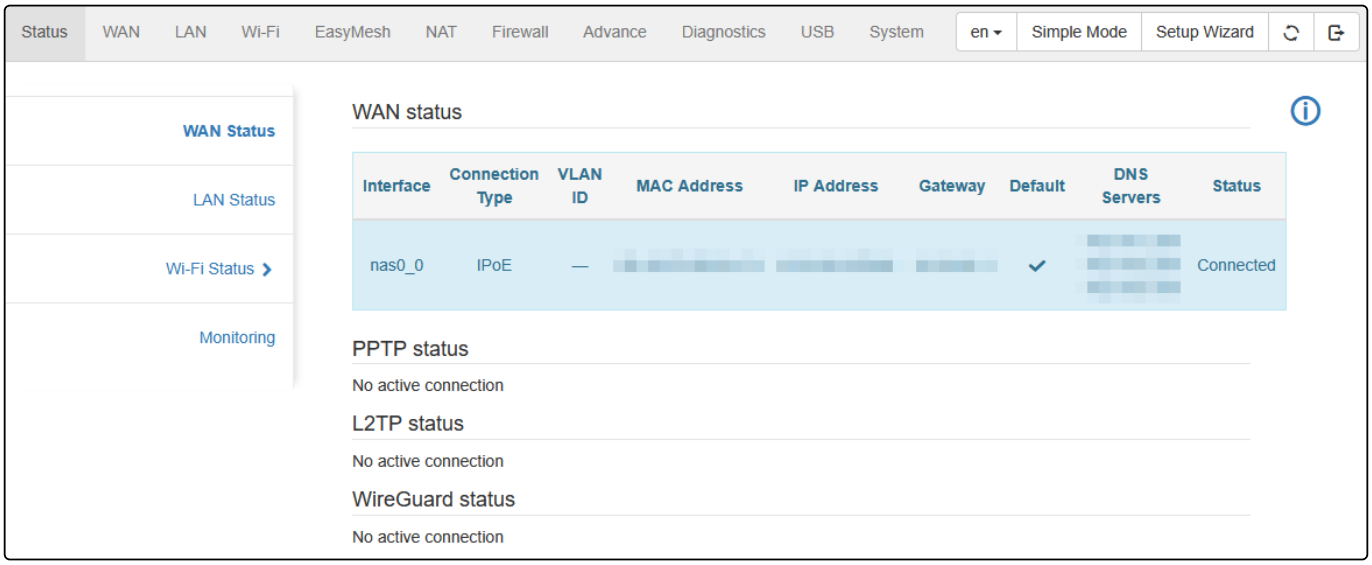
1. Menu for changing the web interface language, mode of the web interface, launching the Setup Wizard, with reboot and log out buttons;
2. The upper horizontal menu;
3. Control panel submenus;
4. The main field of the device settings, corresponding to the selected submenu from the field 3;
5. Buttons for applying configuration changes and cancelling to the last saved values.

4.6.2 Status menu

The "Status" menu displays summary information on the status of the device interfaces.

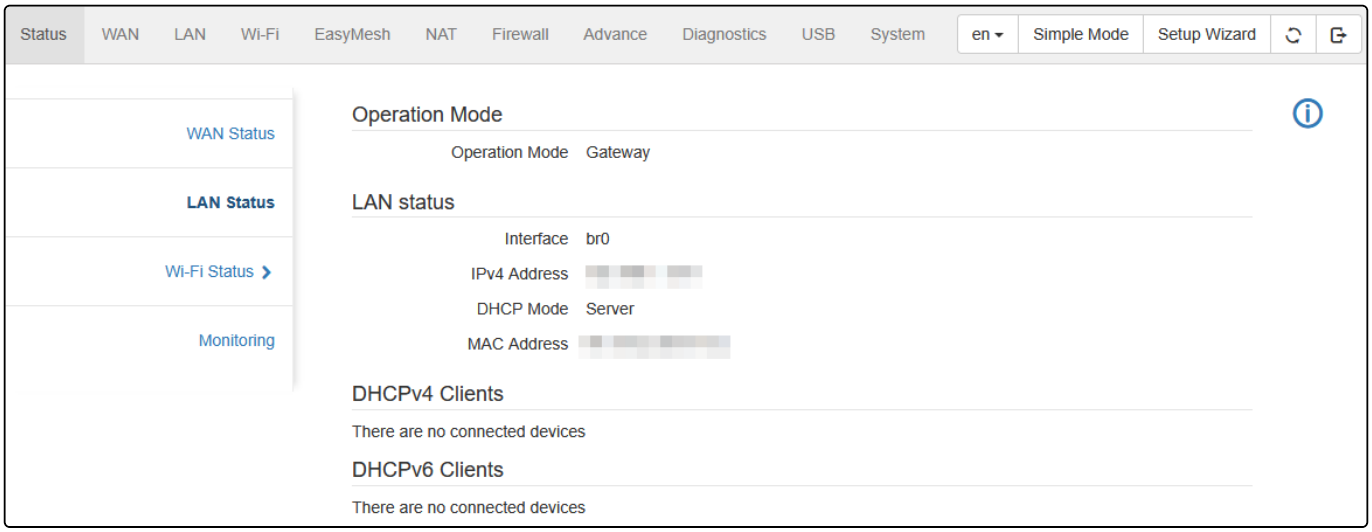
4.6.2.1 WAN Status submenu

This submenu displays information about configured WAN connections.



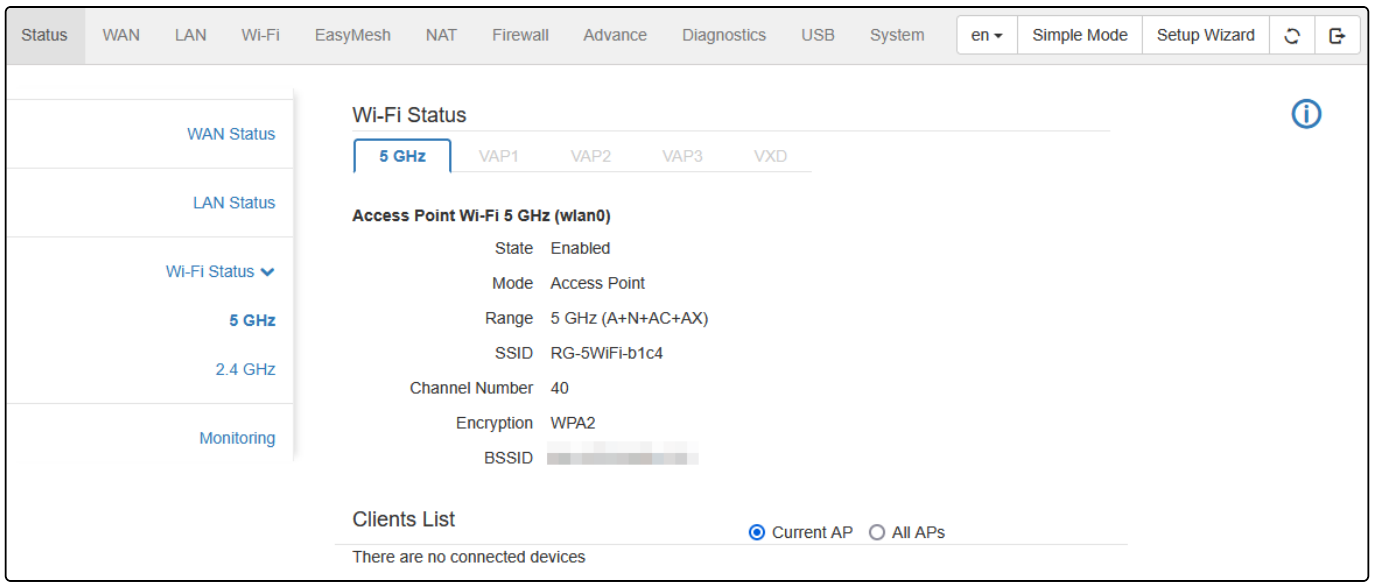
4.6.2.2 LAN Status submenu

The "LAN Status" submenu displays information about the device operating mode, the LAN bridge interface, and connected DHCPv4 and DHCPv6 clients.



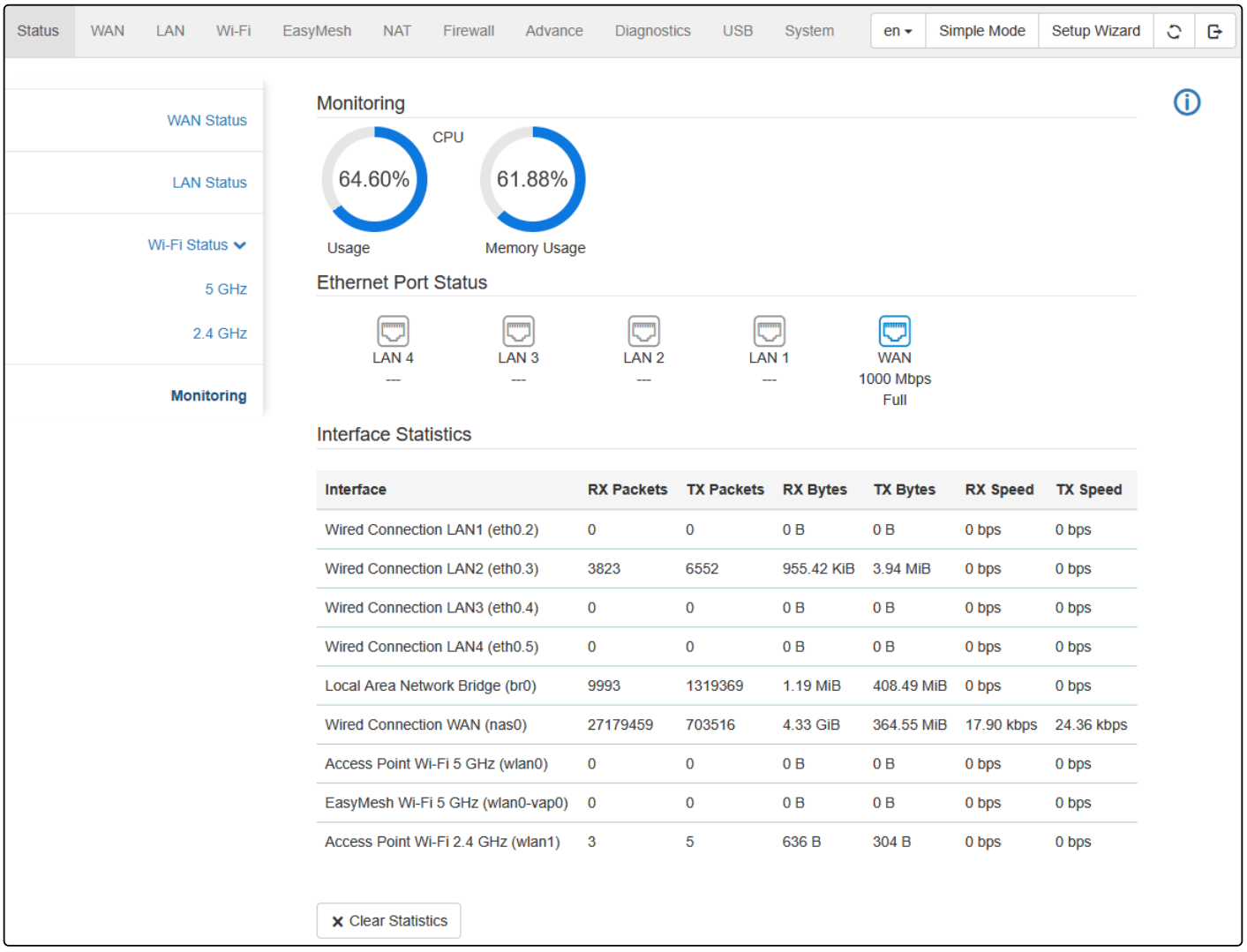
4.6.3 Wi-Fi Status submenu

This submenu contains a list of wireless clients for each of the frequency ranges individually, as well as basic access point (AP) parameters such as SSID, channel, and encryption. Clients are displayed for each VAP separately (select "Current AP") or for the entire range at once (select "All APs").



4.6.4 Monitoring submenu

Monitoring shows the CPU and memory usage, the status of the Ethernet ports, as well as the number of transmitted and received packets, and the current receive and transmit speeds for each interface.



Clear Statistics — a button to reset the counters of received and transmitted packets.

4.6.5 WAN menu

In this menu, the parameters of the device's WAN interfaces, as well as the parameters of VLAN connections, are available for configuration.

4.6.5.1 Ethernet WAN submenu

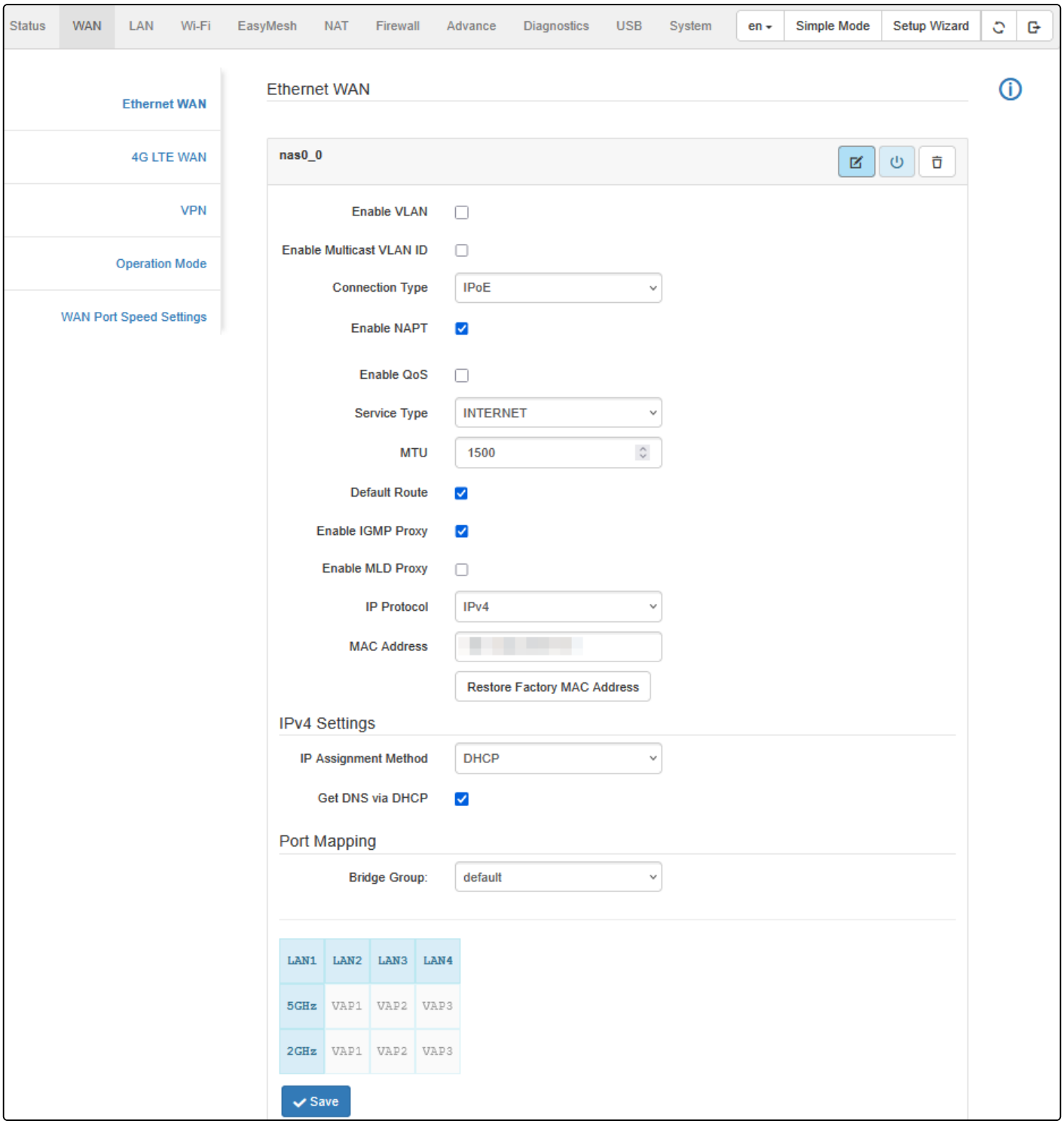
In the "Ethernet WAN" submenu, one can configure multiple WAN interfaces.

To add a new WAN connection, click  .

To delete the current WAN connection, click  .

To turn it off, click  . Clicking the button again will turn on this WAN interface.

To edit the WAN connection, click  .



Enable VLAN — when the flag is set, it allows one to use tags of the 802.1Q standard:

- *VLAN ID* — selection of the VLAN number to be used for this WAN;
- *1p Priority* is the value of the Priority code point (PCP) field used by the IEEE 802.1p standard to set the priority of transmitted traffic.

Enable Multicast VLAN ID — when the flag is set, it allows one to use tags of the 802.1Q standard for multicast traffic.

- *Multicast VLAN ID* — selecting the VLAN number to be used for routing multicast traffic for this WAN.

Connection Type — selection of protocol used to connect the device WAN interface to the provider's service network:

- *IPoE* — the mode of operation in which the device routes traffic with or without NAT; network settings can be obtained from the DHCPv4 server/DHCPv6 server/RADVD or configured manually;
- *Bridged* — network bridge mode; network settings can be obtained from the DHCPv4/ DHCPv6 server/ RADVD or configured manually;
- *PPPoE* — the mode of operation in which the RPPoE session is reconnected on the WAN interface; network settings can be obtained from the PPPoE server/DHCPv6 server/RADVD;
- *6rd* — the mode of operation in which it is possible to provide access to an IPv6 network on top of an existing IPv4 network.

MTU — the maximum packet size in bytes.
MAC Address — the MAC address substitution for a given WAN.
Restore Factory MAC Address — restoring the factory MAC address for a given WAN.
Port Mapping — a port forwarding feature.

IPoE connection type

Enable NAPT — enable network address/port translation. *Enable QoS* — enable the QoS feature for this WAN.
Service Type:

- *INTERNET* — provides Internet access.
- *TR069* — runs the TR069 client on the interface.
- *TR069_INTERNET* — provides Internet access and runs the TR069 client on the interface.

Default Route — when the flag is set, the default route will be set for this WAN.
Enable IGMP Proxy — enabling IGMP Proxy for multicast traffic tracking and broadcasting.
Enable MLD Proxy — enabling the MLD Proxy feature for multicast tracking and broadcasting.
IP Protocol — selection of network protocols used for this WAN:

- *IPv4* — the mode of operation with network access over IPv4 only;
- *IPv6* — the mode of operation with network access over IPv6 only;
- *IPv4/IPv6* — a Dual Stack mode with network access over both IPv4 and IPv6.

IPv4

IP Assignment Method:

- *DHCP* — mode of operation with receiving settings from the DHCP server:
  - *Get DNS via DHCP* — when the flag is set, the DNS settings will be received via DHCP. Without the flag set, the following fields will be displayed:
    - *Preferred DNS Server* — setting the address of the primary DNS server;
    - *Alternative DNS Server* — setting the address of the additional DNS server.
- *Fixed IP* — operating mode with manual setting of the address and network parameters:
  - *IP Address* — IP address of the WAN interface of the device on the provider network;
  - *Gateway* — address of the default gateway to which the packet is sent if no route is found for it in the routing table;
  - *Subnet Mask* — external subnet mask;
  - *Preferred DNS* Server — setting the address of the primary DNS server;
  - *Alternative DNS Server* — setting the address of an additional DNS-server.
- *No IP Assignment* — mode of operation with no network address on the interface.

IPv6

IP Assignment Method:

- *Stateful DHCPv6* is a mode of operation with automatic address and network settings via Gateway is set using ICMPv6. Routing and prefix delegation to the local network are provided:

  Get DNS automatically — when the flag is set, DNS settings will be received via ICMPv6/DHCPv6 (depending on the settings in the router message). The following fields will be displayed without the flag set:

  - *Preferred DNS* Server — setting the address of the primary DNS server;
  - *Alternative DNS Server* — setting the address of an additional DNS-server.

  Request IANA — request a permanent address via DHCPv6;

  Request IAPD — request a delegated prefix via DHCPv6;

  DS-Lite — the setting of an address for a technology that allows IPv4 access without changing the end-user software.

  AFTR IP Assignment Method — the method of obtaining a network address for AFTR:

  Static — operation mode with manual address setting:

  AFTR IP address — the AFTR IP address.

  Auto — the mode of operation with automatic address setting.

- *Stateless DHCPv6+SLAAC* — a mode of operation with ICMPv6 address settings and DHCPv6 network settings. Gateway is set using Routing and prefix delegation to the local network are provided:

  Get DNS automatically — when the flag is set, DNS settings will be received via DHCPv6. The following fields will be displayed without the flag set:

  - *Preferred DNS* Server — setting the address of the primary DNS server;
  - *Alternative DNS Server* — setting the address of an additional DNS-server.

  DS-Lite — the setting of an address for a technology that allows IPv4 access without changing the end-user software.

AFTR IP Assignment Method — the method of obtaining a network address for AFTR:

Static — operation mode with manual address setting:

AFTR IP address — the AFTR IP address.

Auto — the mode of operation with automatic address setting.

- *SLAAC* — a mode of operation with the configuration of the address, network settings and gateway via Prefix routing and delegating to the local network is only possible if the prefix is statically set on the LAN:

  Get DNS automatically — when the flag is set, DNS settings will be received via ICMPv6. Without the flag set, the following fields will be displayed:

  - *Preferred DNS Server* — setting the address of the primary DNS server;
  - *Alternative DNS Server* — setting the address of the additional DNS server.

  DS-Lite is the setting of an address for a technology that allows IPv4 access without changing the end-user software.

  AFTR IP Assignment Method is the method of obtaining a network address for AFTR:

  Static — operation mode with manual address setting:

  AFTR IP address is the AFTR IP address.

  Auto — the mode of operation with automatic address setting.

- *Fixed IP* — a mode of operation with manual setting of the address and network parameters. Prefix routing and delegating to the local network is only possible if the prefix is statically set on the LAN:

  IPv6 address — the IP address of the WAN interface of the device on the provider's network.

  IPv6 gateway — the default gateway address to which the packet is sent if no route is found for it in the routing table.

  Ipv6 Address Prefix Length — external subnet prefix;

  Preferred DNS server — the setting of the primary DNS server address;

  Alternative DNS server — the setting of the additional DNS server address;

  DS-Lite — the setting of an address for a technology that allows IPv4 access without changing the end-user software.

  AFTR IP Assignment Method — the method of obtaining a network address for AFTR:

  Static — operation mode with manual address setting:

  AFTR IP address — the AFTR IP address.

  Auto — the mode of operation with automatic address setting.

- *Autodetection* — a mode of operation with automatic configuration of the address and network settings via ICMPv6/DHCPv6. Gateway is set using Routing and prefix delegation to the local network are provided:

  Get DNS automatically — when the flag is set, DNS settings will be received via ICMPv6/DHCPv6. The following fields will be displayed without the flag set:

  - *Preferred DNS* Server — setting the address of the primary DNS server;
  - *Alternative DNS Server* — setting the address of an additional DNS-server.

  DS-Lite is the setting of an address for a technology that allows IPv4 access without changing the end-user software.

AFTR IP Assignment Method is the method of obtaining a network address for AFTR:

Static — operation mode with manual address setting:

AFTR IP address is the AFTR IP address.

Auto — the mode of operation with automatic address setting.

Bridged Connection Type

802.1d Spanning Tree — enabling the STP feature.

Enable IGMP Proxy — enabling IGMP Proxy for multicast traffic tracking and broadcasting.

IPv4

IP Assignment Method:

- *DHCP* — mode of operation with receiving settings from the DHCP server:

  Get DNS via DHCP — when the flag is set, the DNS settings will be received via DHCP. Without the flag set, the following fields will be displayed:

  - *Preferred DNS Server* — setting the address of the primary DNS server;
  - *Alternative DNS Server* — setting the address of the additional DNS server.
- *Fixed IP* — operating mode with manual setting of the address and network parameters:

  IP Address — IP address of the WAN interface of the device on the provider network.

  Gateway — address of the default gateway to which the packet is sent if no route is found for it in the routing table.

  Subnet Mask — external subnet mask.

  Preferred DNS Server — setting the address of the primary DNS server;

  Alternative DNS Server — setting the address of an additional DNS-server.
- *No IP Assignment* — mode of operation with no network address on the interface.

PPPoE Connection Type

Enable NAPT — enable network address/port translation.

Enable QoS — enable the QoS feature for this WAN.

Service Type:

- *INTERNET* — provides Internet access;
- *TR069* — runs the TR069 client on the interface;
- *TR069_INTERNET* — provides Internet access and runs the TR069 client on the interface.

Default Route — when the flag is set, the default route will be set for this WAN.

Enable IGMP Proxy without encapsulation — multicast traffic will go to the transport WAN-interface.

Enable IGMP Proxy with encapsulation — multicast traffic will go inside the PPPoE tunnel just like regular traffic.

Enable MLD Proxy — enabling the MLD Proxy feature for multicast tracking and broadcasting.

IP Protocol — selection of network protocols used for this WAN:

- *IPv4* — the mode of operation with network access over IPv4 only;
- *IPv6* — the mode of operation with network access over IPv6 only;
- *IPv4/IPv6* is a Dual Stack mode with network access over both IPv4 and

Username is the username for authorization on the PPPoE server.

Password is the password for authorization.

PPPoE Connection Type — select the type of PPPoE connection:

- *Continuous* — the PPPoE session is permanently established.
- *On Demand* — the PPPoE session is established when there is network activity and terminated when there is no activity due to timeout.
    - *Idle Time (sec)* is the time after which an inactive PPP connection will be terminated.

Authentication Method is the authentication method on the PPPoE server.

Access Concentrator Name is the value of the Host-Uniq tag in the PADI message, which defines the name of the Access Concentrator (optional field).

Service Name is the value of the Service Name tag in the PADI message (optional field).

Get DNS automatically — when the flag is set, DNS settings will be received via PPP IPCP.

The following fields will be displayed without the flag set:

- *Preferred DNS* Server — setting the address of the primary DNS server;
- *Alternative DNS Server* — setting the address of an additional DNS-server.

IPv6

IP Assignment Method:

- *Stateful DHCPv6* is a mode of operation with automatic address and network settings via Gateway is set using ICMPv6. Routing and prefix delegation to the local network are provided:

    Get DNS automatically — when the flag is set, DNS settings will be received via ICMPv6/DHCPv6 (depending on the settings in the router message). The following fields will be displayed without the flag set:

    - *Preferred DNS* Server — setting the address of the primary DNS server;
    - *Alternative DNS Server* — setting the address of an additional DNS-server.

    Request IANA — request a permanent address via DHCPv6;

    Request IAPD — request a delegated prefix via DHCPv6;

    DS-Lite is the setting of an address for a technology that allows IPv4 access without changing the end-user software.

    AFTR IP Assignment Method is the method of obtaining a network address for AFTR:

    Static — operation mode with manual address setting:

    AFTR IP address is the AFTR IP address.

    Auto — the mode of operation with automatic address setting.

- *Stateless DHCPv6+SLAAC* is a mode of operation with ICMPv6 address settings and DHCPv6 network settings. Gateway is set using Routing and prefix delegation to the local network are provided:

    Get DNS automatically — when the flag is set, DNS settings will be received via DHCPv6. Without the flag set, the following fields will be displayed:

    - *Preferred DNS Server* — setting the address of the primary DNS server;
    - *Alternative DNS Server* — setting the address of the additional DNS server.

    DS-Lite —the setting of an address for a technology that allows IPv4 access without changing the end-user software.

    AFTR IP Assignment Method — the method of obtaining a network address for AFTR:

Static — operation mode with manual address setting:

AFTR IP address — the AFTR IP address.

Auto — the mode of operation with automatic address setting.

- *SLAAC* — a mode of operation with the configuration of the address, network settings and gateway via Prefix routing and delegating to the local network is only possible if the prefix is statically set on the LAN:

  Get DNS automatically — when the flag is set, DNS settings will be received via ICMPv6. Without the flag set, the following fields will be displayed:

  - *Preferred DNS Server* — setting the address of the primary DNS server;
  - *Alternative DNS Server* — setting the address of the additional DNS server.

  DS-Lite — the setting of an address for a technology that allows IPv4 access without changing the end-user software.

  AFTR IP Assignment Method — the method of obtaining a network address for AFTR:

  Static — operation mode with manual address setting:

  AFTR IP address — the AFTR IP address.

  Auto — the mode of operation with automatic address setting.

- *Fixed IP* — a mode of operation with manual setting of the address and network parameters. Prefix routing and delegating to the local network is only possible if the prefix is statically set on the LAN:

  IPv6 address — the IP address of the WAN interface of the device on the provider's network.

  IPv6 gateway — the default gateway address to which the packet is sent if no route is found for it in the routing table.

  Ipv6 Address Prefix Length — external subnet prefix; *Preferred DNS server* is the setting of the primary DNS server address; *Alternative DNS server* is the setting of the additional DNS server address;

  DS-Lite — the setting of an address for a technology that allows IPv4 access without changing the end-user software.

  AFTR IP Assignment Method — the method of obtaining a network address for AFTR:

  Static — operation mode with manual address setting:

  AFTR IP address — the AFTR IP address.

  Auto — the mode of operation with automatic address setting.

- *Autodetection* — a mode of operation with automatic configuration of the address and network settings via ICMPv6/DHCPv6. Gateway is set using Routing and prefix delegation to the local network are provided:

  Get DNS automatically — when the flag is set, DNS settings will be received via ICMPv6/DHCPv6. Without the flag set, the following fields will be displayed:

  - *Preferred DNS Server* — setting the address of the primary DNS server;
  - *Alternative DNS Server* — setting the address of the additional DNS server.

  DS-Lite — the setting of an address for a technology that allows IPv4 access without changing the end-user software.

  AFTR IP Assignment Method — the method of obtaining a network address for AFTR:

  Static — operation mode with manual address setting:

  AFTR IP address — the AFTR IP address.

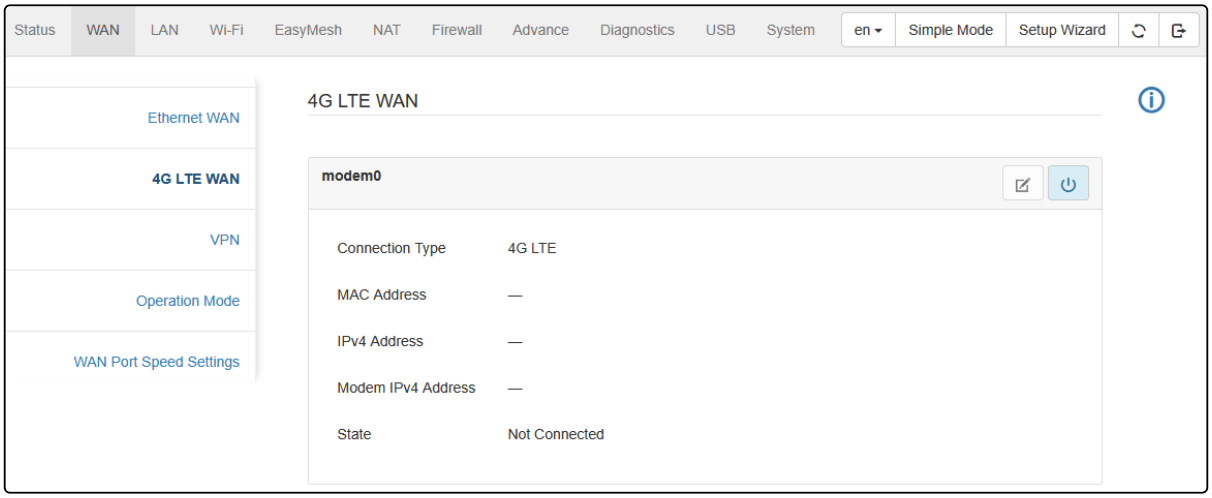
Auto — the mode of operation with automatic address setting.

4.6.5.2 4G LTE WAN submenu

In this submenu, one can set up a USB modem connection.

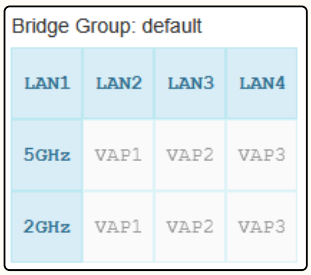
To turn it off, click  . Clicking the button again will enable the connection via USB modem.

To edit the connection, click  .



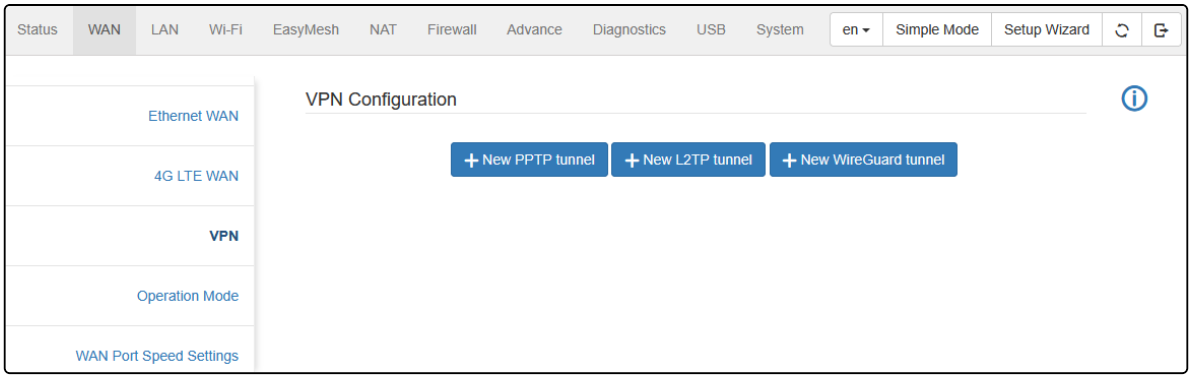
Connection settings and authorization data must be configured in the web interface of the USB modem. To access the USB modem web interface, click the modem IPv4 address.

When connecting a USB modem, the default WAN connection port group will be used. This means that ports configured for IPTV (Bridge connections) will not be able to access the network via a USB modem.
LAN1-4, 2.4 GHz and 5 GHz clients will have access to the network via a USB modem at factory settings.



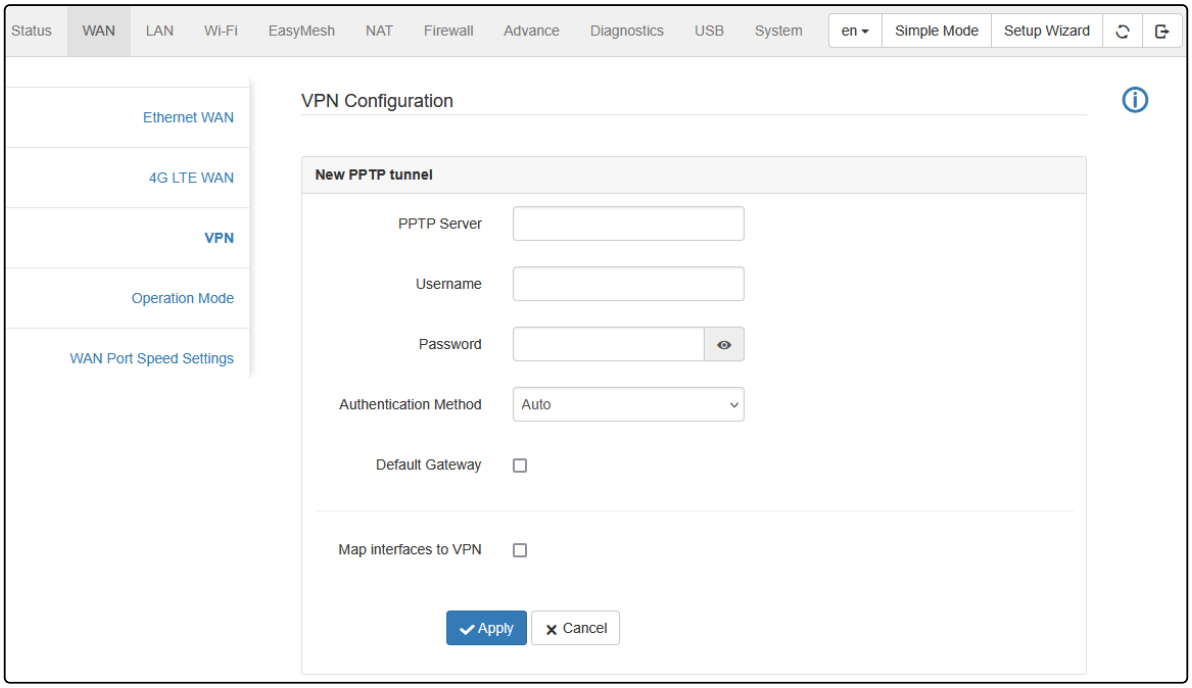
4.6.5.3 VPN submenu

In this submenu, one can configure the PPTP, L2TP (without IPsec) and WireGuard tunnels, which will be configured on the WAN interface with the default route. PPTP, L2TP, and WireGuard tunnels are created by clicking the corresponding buttons in the image below.



New PPTP tunnel

Clicking the "New PPTP tunnel" button opens a menu for configuring a PPTP tunnel which will be configured on the WAN interface with the default route.



PPTP Server — the address of the PPTP server.

Username — the username for authorization on the PPTP server.

Password — the key for authorization on the PPTP server.

Authentication Method — the authentication method on the PPTP server.

Encryption Type (available when CHAPMSV2 authentication method is selected) — a set of CHAPMSV2 ciphers.

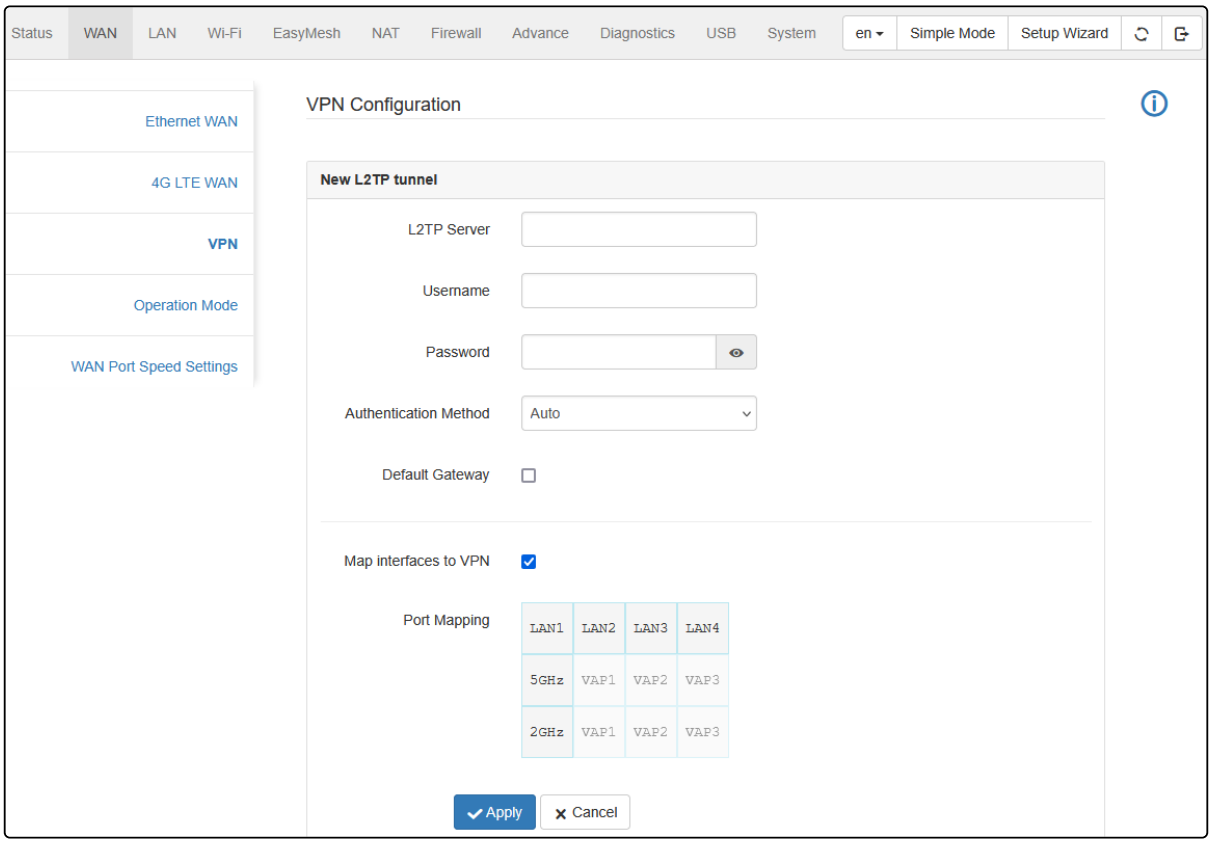
Default Gateway — enabling the default gateway.

Map interfaces to VPN — enable traffic redirection via VPN connection only from selected interfaces.

Port Mapping — selection of interfaces from which traffic is linked to a VPN connection.

New L2TP tunnel

Clicking the "New L2TP tunnel" button opens a menu for configuring an L2TP tunnel (without IPsec), which will be established on the WAN interface with the default route.



L2TP Server — address of the L2TP server;

Username — username for authorization on the L2TP server;

Password — the key for authorization on the L2TP server;

Authentication Method — the authentication method on the PPTP server;

Encryption Type (available when CHAPMSV2 authentication method is selected) — a set of CHAPMSV2 ciphers;

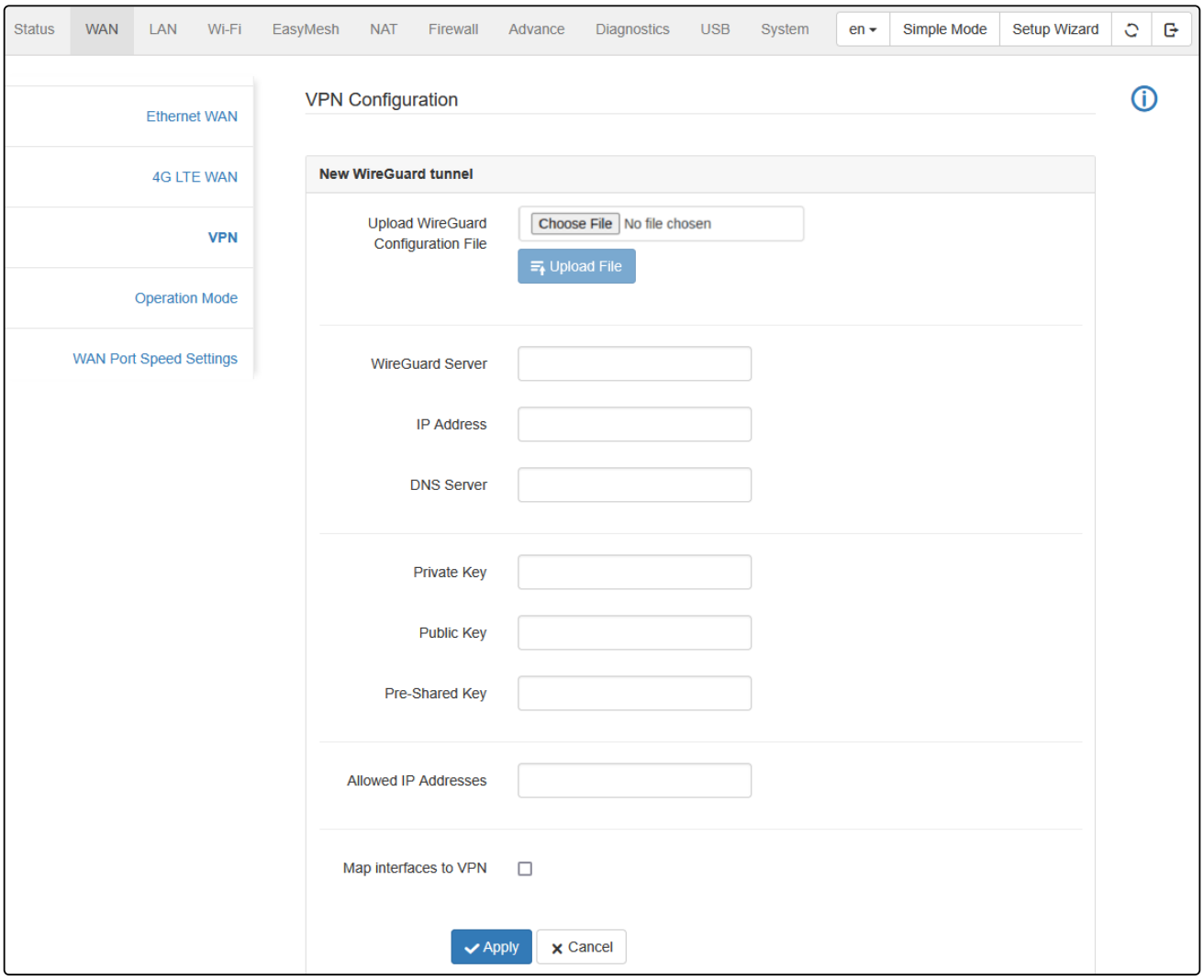
Default Gateway — enabling the default gateway;

Map interfaces to VPN — enable traffic redirection via VPN connection only from selected interfaces;

Port Mapping — selection of interfaces from which traffic is linked to a VPN connection.

New WireGuard tunnel

Clicking the "New WireGuard tunnel" button opens a menu for configuring the WireGuard tunnel, which will be established on the WAN interface with the default route.



Upload WireGuard Configuration File — select the configuration file saved on the local computer. To update the configuration, click the "Select File" button, select the file (in .conf format) and click the "Upload File" button.

WireGuard Server — address of the WireGuard server.

IP Address — client address used in the tunnel.

DNS Server — address of the DNS server used in the tunnel.

Private Key — key of the WireGuard client for decryption.

Public Key — key of the WireGuard server for encryption.

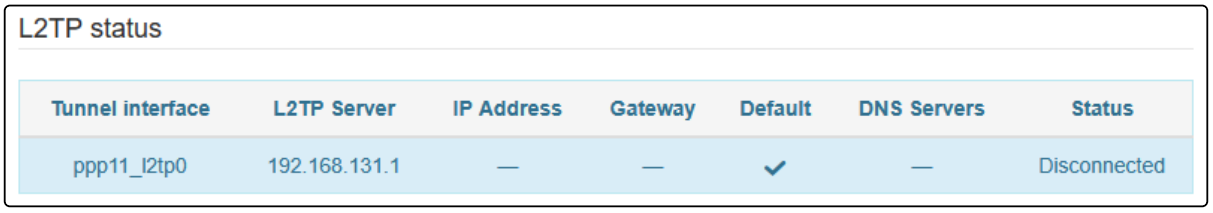
Pre-Shared Key — WireGuard server key for additional traffic encryption.

Allowed IP Addresses — IP addresses that will be allowed to access the server.

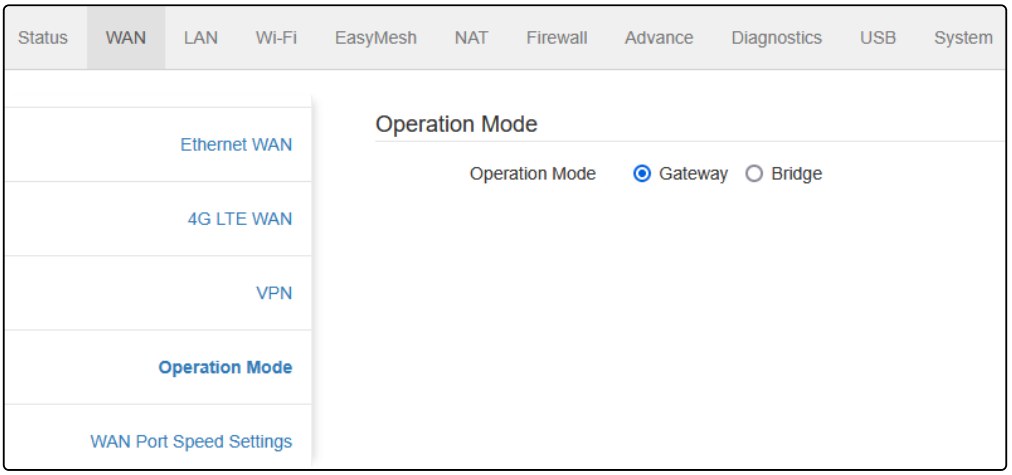
Map interfaces to VPN — enable traffic redirection via VPN connection only from selected interfaces.

Port Mapping — selection of interfaces from which traffic is linked to a VPN connection.

Example of displaying a configured L2TP tunnel



4.6.5.4 Operation Mode submenu

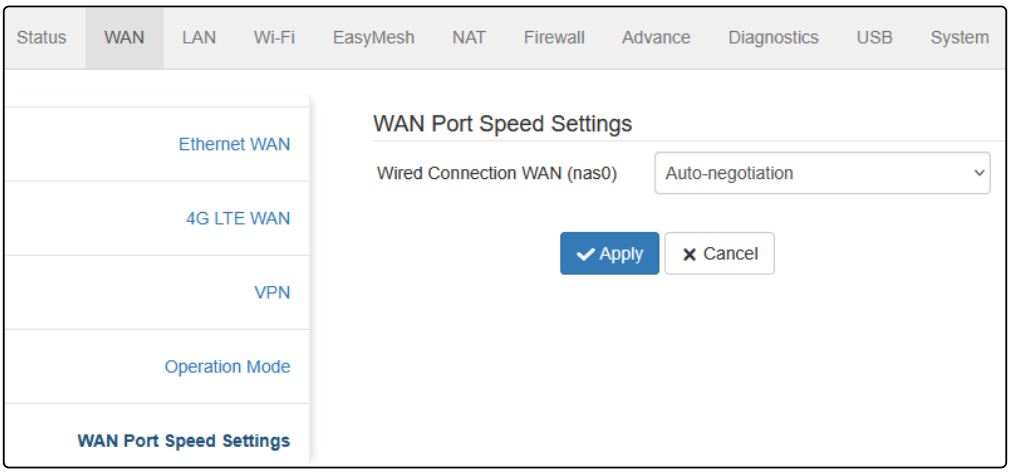


Gateway — standard operation mode of the router. NAT is enabled, the DHCP client is running on the WAN and the DHCP server on the LAN side.

Bridge — in this operation mode device is fully switched to bridge mode, all interfaces are combined at the link level and NAT is disabled. Access to the device will be saved only from a statically set IP address from the router's subnet (by default, 192.168.1.1/24). If necessary, it is possible to configure the desired DHCP operation mode in this mode in the IPv4 Network Setting submenu in LAN menu → LAN Interface Settings.

4.6.5.5 WAN Port Speed Settings submenu

This submenu contains speed settings for the WAN port.



Wired Connection WAN (nas0) — there are 10 modes available:

Auto-negotiation — automatic configuration of the data transfer rate by Ethernet nodes using IEEE 802.3 technology.

Auto-negotiation, full — automatic adjustment of the data transfer rate by Ethernet nodes using IEEE 802.3 technology in duplex mode.

2500M, full — duplex data transfer mode with speeds up to 2.5 Gbps.

1000M, full — duplex data transfer mode with speeds up to 1 Gbps.

100M, full — duplex data transfer mode with speeds up to 100 Mbps.

100M, half — half-duplex data transfer mode with speeds up to 100 Mbps.

100M, auto-negotiation — automatic duplex/half-duplex mode setting with data transfer speeds up to 100 Mbps.

10M, full — duplex data transfer mode with speeds up to 10 Mbps.

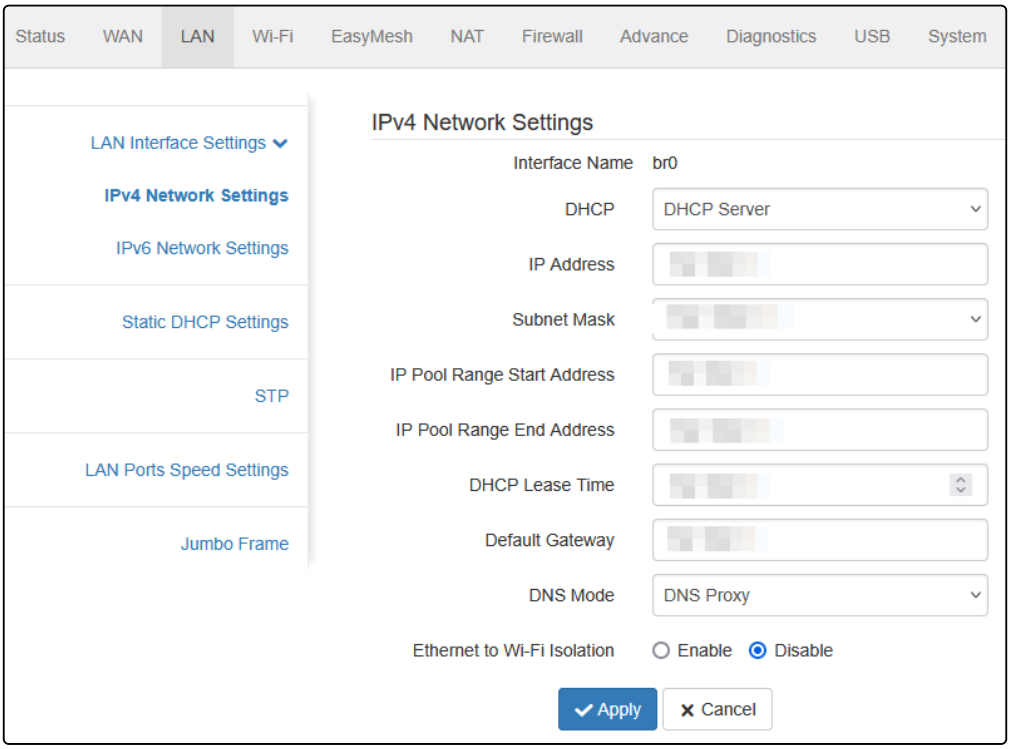
10M, half — half-duplex data transfer mode with speeds up to 10 Mbps.

10M, auto-negotiation — automatic duplex/half-duplex mode setting with data transfer speeds up to 10 Mbps.

4.6.6 LAN menu

4.6.6.1 LAN Interface Settings. IPv4 Network Settings submenu

In the "IPv4 Network Settings" submenu, the parameters of the local bridge interface over the IPv4 protocol are configured.



DHCP — operating mode of DHCP. The following modes are available:

- *Disabled* — DHCP on LAN is disabled, the device IP address is set manually.
- *DHCP Relay* — the client DHCP requests will be redirected to the address specified in the "*DHCP Server IP Address*" field;
- *DHCP Server* — IP addresses in the LAN network are provided by the device;
- *DHCP Client* — the device IP address for the LAN network will be obtained from a third-party DHCP server.

IP Address — the local IP address of the device.

Subnet Mask — the value of the LAN network mask.

IP Pool Range Start Address — the start IP address from which addresses will be issued to clients. The address must fall within the range of the selected network.

IP Pool Range End Address — the last IP address that the device can issue to a client. Upon reaching it, the pool is considered exhausted until the already occupied address is released. The address must fall within the range of the selected network.

DHCP Lease Time — lease time in seconds, after which the client must either release the address or extend it for the same period.

Default Gateway — the IP address of the gateway, which will be transmitted to LAN clients in DHCP option 3.

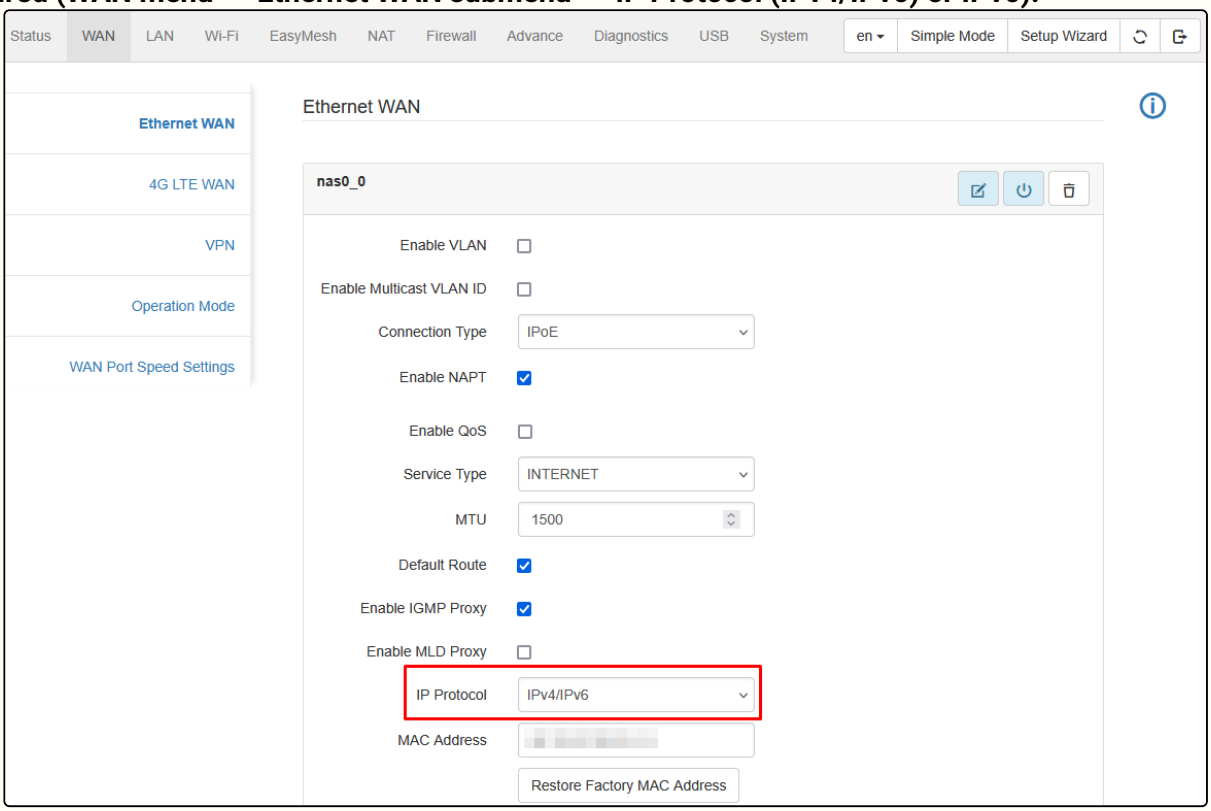
DNS Mode — mode of operation of the DNS protocol for LAN devices. The following values are available:

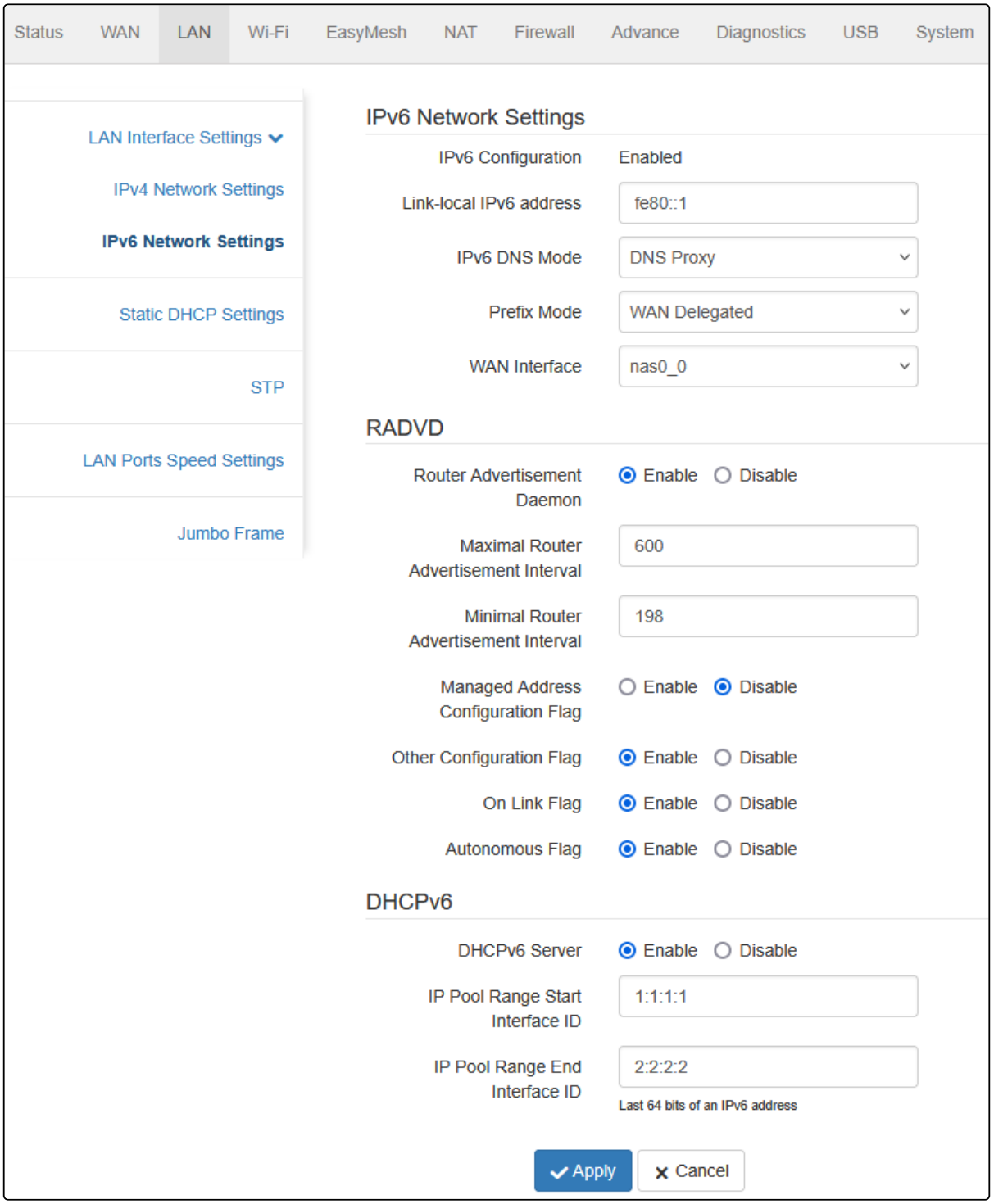
- *DNS Proxy* — LAN address of the device will be transmitted to clients in the DHCP option 6 as the DNS server;
- *Set Manually* — manually set DNS server addresses will be transmitted to clients in the DHCP option 6;
- *WAN Connection* — DNS addresses received from the specified WAN interface will be transmitted to clients in the DHCP option 6;

Ethernet to Wi-Fi Isolation — when the feature is enabled, wired clients will be isolated from wireless ones.

4.6.6.2 IPv6 Network Settings submenu

To configure the IPv6 LAN interface, a Dual Stack WAN (IPv4/IPv6) or IPv6 WAN connection is required (WAN menu → Ethernet WAN submenu → IP Protocol (IPv4/IPv6) or IPv6).





IPv6 Network Settings

IPv6 Configuration — enabled.

Link-local IPv6 address — link-local IPv6 address of the device.

IPv6 DNS Mode — DNS protocol operation mode, the default is DNS Proxy.

Prefix Mode — mode of setting the prefix in the local subnet, the default is WAN Delegated.

WAN Interface — selecting the WAN interface for RADVD prefix delegation.

RADVD

Router Advertisement Daemon — a router advertisement daemon, used for sending network information and auto-configuration on an IPv6 network.

- *Maximal Router Advertisement Interval* — the maximum interval for sending a router message.
- *Minimum Router Advertisement Interval* — the minimum interval for sending a router message.
- *Managed Address Configuration Flag* — configuration flag for the managed address, when enabled the IP address will be received via DHCPv6 (Stateful mode only).
- *Other Configuration Flag* — flag of other configuration. When DNS is enabled, other settings will be received via DHCPv6 (Stateful mode only).
- *On Link Flag* — direct availability flag. When enabled, it indicates the availability of the prefix in the broadcast domain.
- *Autonomous Flag* — flag for offline address configuration. When enabled, offline address configuration without tracking the status is allowed.

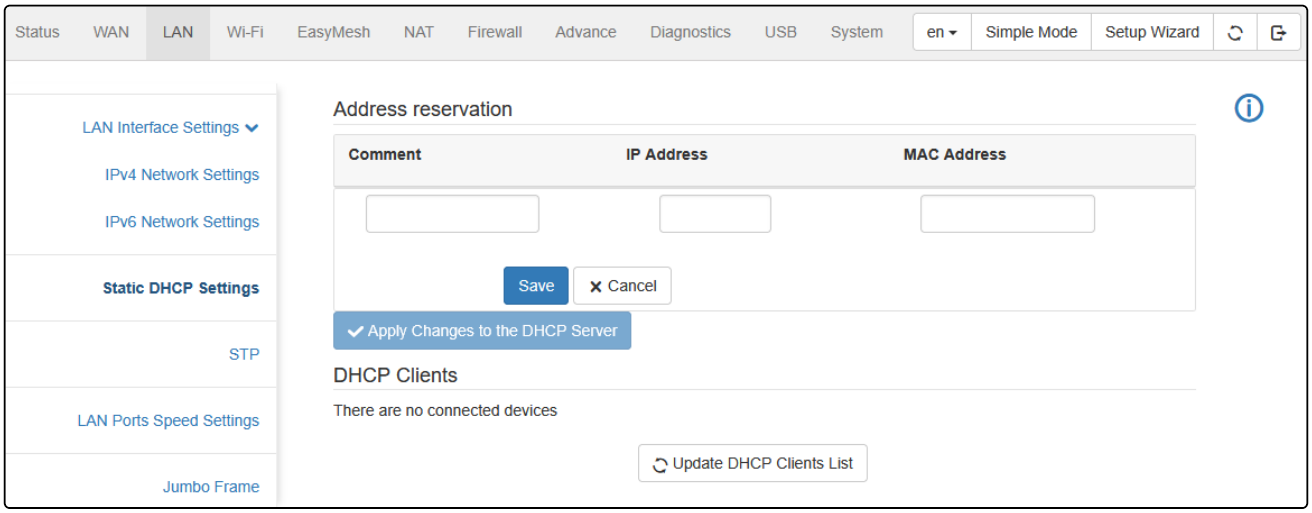
DHCPv6

DHCPv6 Server — enabling the DHCPv6 server:

- *IP Pool Range Start Interface ID* — the minimum interface ID (the last 64 bits of the address) issued via The first 64 bits are taken from the LAN prefix.
- *IP Pool Range End Interface ID* — the maximum interface ID (the last 64 bits of the address) issued via The first 64 bits are taken from the LAN prefix.

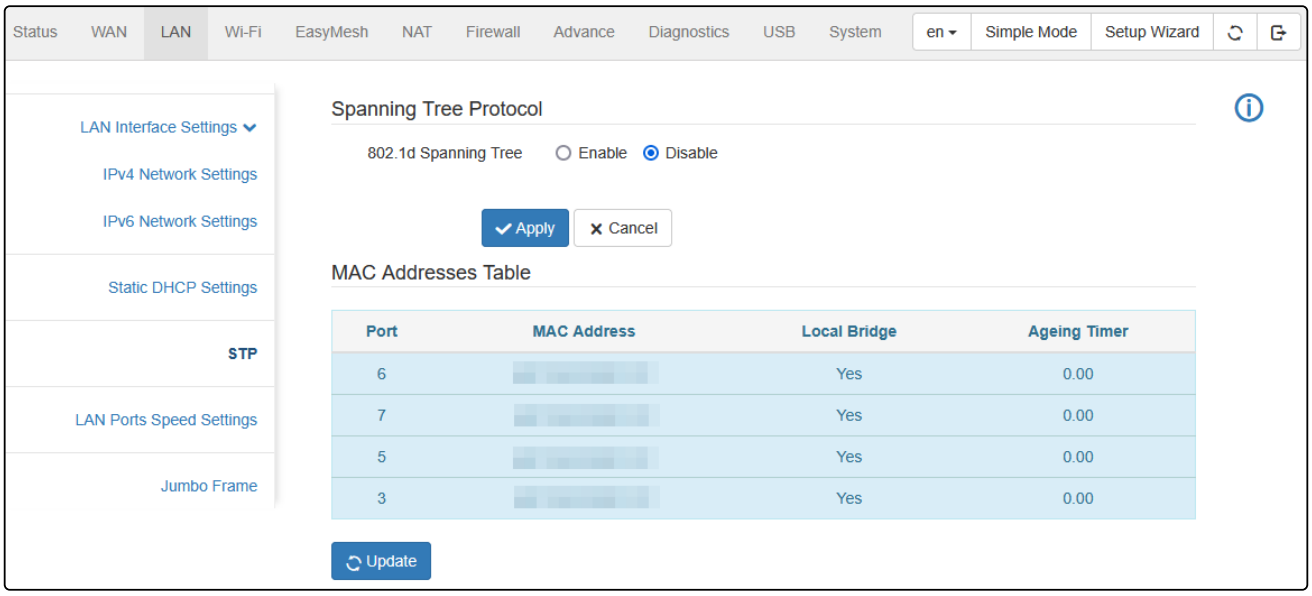
4.6.6.3 Static DHCP Settings submenu

This submenu contains a list of clients of the DHCP server, and it is also possible to reserve an address. To reserve an address for an active client, click the  ("Edit") button. Next, one can change the IP address, add a comment, and save the settings. To reserve an address for an inactive device, click  ("Add") button and fill in the MAC and IP address fields.



4.6.6.4 STP submenu

This submenu configures the STP protocol.



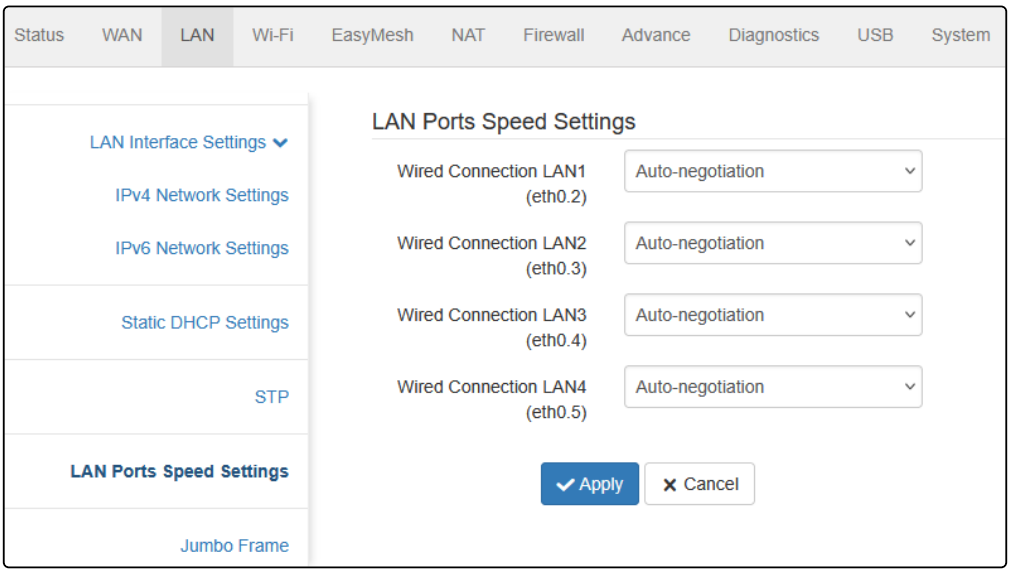
802.1d Spanning Tree — enabling the STP feature.

MAC Addresses Table — a display of the STP MAC address table.

Ageing Timer — the lifetime of records of dynamically learned MAC addresses by the device local bridge.

4.6.6.5 LAN Port Speed Settings submenu

This submenu contains the speed selection settings for each port according to its serial number.



There are 9 modes available:

Auto-negotiation — automatic configuration of the data transfer rate by Ethernet nodes using IEEE 802.3 technology.

Auto-negotiation, full — automatic adjustment of the data transfer rate by Ethernet nodes using IEEE 802.3 technology in duplex mode.

1000M, full — duplex data transfer mode with speeds up to 1 Gbps.

100M, full — duplex data transfer mode with speeds up to 100 Mbps.

100M, half — half-duplex data transfer mode with speeds up to 100 Mbps.

100M, auto-negotiation — automatic duplex/half-duplex mode setting with data transfer speeds up to 100 Mbps.

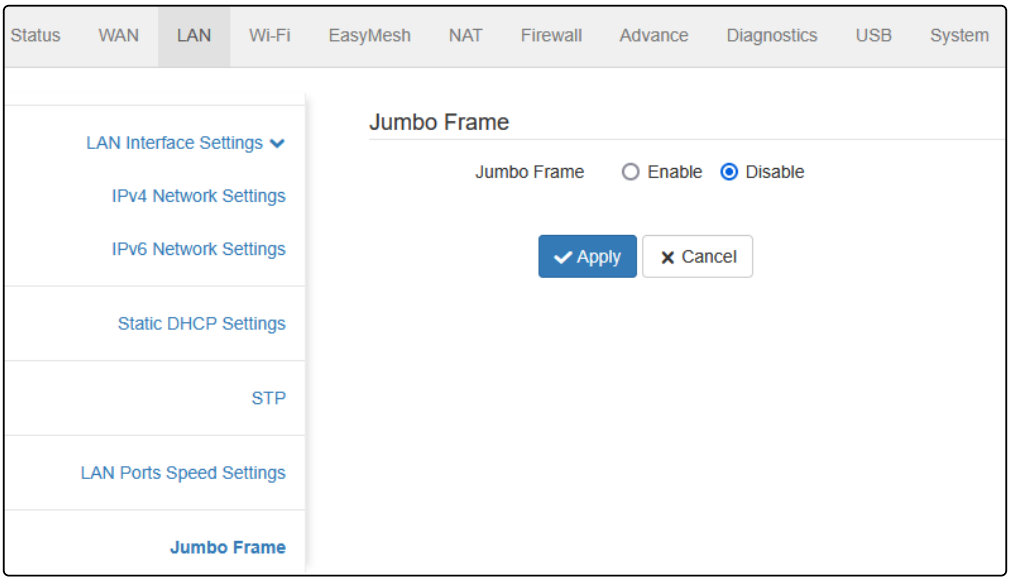
10M, full — duplex data transfer mode with speeds up to 10 Mbps.

10M, half — half-duplex data transfer mode with speeds up to 10 Mbps.

10M, auto-negotiation — automatic duplex/half-duplex mode setting with data transfer speeds up to 10 Mbps.

4.6.6.6 Jumbo Frame submenu

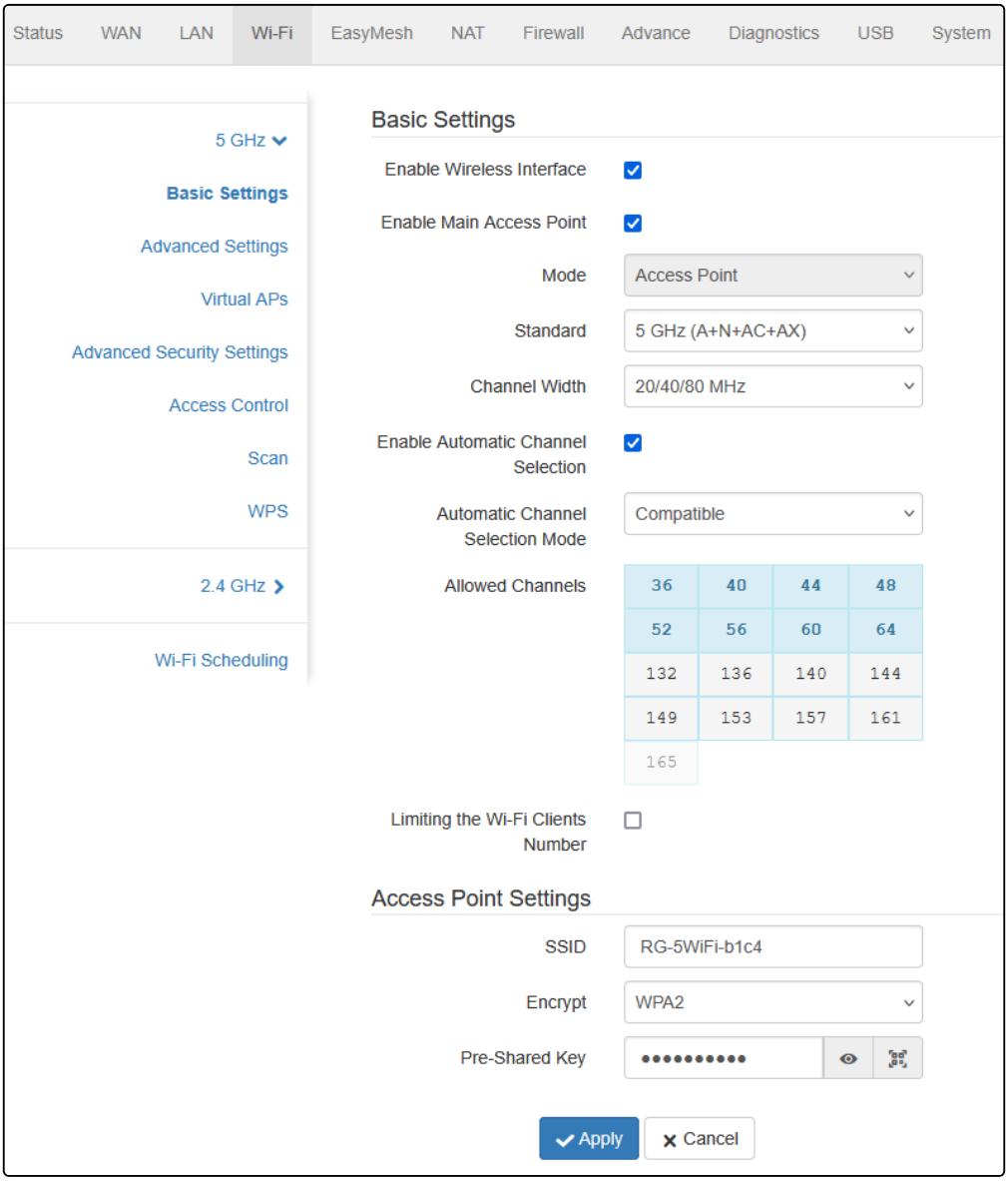
This submenu is used to configure the interfaces of devices that work with Ethernet frames values exceeding the standard 1,500 bytes.



4.6.7 Wi-Fi menu

In the "Wi-Fi" menu, the settings of the wireless Wi-Fi network are performed. The settings are made for the Wi-Fi network at a frequency of 2.4 GHz or 5 GHz. The device supports simultaneous operation in two frequency bands.

4.6.7.1 Basic Settings submenu



Basic Settings

Enable Wireless Interface — when the flag is set Wi-Fi interface in the range 2.4/5 GHz is enabled.

Enable Main Access Point — when the flag is set, the main Wi-Fi access point in the selected 2.4/5 GHz band will be enabled.

Mode — allows one to select which mode the radio module will operate in:

- *Access Point* — *access* point operating mode.
- *Client* — client operating mode;
- *Repeater* — repeater operating mode.

Standard — selection of the operating mode for the wireless interface in accordance with the Wi-Fi 802.11 series of standards.

- *For 2.4 GHz*:
  - *2.4 GHz (B)* — if all wireless clients support the 802.11b standard, the maximum speed according to this standard is 11 Mbps;
  - *2.4 GHz (G)* — according to the 802.11g standard, the maximum speed is 54 Mbps;
  - *2.4 GHz (N)* — according to the 802.11n standard, the maximum speed is 300 Mbps;
  - *2.4 GHz (B+G)* — if the network has wireless clients with 802.11b and 802.11g support, according to the 802.11g standard, the maximum speed is 54 Mbps;
  - *2.4 GHz (G+N)* — if the network has wireless clients with 802.11g and 802.11n support, the maximum speed is 300 Mbps;
  - *2.4 GHz (B+G+N)* — if the network has wireless clients with support for 802.11b, 802.11g and 802.11n, then the maximum speed is 300 Mbps;
  - *2.4 GHz (AX)* — according to the 802.11ax standard, the maximum speed is 573.5 Mbps;
  - *2.4 GHz (B+G+N+AX)* — the mode supports devices with 802.11b, 802.11g, 802.11n and 802.11ax.
- *For 5 GHz*:
  - *5 GHz (A)* — the maximum speed is 54 Mbps;
  - *5 GHz (N)* — themode provides a maximum speed of up to 300 Mbps;
  - *5 GHz (A+N)*— the mode supports the operation of devices with 11a and 802.11n;
  - *5 GHz (AC)* — themode provides a maximum speed of up to 7 Mbps;
  - *5 GHz (N+AC)* — the mode supports operation of devices with 11n and 802.11ac;
  - *5 GHz (A+N+AC)* — the mode supports devices with 11a, 802.11n and 802.11ac;
  - *5 GHz (AX)* — themode provides a maximum speed of up to 1201 Mbps;
  - *5 GHz (A+N+AC+AX)* — the mode supports devices with 11a, 802.11n, 802.11ac and 802.11ax.

Channel Width — bandwidth of the channel on which the wireless access point operates. It takes values of 20, 40 MHz at 2.4 GHz or 20, 40, 80 MHz at 5 GHz.

Enable Automatic Channel Selection — when the flag is set, additional fields are displayed with the option to select the automatic channel detection mode:

- *Automatic Channel Selection Mode*:
  - *Compatible* — enabled from channel 1 to channel 11 for 4 GHz, from channel 36 to 64 for 5 GHz;
  - *Manual* — the user selects the channel to turn on;
  - *Full* — all available channels are enabled.

Allowed Channels — selection of channels on which the access point will operate.

Limiting the Wi-Fi Clients Number — when the flag is set, it allows one to limit the maximum number of clients connected to the access point (maximum is 64 clients).

Access Point/Client Settings

SSID — name of the wireless network used to connect to the device. The maximum length of the name is 32 characters, case-sensitive. This parameter can consist of numbers, Latin letters, spaces, and symbols “-“, “_”, “.”, “!”, “;”, “#”, but the symbols “!”, “;” , “#” and space cannot stand first.

Encrypt — selecting the wireless network security mode:

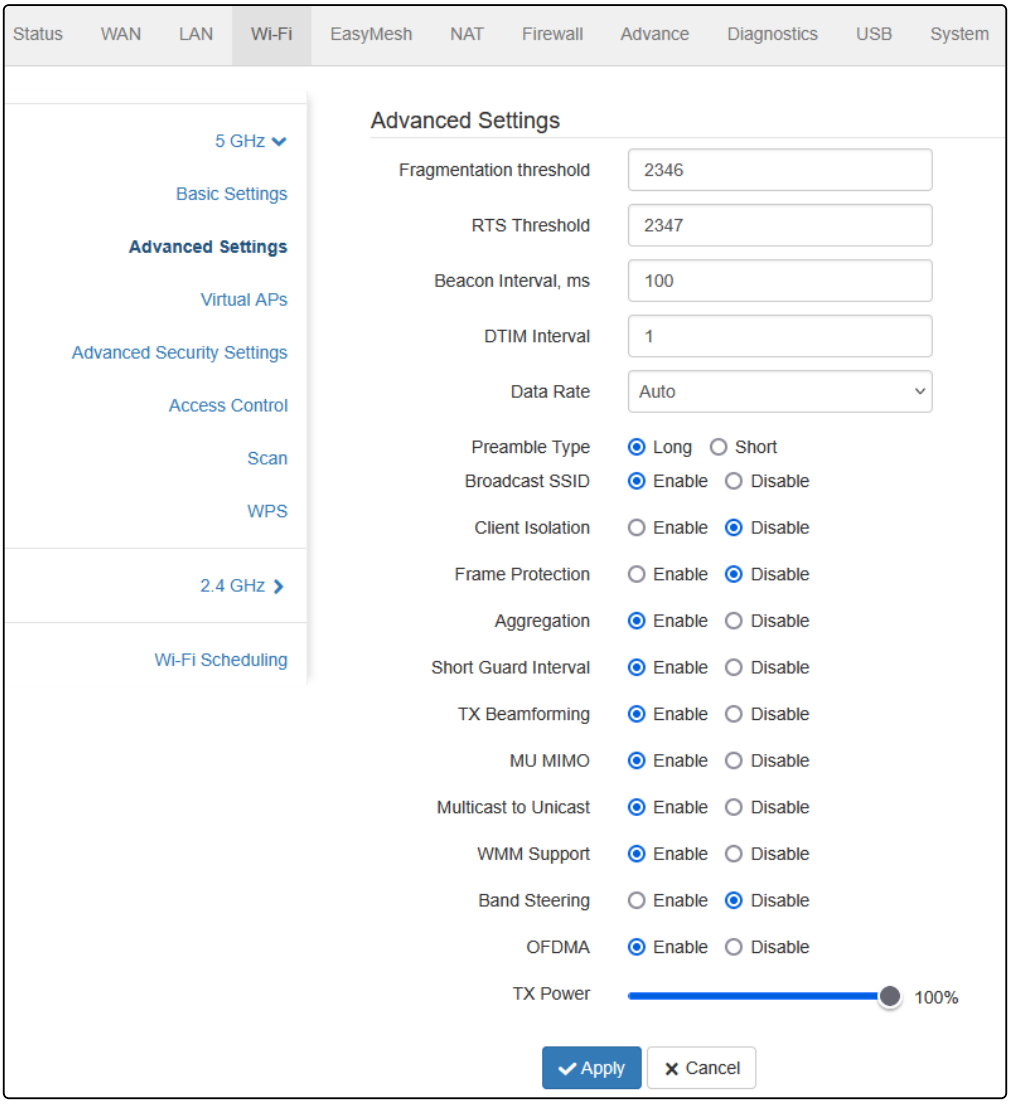
- *Disabled* — no wireless network encryption, low security level.
- *WEP* — WEP encryption. WEP Pre-Shared Key must consist of hexadecimal digits and be 10 or 26 characters long, or it must be a string (characters a-z, A-Z, 0-9, ~!@#$%^&*()_-+=) and have a length of 5 or 13 characters (by default, 26 characters HEX/13 ASCII characters, to switch to 10 HEX/5 ASCII characters, go to the Advanced mode, Wi-Fi menu → Advanced Security Settings submenu and specify the Key Length — web64, when WEP Encryption is selected);
- *WPA* — WPA encryption. The key length ranges from 8 to 63 characters. It is allowed to use only the following characters: a-z, A-Z, 0-9, ~!@#$%^&*()_-+=;:\\|/?.,<>”` or a space.

- *WPA2* — WPA2 encryption. The key length ranges from 8 to 63 characters. It is allowed to use only the following characters: a-z, A-Z, 0-9, ~!@#$%^&*()_-+=;:\\|/?.,<>”` or a space.
- *WPA/WPA2* is a mixed encryption mode that supports WPA and The key length ranges from 8 to 63 characters. It is allowed to use only the characters: a-z, A-Z, 0-9, ~!@#$%^&*()_-+=;:\\|/?.,<>”` or a space;
- *WPA3* — WPA3 encryption, has a higher level of security compared to The key length ranges from 8 to 63 characters. It is allowed to use only the following characters: a-z, A-Z, 0-9, ~!@#$%^&*()_-+=;:\\|/?.,<>”` or a space.
- *WPA2/WPA3* is a mixed encryption mode that supports WPA2 and The key length ranges from 8 to 63 characters. It is allowed to use only the characters: a-z, A-Z, 0-9, ~!@#$%^&*()_-+=;:\\|/?.,<>”` or a space.

Pre-Shared Key — the encryption key that will provide access to the network, a QR code connection is also available.

4.6.7.2 Advanced Settings submenu

This submenu contains additional settings for the Wi-Fi interface. It is not recommended to change the default settings unnecessarily.



Fragmentation threshold — the maximum size of a continuous block of data to be transmitted over a wireless network. Larger data will be split into parts — fragmented; it takes values from 256 to 2346.

RTS Threshold — the maximum requested data block size for transmission. In CSMA/CA technology, RTS (request to send) packets are sent to the base station before the real data is transmitted. If there is a free window, the database responds with a CTS (clear to send) packet, and the client sends a packet of the

requested size. The smaller the RTS size, the more likely it is to receive permission from the base station, the faster the network recovers from collisions, but the lower the overall network performance. It takes values from 0 to 2347.

Beacon Interval, ms — the time interval between service messages (beacons) in a wireless network. Service messages transmit parameters of frequencies, protocols, security, transmitter power, delays, etc. It takes values from 20 to 1024.

DTIM interval — the time interval after which buffered broadcast and multicast packets will be delivered to wireless clients.

Data Rate — allows one to set a static data transfer rate for a wireless network. Auto detection of MCS is set by default.

Preamble Type determines the length of the control block using a cyclic redundant code (CRC) used for data exchange between the router and wireless clients. If no 802.11b devices are used on the network, one can specify the Short value as the type of preamble to ensure optimal performance. The Long type of preamble is used when there are both 802.11g and 802.11b devices on the network.

Broadcast SSID — the feature disables SSID broadcasting for the access point, so client devices will not be able to detect it in the list of available wireless networks. At the same time, it remains possible to connect to clients who know the SSID and password of the wireless network.

Client Isolation — activation of a ban on the interaction of wireless clients of the main access point (AP) with each other.

Frame Protection — a special mechanism for 802.11b/g networks. Enabling the mechanism ensures that slow b-standard devices can operate in an environment with a large number of high-speed g-standard devices. This is achieved by increasing the service time for older clients, making the RTS window smaller for them, and reducing overall network performance.

Aggregation — enabling the possibility of combining several small packets for transmission in one large one.

Short Guard Interval — a mean of reducing errors when radio devices interaction — an empty space between transmitted hexadecimal characters (0, 1, ... E, F). The standard Long Guard Interval (Long GI) has a duration of 800 ns. It is assumed that during this time the signal reaches the receiver completely, taking into account all delays and reflections. After this interval expires, the next character is transmitted. The Short GI lasts 400 ns. Using Short GI increases the overall performance of a wireless network by about 11%, but sometimes leads to increased reception/transmission errors.

TX Beamforming — a technology that involves the formation of the electromagnetic field of the base station antenna in the far zone in the form of a narrowly directional main lobe oriented towards a subscriber device with the possibility of changing directional properties when changing the position of this equipment.

MU MIMO — a technology for increasing the spectral efficiency of a radio channel. This is achieved by spatial signal coding, when data reception and transmission are carried out by systems of several antennas on the same channel.

Multicast to Unicast — allows a Multicast stream to be transmitted to wireless devices as a Unicast stream.

WMM Support — provides basic QoS functions for IEEE 802.11 wireless networks, provides priority to multimedia application network packets over regular network data packets, allowing multimedia applications to run more stable.

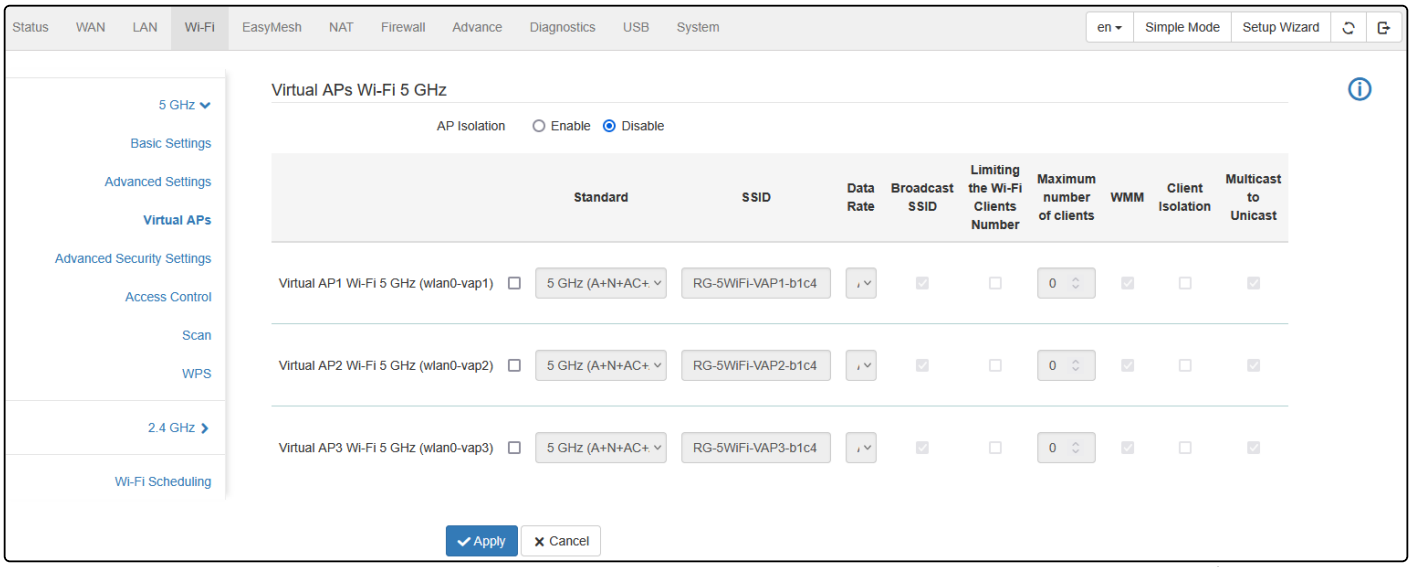
Band Steering — sets wireless network connection priorities for clients that support both Wi-Fi bands. It is usually used to switch clients from the overloaded 2.4 GHz band to the 5 GHz band.

OFDMA — a technology that allows a device to simultaneously transmit data to several clients by splitting the signal into subcarrier frequencies.

TX Power — the selection of the power value of the Wi-Fi module.

4.6.7.3 Virtual APs submenu

This submenu configures the settings for wireless virtual access points. The "Advanced Security Settings" submenu provides security settings for wireless virtual access points.



AP Isolation — enabling the ban of interaction of one Virtual AP clients with another AP clients (main and virtual).

When a "Virtual AP" is activated, the configuration of its parameters becomes available:

Standard — selection of the operating mode for the wireless interface in accordance with the Wi-Fi 802.11 series of standards.

SSID — selection of the name of the wireless network used to connect to the device.

Data Rate — setting of a static value for the data transfer rate.

Broadcast SSID — a feature for disabling SSID broadcasting for the access point.

Limiting the Wi-Fi Clients Number — a feature for enabling the limitation of Wi-Fi clients number.

> *Maximum number of clients* — setting the maximum number of clients when the Limiting feature is enabled.

WMM — a feature for providing basic QoS functions for IEEE 802.11 wireless networks.

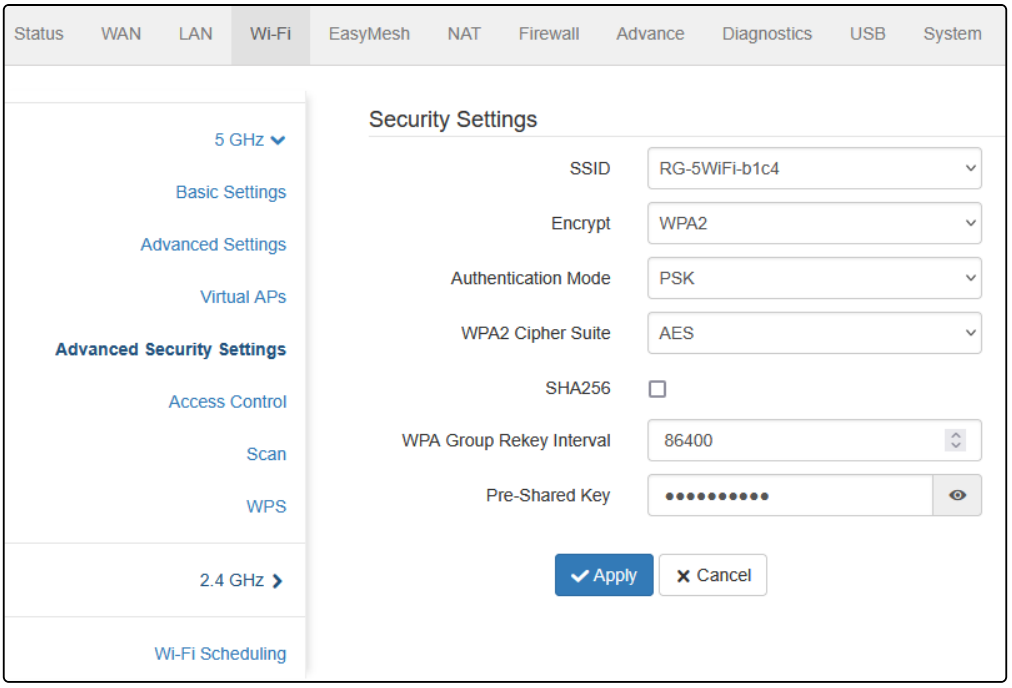
Client Isolation — enabling the ban on the interaction of wireless clients of one Virtual AP with each other.

Multicast to Unicast — a feature that implements Multicast stream transmission to wireless devices in the form of Unicast.

> ⚠ **When adding a new virtual network, it must be added to the existing WAN connection.**

4.6.7.4 Advanced Security Settings submenu

This submenu duplicates the SSID, encryption, and network key settings, and contains advanced settings such as authentication mode and rekey interval. Here one can configure the security settings for virtual access points. To do this, open the drop-down list in the SSID field and select the desired access point.



Security Settings

SSID — selection of the necessary access point for security settings.

Encrypt — selecting the wireless network security mode:

- *Disabled* — no wireless network encryption, low security level.
- *WEP* — WEP encryption. The WEP key must consist of hexadecimal digits and be 10 or 26 characters long, or it must be a string (characters a-z, A-Z, 0-9, ~!@#$%^&*()_-+=) and have a length of 5 or 13 characters (by default, 26 HEX characters / 13 ASCII characters. For switching for 10 HEX characters / 5 ASCII characters, go to the "Advanced Security Settings" submenu and specify the key length — web64, when choosing Encrypt — WEP);
- *WPA* — WPA encryption. The key length ranges from 8 to 63 characters. It is allowed to use only the following characters: a-z, A-Z, 0-9, ~!@#$%^&*()_-+=;:\\|/?.,<>"` or a space.
- *WPA2* — WPA2 encryption. The key length ranges from 8 to 63 characters. It is allowed to use only the following characters: a-z, A-Z, 0-9, ~!@#$%^&*()_-+=;:\\|/?.,<>"` or a space.
- *WPA/WPA2* is a mixed encryption mode that supports WPA and The key length ranges from 8 to 63 characters. It is allowed to use only the characters: a-z, A-Z, 0-9, ~!@#$%^&*()_-+=;:\\|/?.,<>"` or a space;
- *WPA3* — WPA3 encryption, has a higher level of security compared to The key length ranges from 8 to 63 characters. It is allowed to use only the following characters: a-z, A-Z, 0-9, ~!@#$%^&*()_-+=;:\\|/?.,<>"` or a space.
- *WPA2/WPA3* is a mixed encryption mode that supports WPA2 and The key length ranges from 8 to 63 characters. It is allowed to use only the characters: a-z, A-Z, 0-9, ~!@#$%^&*()_-+=;:\\|/?.,<>"` or a space.

The WPA2/WPA3 encryption types have a much higher level of protection compared to WEP.

Encrypt (Disabled):

802.1x Authentication — enabling the 802.1x standard (allows users to authenticate using the RADIUS authentication server).

Encryption (WEP):

802.1x Authentication — enabling the 802.1x standard (allows users to authenticate using the RADIUS authentication server, using a WEP key to encrypt data);

Authentication — selecting the authentication mode:

- *Open System* — without authentication;
- *Shared Key* — authentication using the provided key;
- *Auto* — automatic authentication.

Key Length — selection of the keys 64 or 128 bits long (wep64, wep128);

Key format — selection of the key format (ASCII, HEX);

Encryption Key — the encryption key that will provide access to the network.

Encrypt (WPA, WPA2, WPA/WPA2):

Authentication Mode — selection of the authentication method when connecting the device:

- *Enterprise* — a protocol designed to provide centralized authentication, authorization, and user accounting through a RADIUS server;
- *PSK* — authentication using a shared network password.

WPA, WPA2 Cipher Suite — a set of WPA, TKIP, or AES ciphers;

SHA256 — a secure hashing algorithm;

WPA Group Rekey Interval — time in seconds between changing the WPA/WPA2 encryption keys;

Pre-Shared Key — the encryption key that will provide access to the network

⚠ **When setting WPA/WPA2, the default encryption type is TKIP/AES.**

Encrypt (WPA3, WPA2/WPA3):

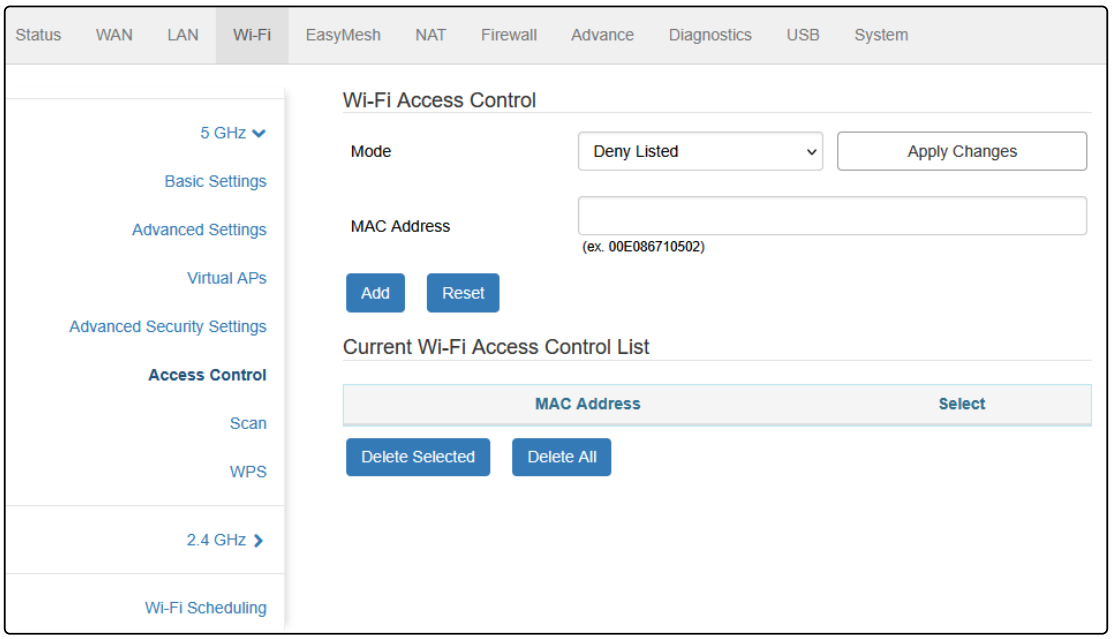
WPA Group Rekey Interval — time in seconds between changing the WPA/WPA2 encryption keys;

Pre-Shared Key — the encryption key that will provide access to the network.

⚠ **When setting WPA3 or WPA2/WPA3, the default encryption type is AES.**

4.6.7.5 Access Control submenu

In the "Access Control" submenu, access filtering by Wi-Fi and the client's MAC address is configured.



Mode — selection of one of three modes of operation with wireless devices:

- *Disabled* — there are no limitations on connecting devices;
- *Allowed Listed* — only devices with MAC addresses from the list can connect to the Wi-Fi;
- *Deny Listed* — all devices can connect to the Wi-Fi network, except those from the list.

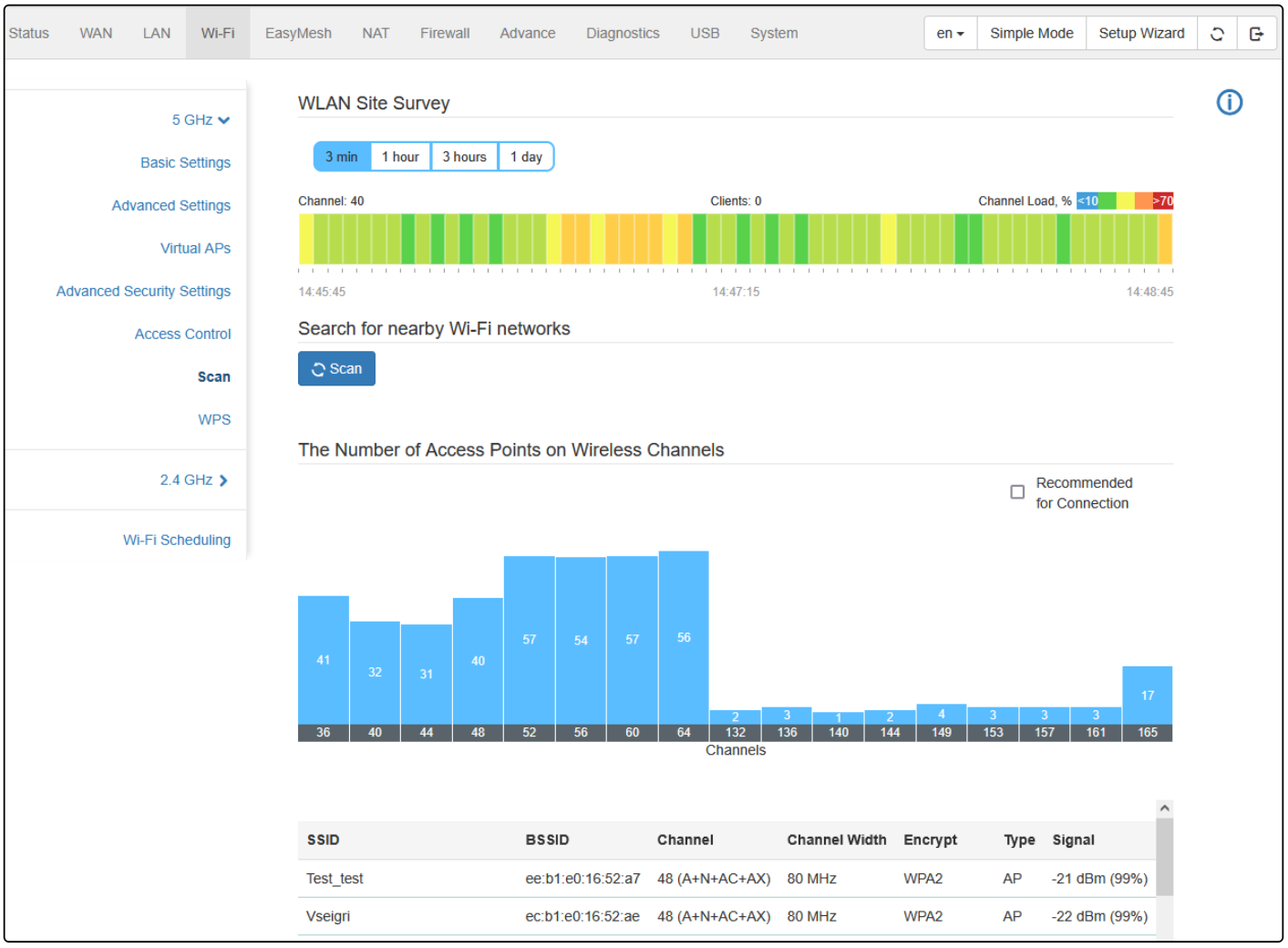
MAC Address — the input field for the MAC address of the device. The address is entered in solid text, for example: a8f94b214fa0.

Current Wi-Fi Access Control List

The table shows the current list of Wi-Fi access controls.

4.6.7.6 Scan submenu

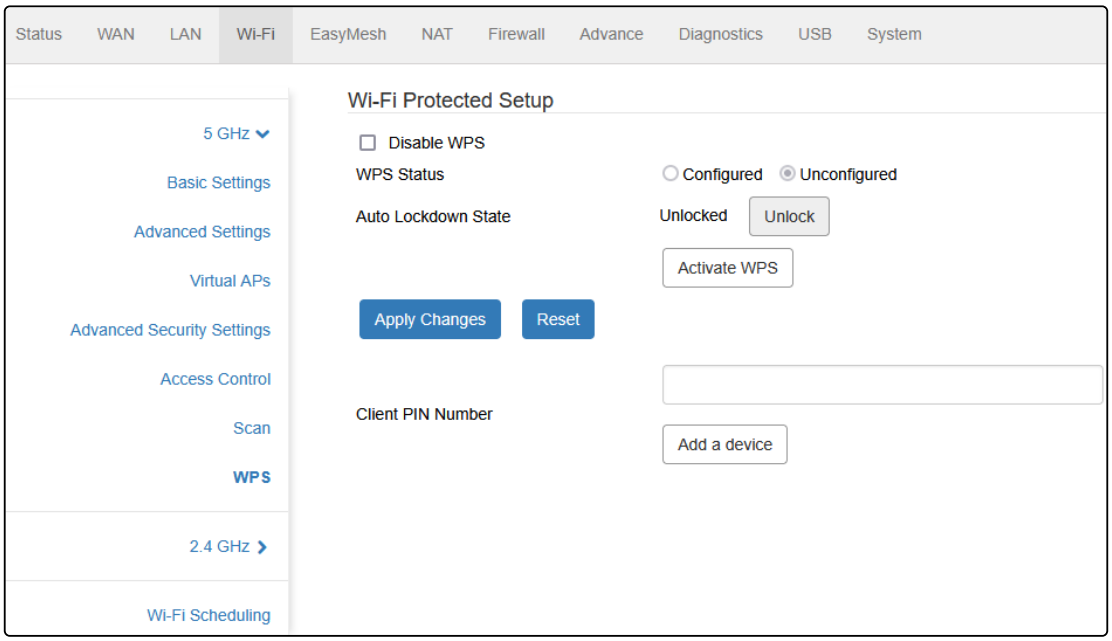
In the submenu, one can search for other Wi-Fi networks in a given frequency range in order to determine the minimum loaded channel when fine-tuning the network.



4.6.7.7 WPS submenu

In the "WPS" submenu, the WPS protocol (Wi-Fi Protected Setup) is configured.

WPS is a standard for semi-automatic creation of a wireless Wi-Fi network. The purpose of the WPS protocol is to simplify the process of setting up a wireless network. WPS automatically designates the network name and sets encryption to protect against unauthorized access to the network, without having to manually set all the parameters.



The WPS function can be used separately for each frequency range.

Depending on the access point status, some WPS functions may be disabled.

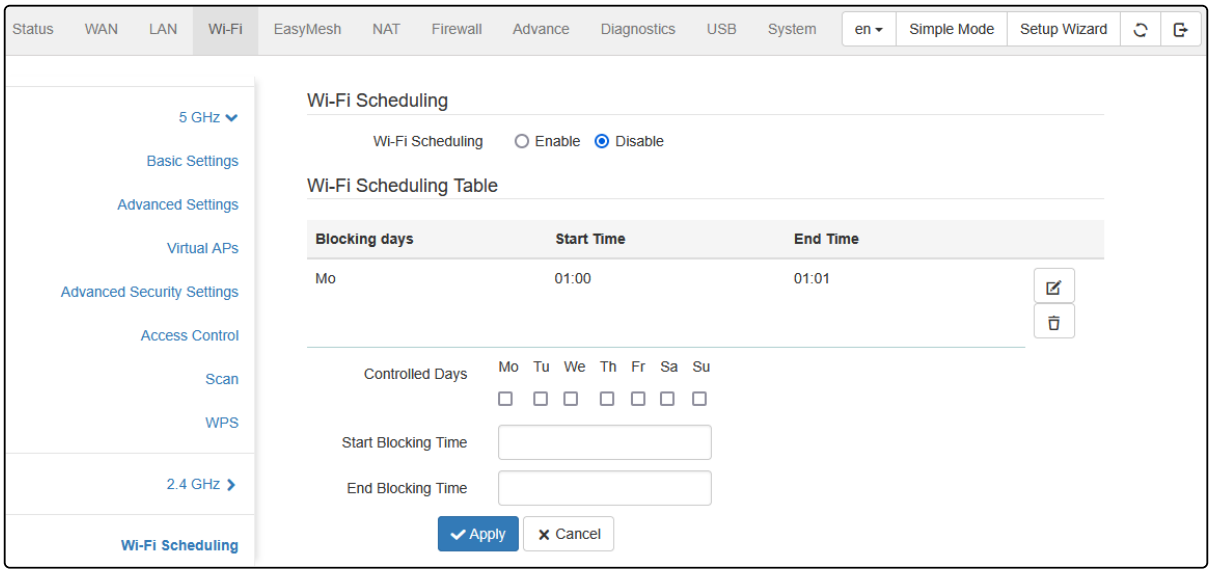
Disable WPS — when the flag is set, the WPS function will be disabled on the selected range;

"Activate WPS" button — performs the functions of the WPS button on the device body. The client is connected automatically after clicking this button. After clicking the button, the WPS function is active for two minutes;

Client PIN Number — input field of the code generated on the client's side for connection via WPS.

4.6.7.8 Wi-Fi Scheduling submenu

In the "Wi-Fi Scheduling" submenu, it is possible to set specific days and time intervals on which Wi-Fi will operate in access point mode.



Wi-Fi Scheduling — when the feature is enabled, the Wi-Fi network is blocked according to the schedule.

Click the "+" button to set the Wi-Fi Scheduling Table.

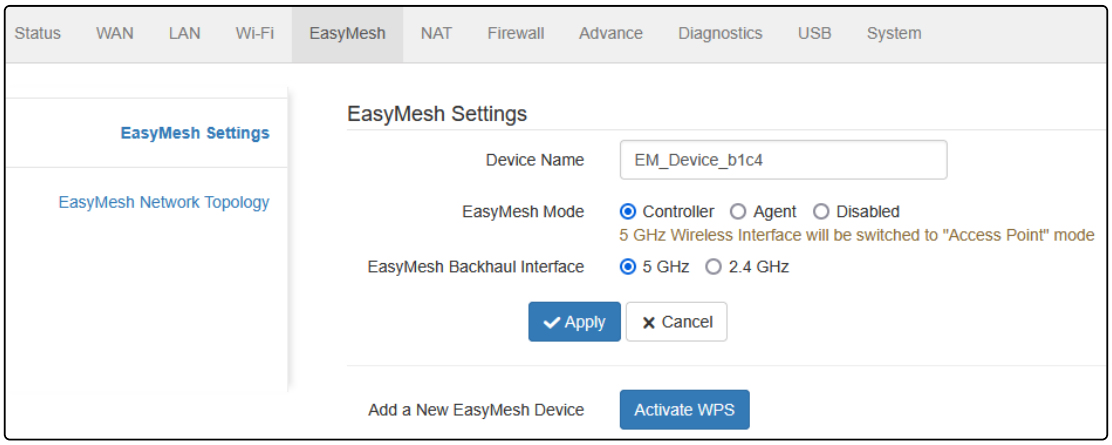
Controlled Days — select the week days when the Wi-Fi network is blocked;

Start Blocking Time — the start time of the Wi-Fi network blocking;

End Blocking Time — the end time of the Wi-Fi network blocking.

4.6.8 EasyMesh menu

4.6.8.1 EasyMesh Settings submenu



Device Name — the input field for changing the device name.

EasyMesh Mode — the router supports EasyMesh technology and can participate in the creation of a wireless, scalable network in one of two roles:

- *Controller* — the root EasyMesh device to which EasyMesh agents can be connected to expand the Wi-Fi network. The controller manages the entire network, makes a decision on switching a Wi-Fi client to the required access point, and also synchronizes interface parameters from the root device to the entire network. In this mode, the entire network topology can be displayed on the "EasyMesh Network Topology" The controller connects to the provider's network and is a gateway;
- *Agent* — switches the device to agent mode, which is necessary to connect to the controller and expand the existing Wi-Fi network;
- *Disabled* — disables EasyMesh mode.

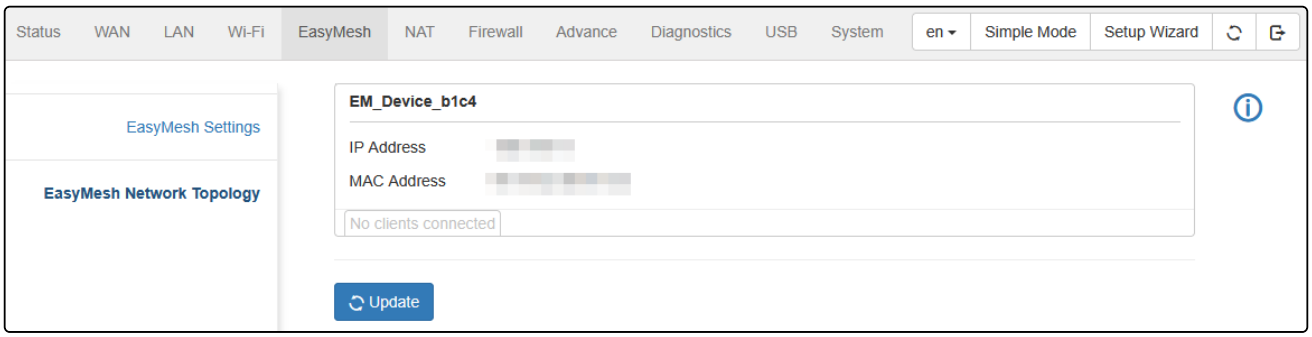
The EasyMesh Backhaul Interface — a wireless interface that EasyMesh agents connect to.

"Activate WPS" button — performs the functions of the WPS button on the device body. The client is connected automatically after clicking this button. After clicking the button, the WPS function is active for two minutes.

In a configured device, pressing the WPS button for more than 5 seconds automatically switches the device to controller mode and activates the procedure for adding an EasyMesh agent.
If the router has default settings, then pressing the WPS button for more than 5 seconds activates the agent mode to add to the controller. After adding, the agent shows the signal strength (RSSI) to the controller with LAN LEDs:
1 LAN LED — below -70 dBm (weak, unacceptable signal);
2 LAN LEDs — from -60 to -70 dBm (sufficient signal);
3 LAN LEDs — from -50 to -60 dBm (good signal);
4 LAN LEDs — above -50 dBm (excellent signal).

4.6.8.2 EasyMesh Network Topology submenu

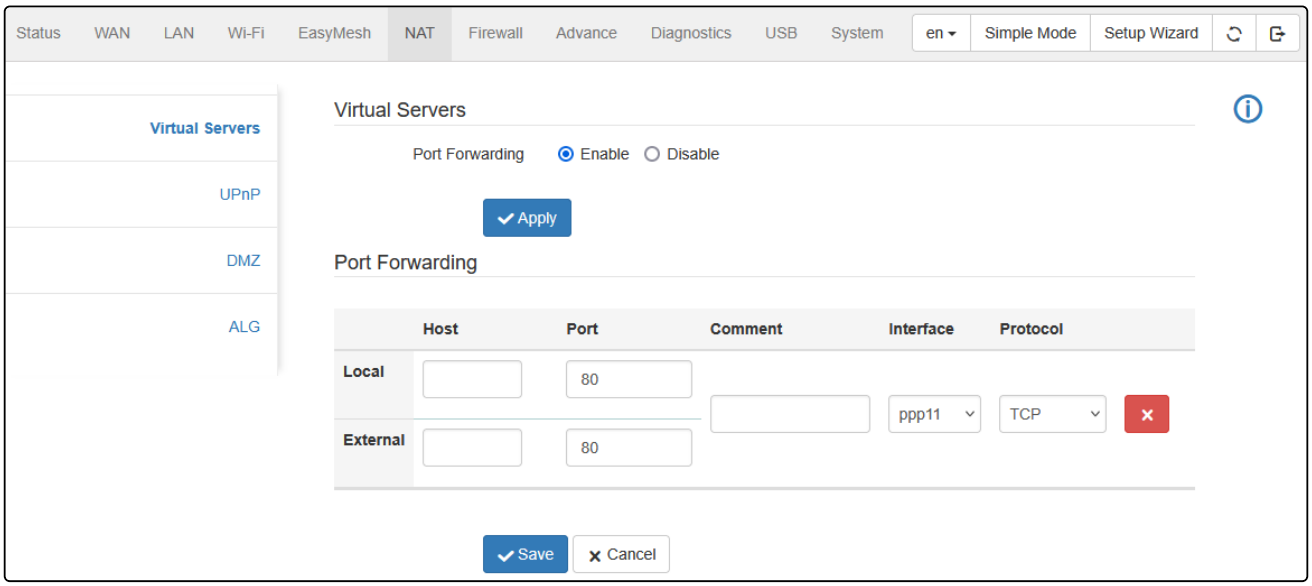
Information about EasyMesh network is available in this submenu.



4.6.9 NAT menu

4.6.9.1 Virtual Servers submenu

Network port forwarding is necessary when a TCP/UDP connection to a local (LAN-connected) computer is established from an external network. This submenu sets rules that allow packets to pass from the external network to the specified address on the local network, thereby making it possible to establish a connection. Port forwarding is mainly necessary when using Torrent and P2P services. In the settings of the Torrent or P2P client, look at the TCP/UDP ports used by it and set the appropriate forwarding rules for these ports to one's computer IP address.



Port Forwarding

Local Host — source IP address;

Local Port — range of ports to be forwarded from the LAN side;

External Host — destination IP address;

External Port — range of ports on the WAN side, it may match or differ from the port number on the LAN side;

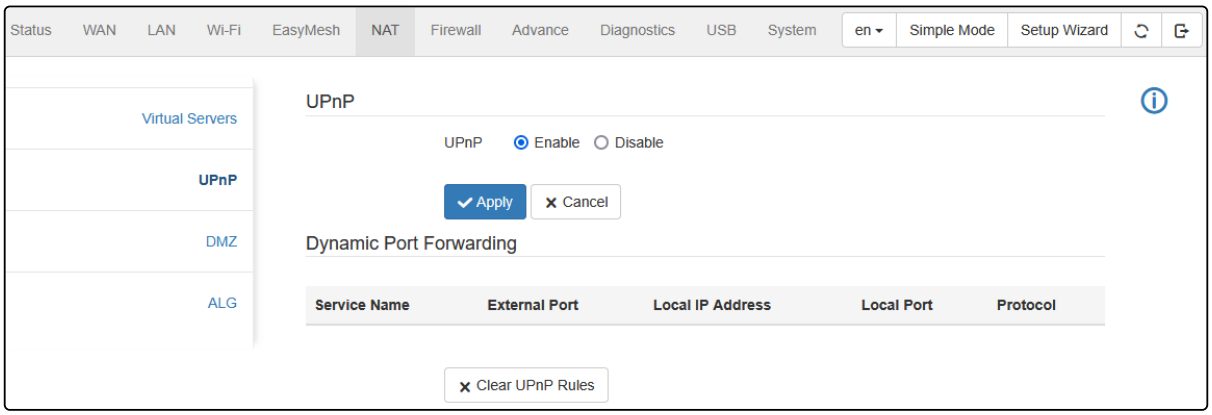
Comment — an input field for notes;

Interface — selection of the WAN interface for which the forwarding rule is added;

Protocol — selection of the type of traffic protocol TCP, UDP or TCP+UDP.

4.6.9.2 UPnP submenu

UPnP is a technology for automatic port forwarding over SSDP and HTTP protocols.

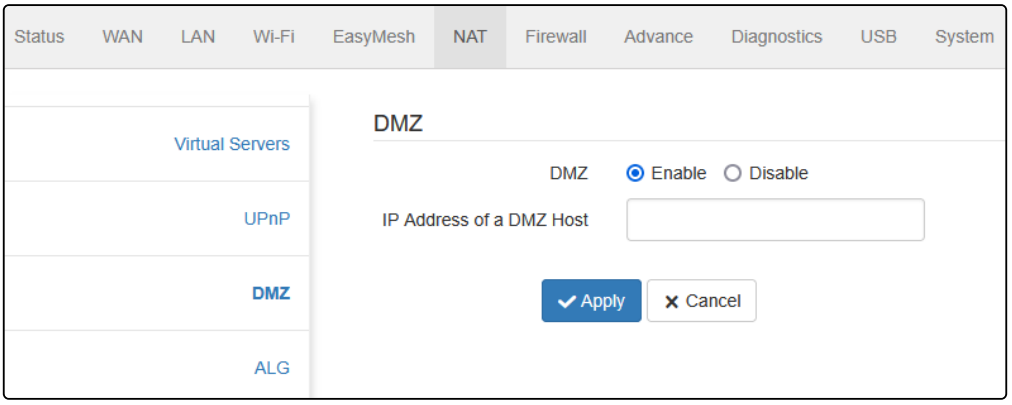


Dynamic Port Forwarding

"Clear UPnP Rules" button — clear the current list of UPnP rules.

4.6.9.3 DMZ submenu

Demilitarized zone (DMZ) allows allocating one client to LAN so that all incoming packets on the router WAN are redirected to this client. A DMZ host usually contains services such as an HTTP/HTTPS server, an FTP server, a DNS server, and others.



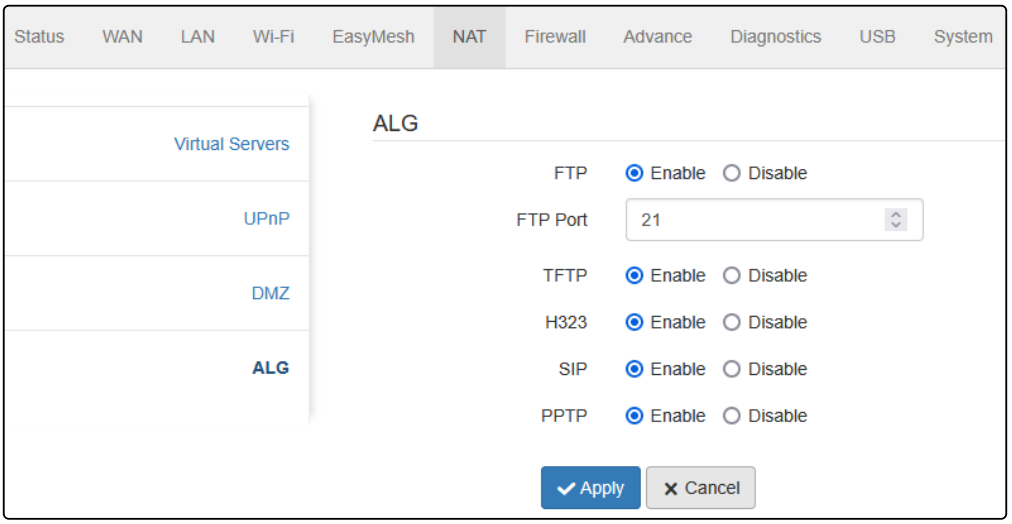
DMZ — when the flag is set, DMZ is enabled;

IP Address of a DMZ Host — IP address of the client in the LAN network that needs to be moved to the DMZ zone.

> ⚠ **If the DMZ is used together with remote access rules or port forwarding rules, the DMZ will have a lower priority.**

4.6.9.4 ALG submenu

The Application Layer Gateway (ALG) is responsible for modifying the application part of the packets for the correct operation of protocols via NAT.



FTP — enables and disables ALG for the FTP protocol;

FTP Port — the port used by the LAN client for the FTP protocol;

TFTP — enables and disables ALG for the TFTP protocol;

H323 — enables and disables ALG for the H.323 standard;

SIP — enables and disables ALG for the SIP protocol;

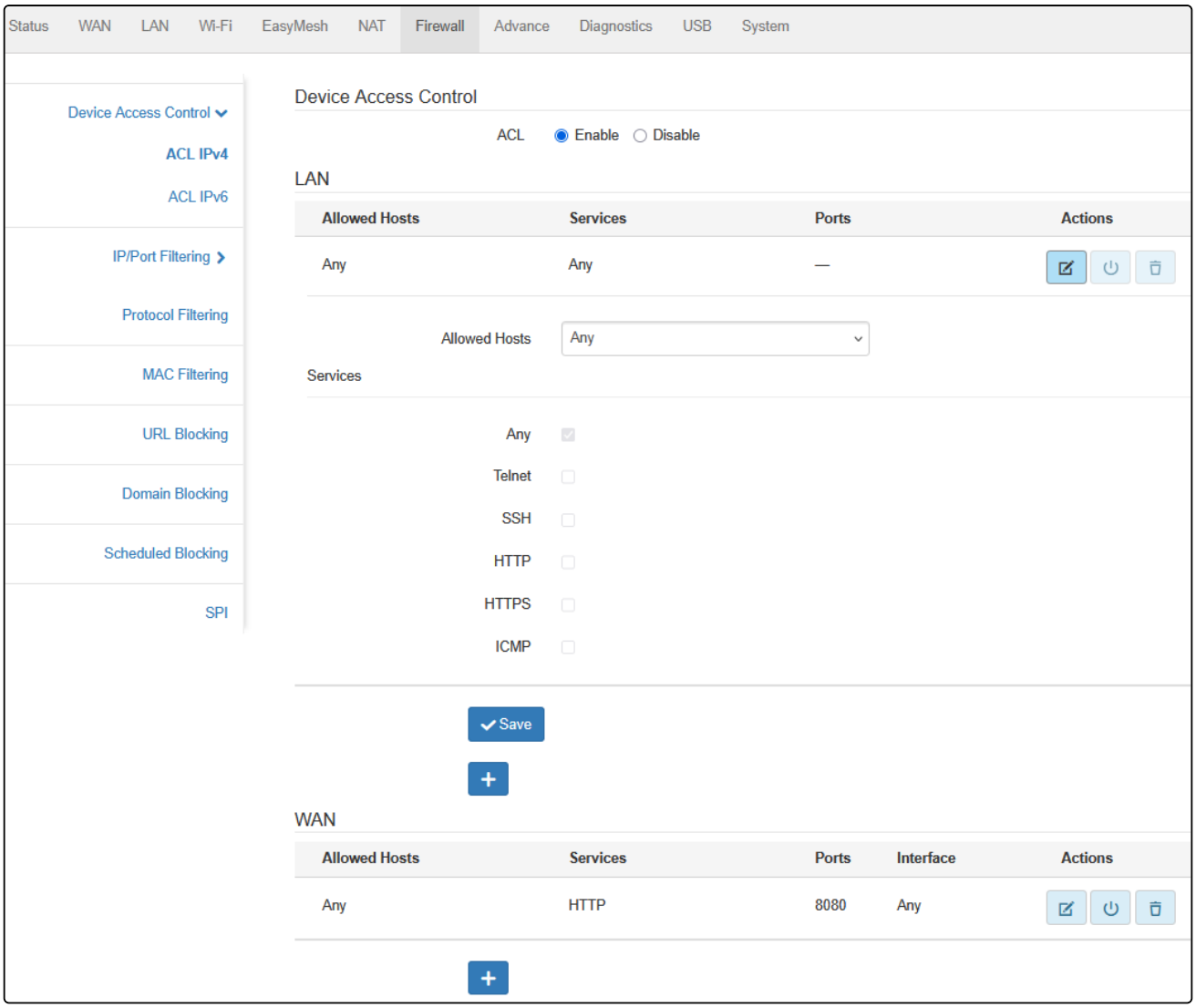
PPTP — enables and disables ALG for the PPTP protocol.

4.6.10 Firewall menu

4.6.10.1 Device Access Control. ACL IPv4 submenu

The "ACL IPv4" submenu configures access to the device over the IPv4 protocol.

Access control can be configured from both the WAN and LAN sides.



ACL — enables and disables access control feature.

LAN

Allowed Hosts — configuring hosts that will be allowed access to the device:

- *IP Address* — restriction of access to the device by IP address:
  - *IP Range* — configuring access by IP address range:
    - *Start IP Address/End IP Address*— fields for assigning the initial and final IP addresses in the range.
  - *Subnet* — configuring access by choosing a subnet:
    - *Network Address* — network address.
    - *Subnet Mask* — selection of the subnet mask.
- *MAC Address* — restriction of access to the device by MAC address:
  - *MAC Address* — physical address.
- *Any* — unlimited access settings.

Services — configuring services that will allow access to the device. Access can be configured using ICMP, Telnet, or HTTP protocols. Unlimited access settings are possible.

For Telnet and SSH to work, it is needed to enable them on the System menu → Telnet submenu. After that Telnet and SSH will be available in the service selection list.

WAN

Allowed Hosts — configuring hosts that will be allowed access to the device:

- *IP Address* — restriction of access to the device by IP address:
  - *IP Range* — configuring access by IP address range:
    - *Start IP Address/End IP Address*— fields for assigning the initial and final IP addresses in the range.
  - *Subnet* — configuring access by choosing a subnet:
    - *Network Address* — network address.
    - *Subnet Mask* — selection of the subnet mask.
- *Any* — unlimited access settings.

Interface — selection of interface when configuring WAN access;

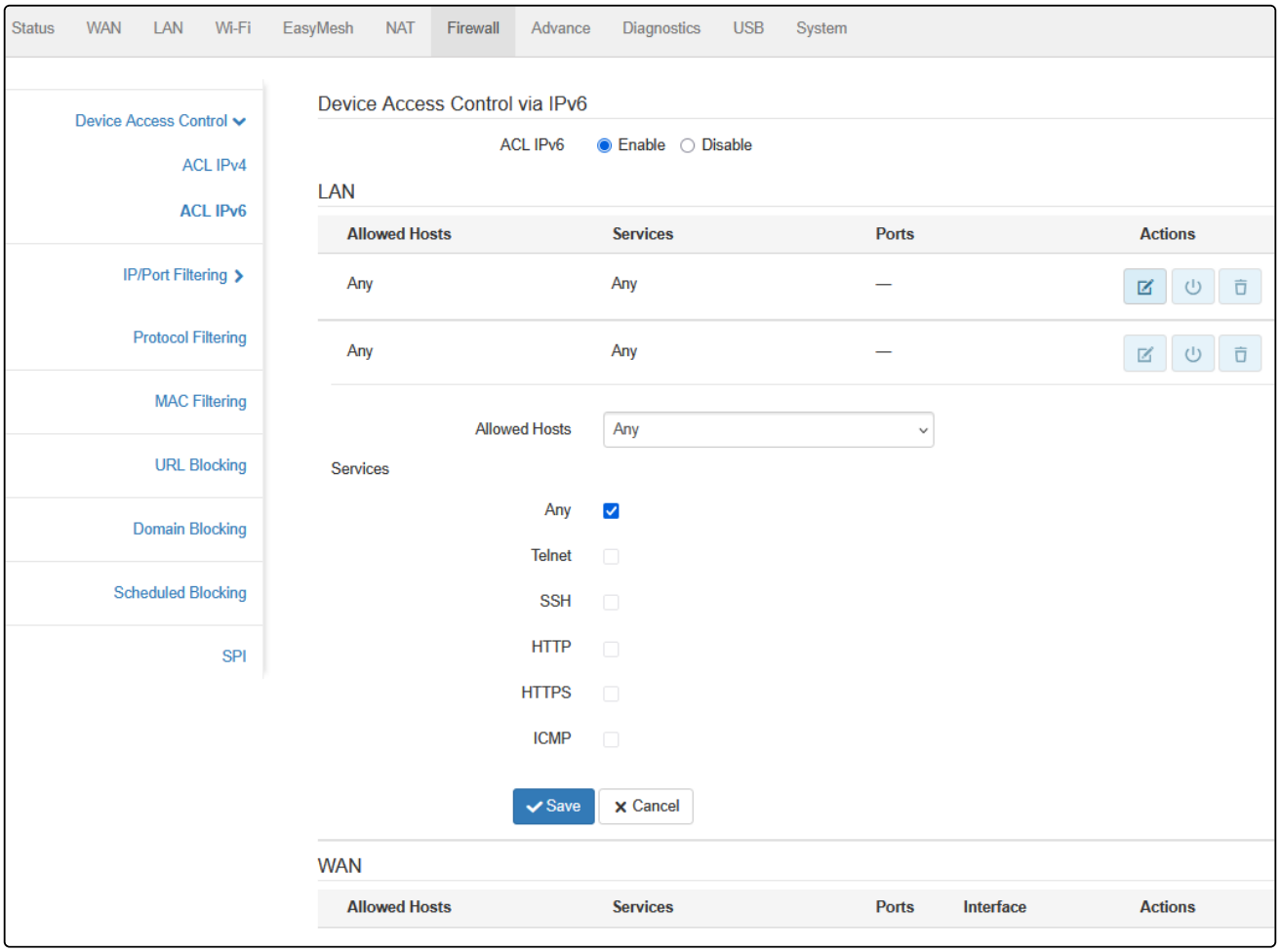
Services — configuring services that will allow access to the device. Access can be configured using ICMP, Telnet, or HTTP protocols.

For Telnet and SSH to work, it is needed to enable them on the System menu → Telnet submenu. After that Telnet and SSH will be available in the service selection list.

4.6.10.2 ACL IPv6 submenu

The "IPv6 ACL" submenu allows one to configure access to the device over the IPv6 protocol.

Access control can be configured from both the WAN and LAN sides.



ACL IPv6 — enabling device access control feature.

LAN

Allowed Hosts — configuring hosts that will be allowed access to the device:

- *IP Address* — restriction of access to the device by IP address:
  - *Network Address* — prefix of the external subnet.
  - *Ipv6 Address Prefix Length* — external subnet prefix.
- *Any — unlimited access settings.*

Services — configuring services that will allow access to the device. Access can be configured using Telnet, SSH, HTTP, HTTPS, and ICMP protocols. Unlimited access settings are possible.

For Telnet and SSH to work, it is needed to enable them on the System menu → Telnet submenu. After that Telnet and SSH will be available in the service selection list.

WAN

Allowed Hosts — configuring hosts that will be allowed access to the device:

- *IP Address* — restriction of access to the device by IP address:
  - *Network Address* — prefix of the external subnet.
  - *Ipv6 Address Prefix Length* — external subnet prefix.
- *Any* — unlimited access settings.

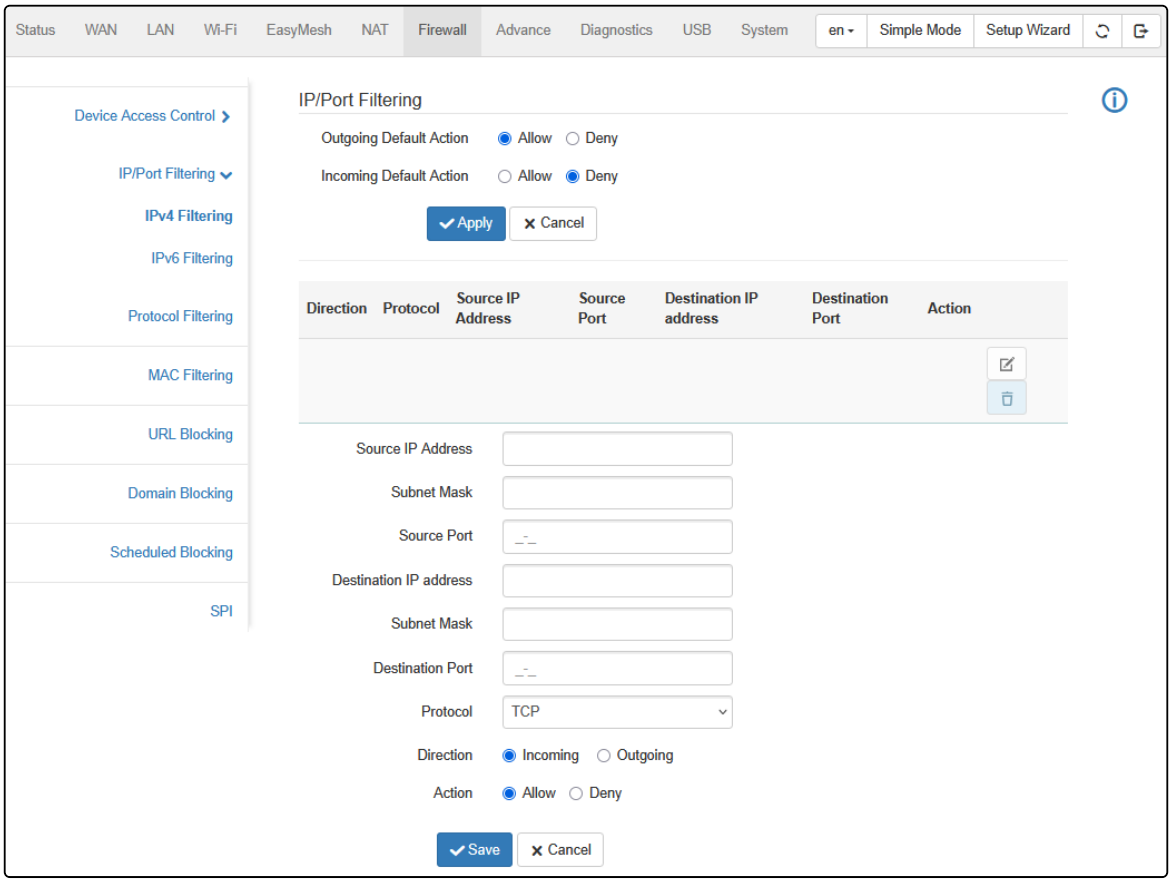
Interface — selection of interface when configuring WAN access.

Services — configuring services that will allow access to the device. Access can be configured using Telnet, SSH, HTTP, HTTPS, and ICMP protocols.

For Telnet and SSH to work, it is needed to enable them on the System menu → Telnet submenu. After that Telnet and SSH will be available in the service selection list.

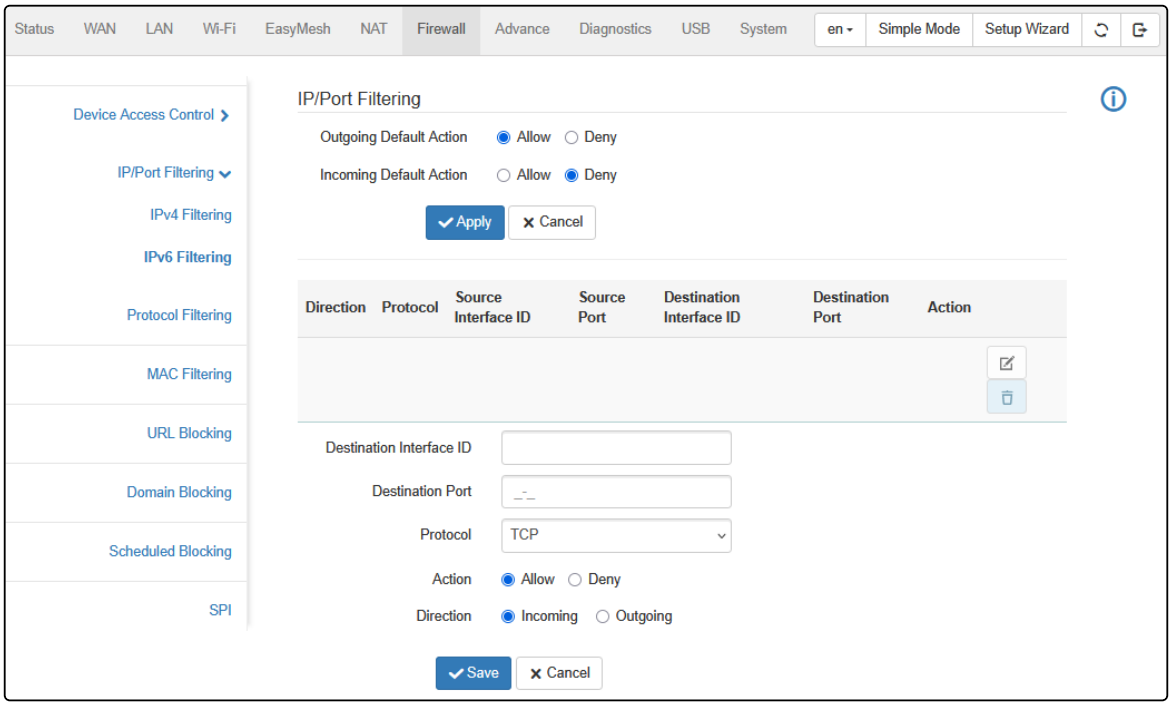
4.6.10.3 IP/Port Filtering. IPv4 Filtering submenu

The feature allows one to restrict access to certain devices by IP address and TCP/UDP port. One can set up a default policy for incoming and outgoing packets, as well as create specific rules.



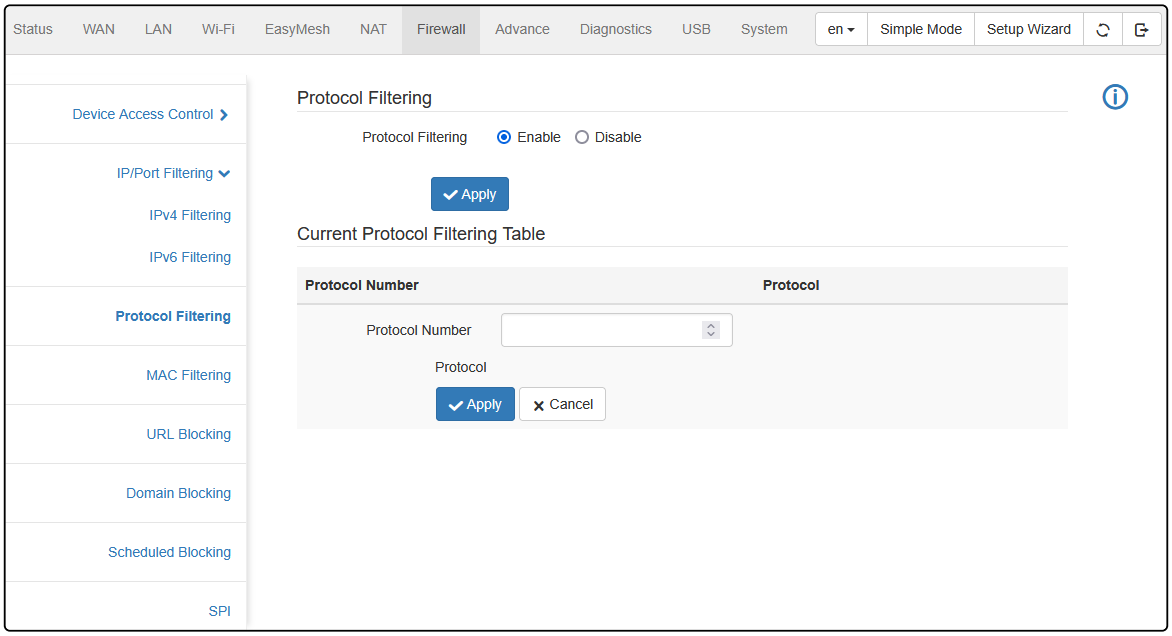
4.6.10.4 IPv6 Filtering submenu

The feature allows one to restrict access to certain devices by interface ID and TCP/UDP port. One can set up a default policy for incoming and outgoing packets, as well as create specific rules.



4.6.10.5 Protocol Filtering submenu

In the "Protocol Filtering" submenu, access restrictions for a specific protocol are configured.



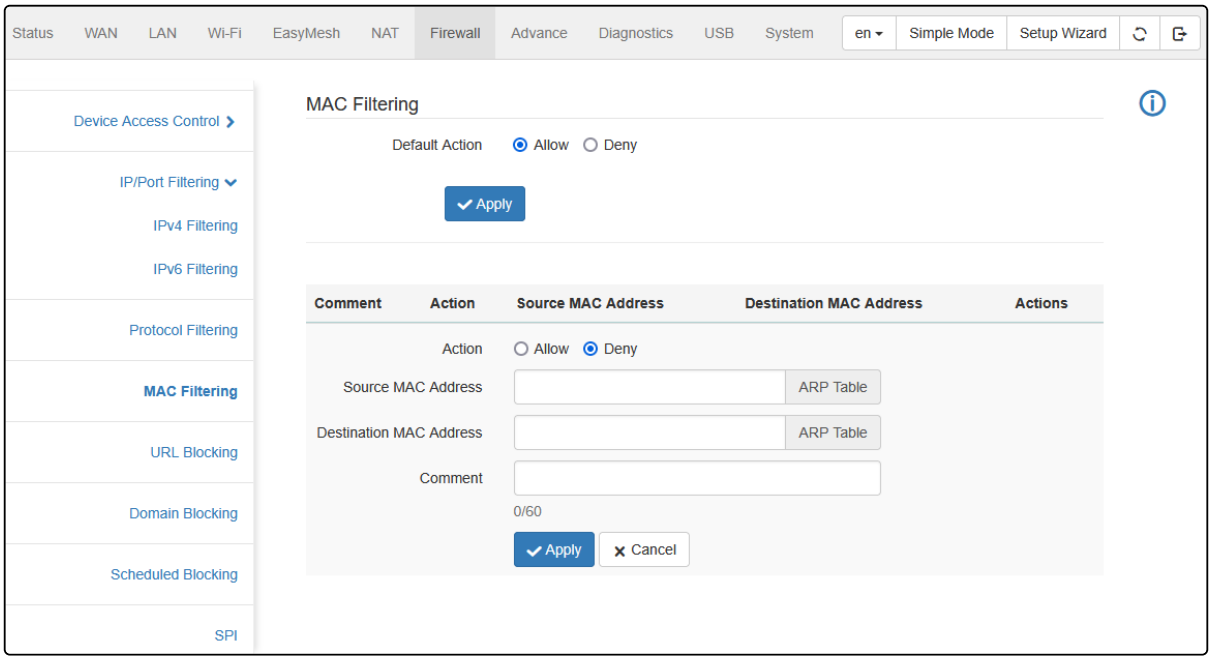
Protocol Filtering — enables or disables filtering.

Protocol Number — specified in the "Protocol" field of the IPv4 packet header or in the "Next header" field of the IPv6 packet.

Protocol — the name of the protocol corresponding to the entered protocol number.

4.6.10.6 MAC Filtering submenu

In the "MAC Filtering" submenu, access filtering is configured by the MAC address of clients in the local subnet. One can set up a default policy for incoming and outgoing packets, as well as create specific rules.



Default Action — set up a policy for incoming and outgoing packets by default.

Action — selecting a destination for the condition being created, deny or allow access.

Source MAC Address — MAC address of the source for setting up the rule.

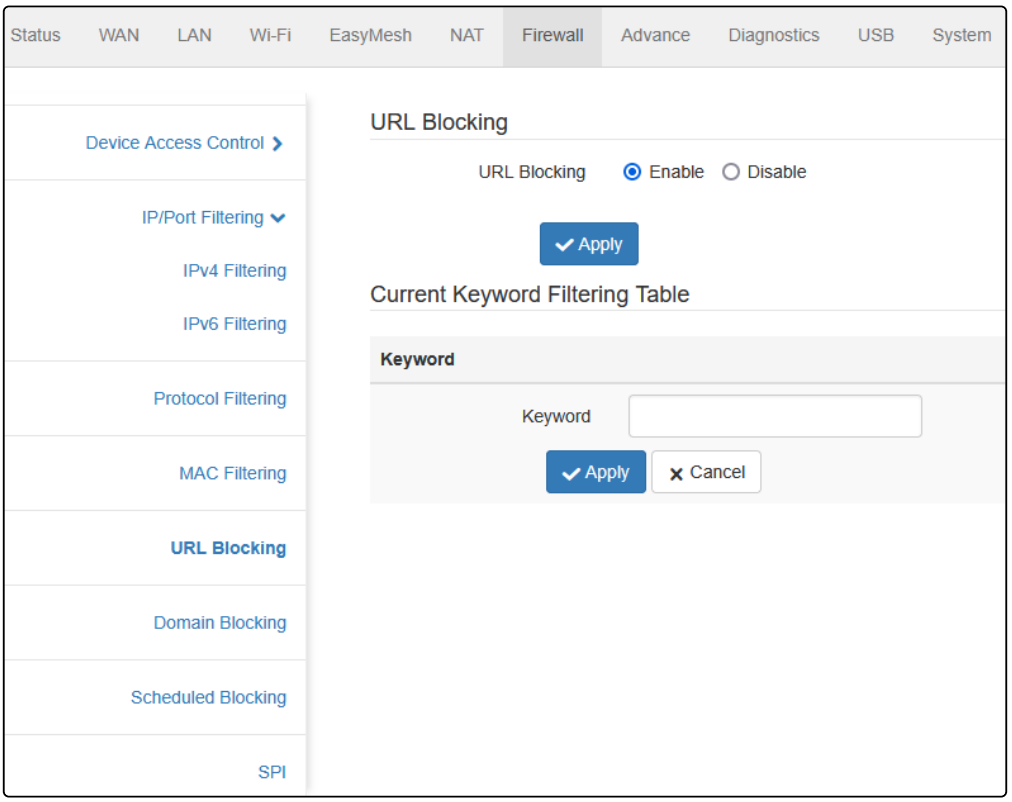
Destination MAC Address — MAC address of the destination for setting up the rule.

ARP Table — displays IP addresses and MAC addresses of network devices.

Comment — an input field for notes to filters.

4.6.10.7 URL Blocking submenu

The URL filter allows one to restrict access to resources on the Internet by their domain addresses (URL).



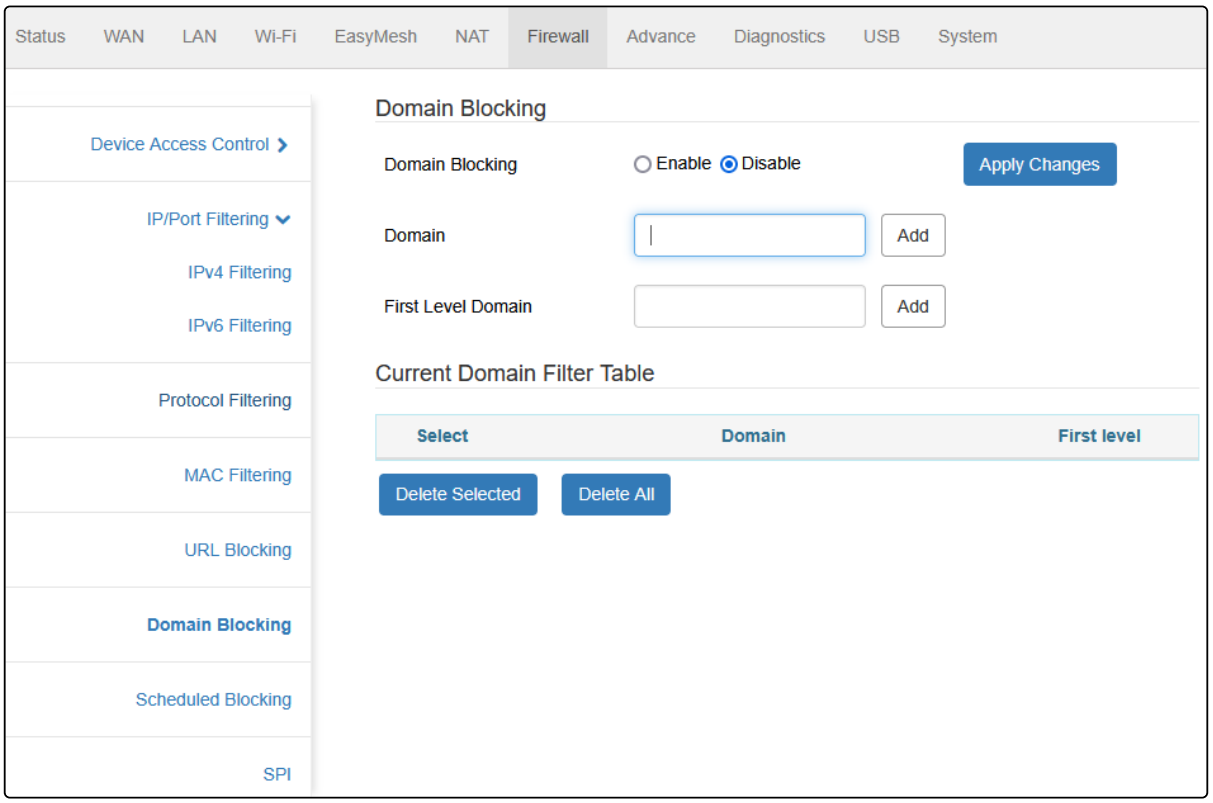
URL Blocking — enables or disables URL blocking.

Keyword — URL of the resource that one wants to block access to.

> ⚠ **URL filtering does not work for HTTPS and other protocols that use TLS or SSL encryption**.

4.6.10.8 Domain Blocking submenu

The domain filter allows one to restrict access to resources on the Internet by a specific domain.



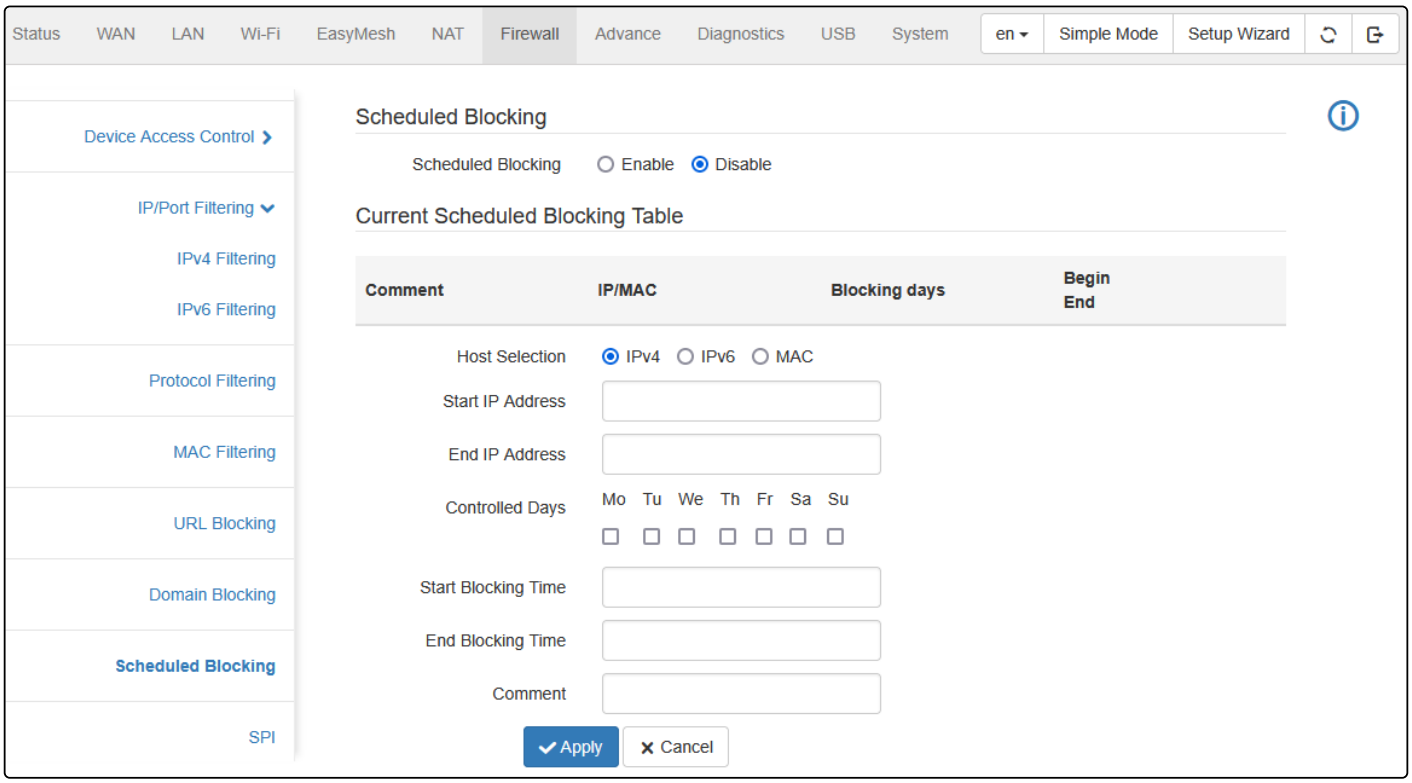
Domain Blocking — enables or disables domain blocking.

Domain — an arbitrary domain that one wants to block access to (by entering example, access to all resources containing this word will be blocked, for example, to the resource www.example.com). In the input field, it is possible to combine multiple domains to block a resource more accurately (input www.example will block access to www.example.com and www.example.su, but will not block access to example.com).

First Level Domain — the top-level domain that one wants to block access to (for example, by entering com, access to all resources ending in this domain will be blocked, for example, to the resource www.example.com , but access to the resource com.example.su will not be blocked). In the input field, it is possible to combine multiple domains to block a resource more accurately (input example.com will block access to example.com and www.example.com but will not block access to example.com.org).

4.6.10.9 Scheduled Blocking submenu

A scheduled filter allows one to restrict access to resources on the Internet by specific time and days.



Scheduled Blocking — enables or disables scheduled domain blocking.

Host Selection — selection of the necessary parameters for blocking (IPv4, IPv6, MAC).

Start IP Address — selection of the initial IP address for the blocking range.

End IP address — selection of the initial IP address for the blocking range.

Controlled Days — selection of week days for blocking.

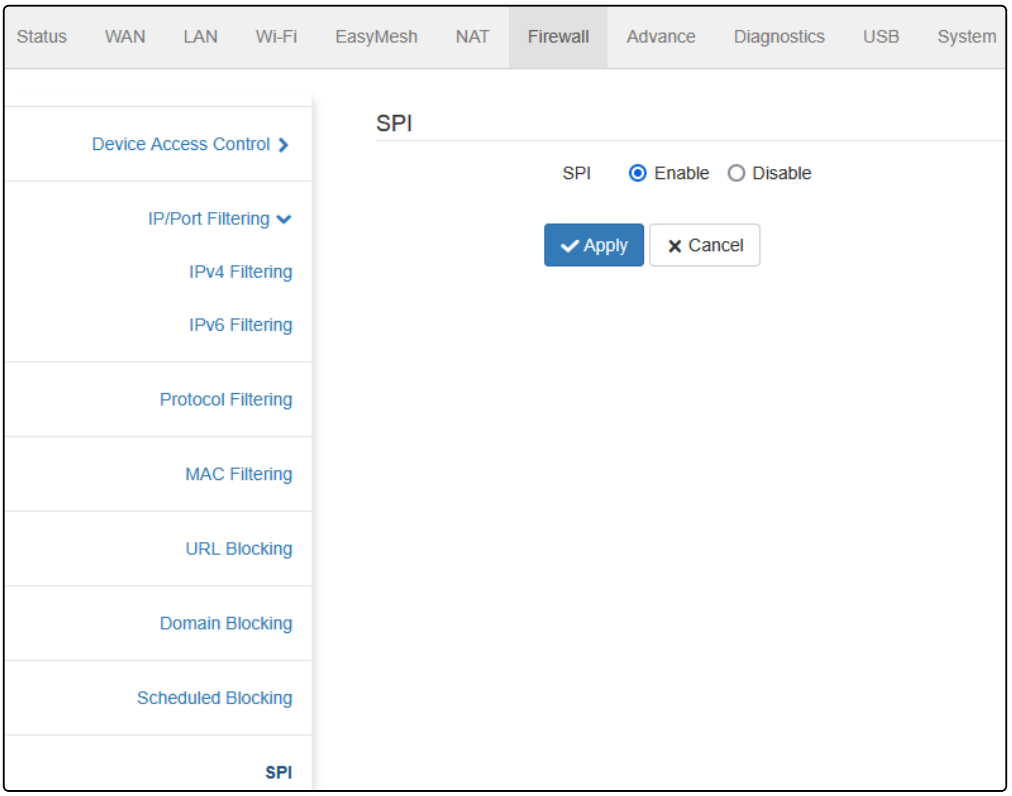
Start Blocking Time — the blocking start time in the hh:mm format.

End Blocking Time — the blocking end time in the hh:mm format.

Comment — a comment field.

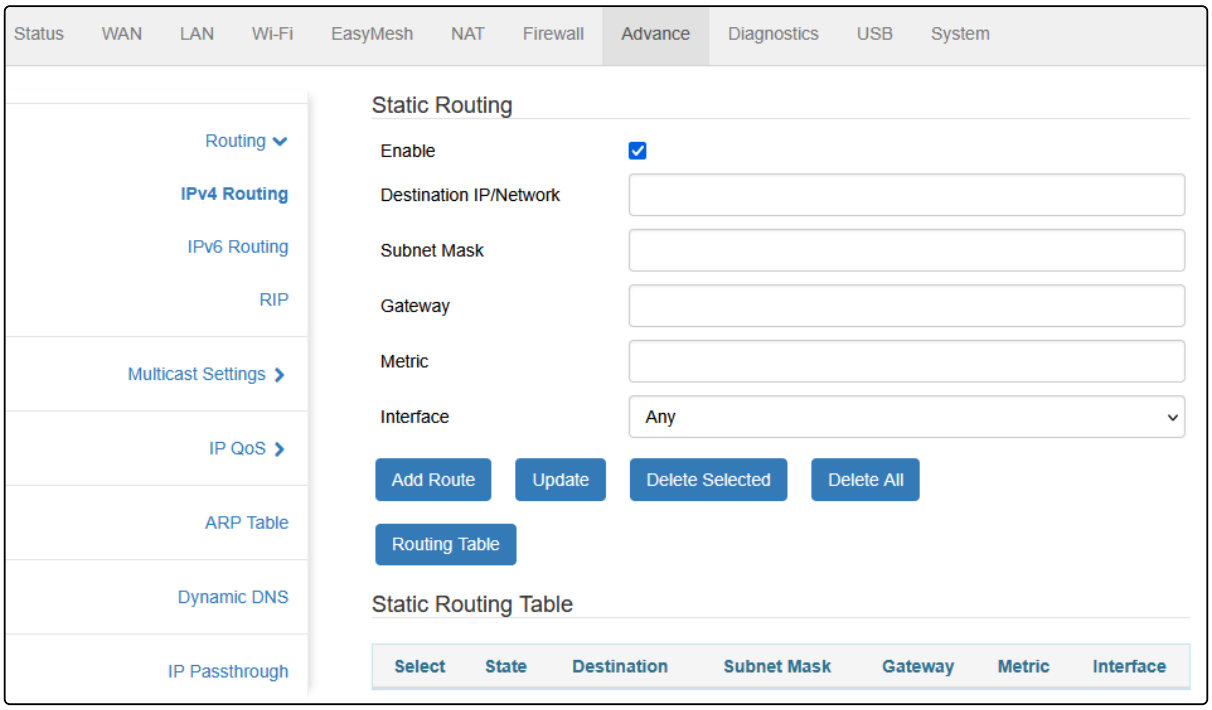
4.6.10.10 SPI submenu

SPI (Stateful Packet Inspection) technology — additionally protects from attacks by checking incoming traffic for correctness (operates at the network, session, and application layers of the OSI model).



4.6.11 Advance menu

4.6.11.1 Routing. IPv4 Routing submenu



Enable — when the flag is set, static routes will be added to the routing table.

Destination IP/Network — the input field for the address of the host or destination network to which the route is specified.

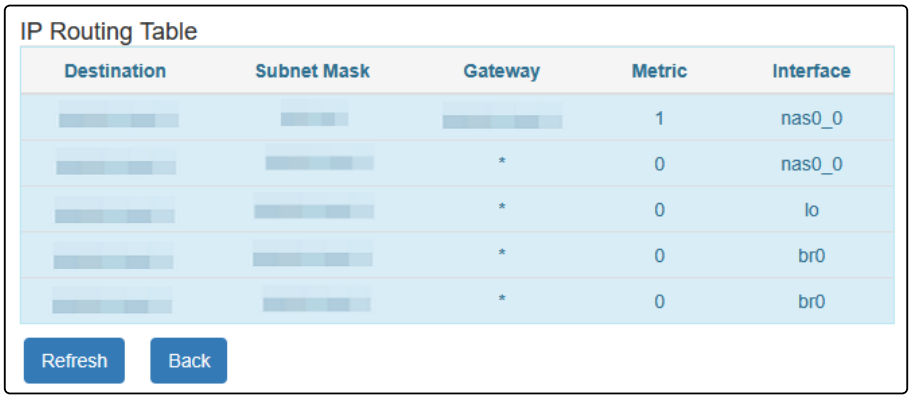
Subnet Mask — the input field for the subnet mask. For the host, the subnet mask is set to 255.255.255.255, for the subnet, depending on its size.

Gateway — the input field of the IP address of the gateway through which the "IP address" is accessed.

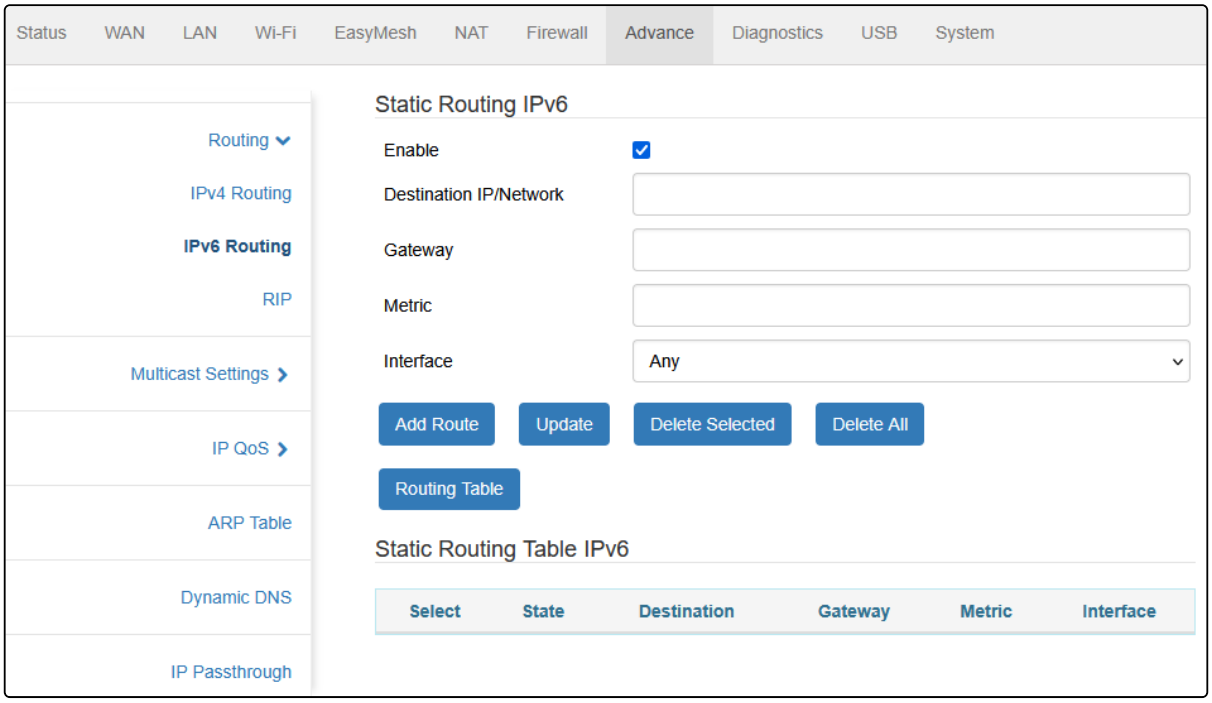
Metric — the input field for a numeric value indicating the preferred route. The lower the number, the more preferred the route.

Interface — selection of the type of device output interface through which the target network is accessible.

Clicking the "Routing Table" button opens the current device routing table in a new window.



4.6.11.2 IPv4 Routing submenu



Enable — when the flag is set, static routes will be added to the routing table.

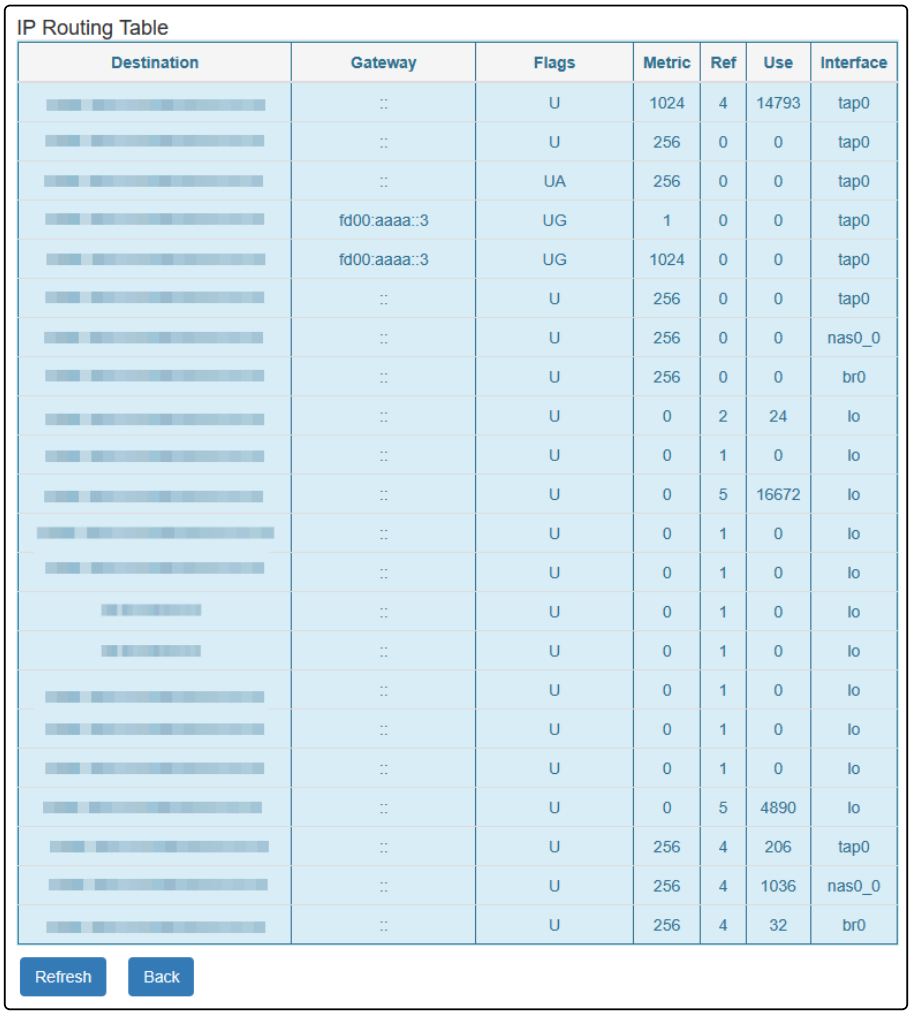
Destination IP/Network — input field for the host or destination network address and prefix in the <IP>/<prefix> format to which the route is specified.

Gateway — the input field of the IP address of the gateway through which the "IP address" is accessed.

Metric — the input field for a numeric value indicating the preferred route. The lower the number, the more preferred the route.

Interface — selection of the type of device output interface through which the target network is accessible.

Clicking the "Routing Table" button opens the current device routing table in a new window.

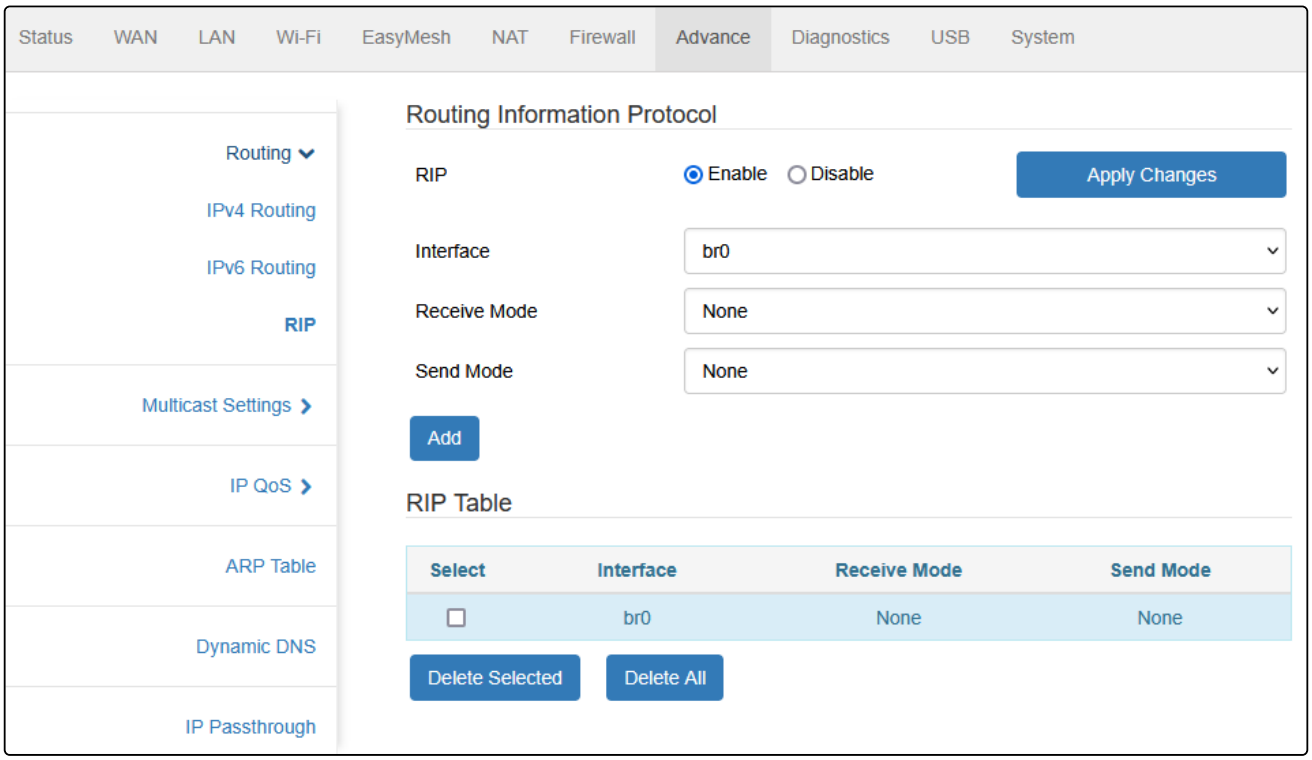

IP Routing Table

Destination	Gateway	Flags	Metric	Ref	Use	Interface
[redacted]	::	U	1024	4	14793	tap0
[redacted]	::	U	256	0	0	tap0
[redacted]	::	UA	256	0	0	tap0
[redacted]	fd00:aaaa::3	UG	1	0	0	tap0
[redacted]	fd00:aaaa::3	UG	1024	0	0	tap0
[redacted]	::	U	256	0	0	tap0
[redacted]	::	U	256	0	0	nas0_0
[redacted]	::	U	256	0	0	br0
[redacted]	::	U	0	2	24	lo
[redacted]	::	U	0	1	0	lo
[redacted]	::	U	0	5	16672	lo
[redacted]	::	U	0	1	0	lo
[redacted]	::	U	0	1	0	lo
[redacted]	::	U	0	1	0	lo
[redacted]	::	U	0	1	0	lo
[redacted]	::	U	0	1	0	lo
[redacted]	::	U	0	1	0	lo
[redacted]	::	U	0	1	0	lo
[redacted]	::	U	0	5	4890	lo
[redacted]	::	U	256	4	206	tap0
[redacted]	::	U	256	4	1036	nas0_0
[redacted]	::	U	256	4	32	br0

Refresh Back

4.6.11.3 RIP submenu

Routing Information Protocol (RIP) is a dynamic routing protocol.



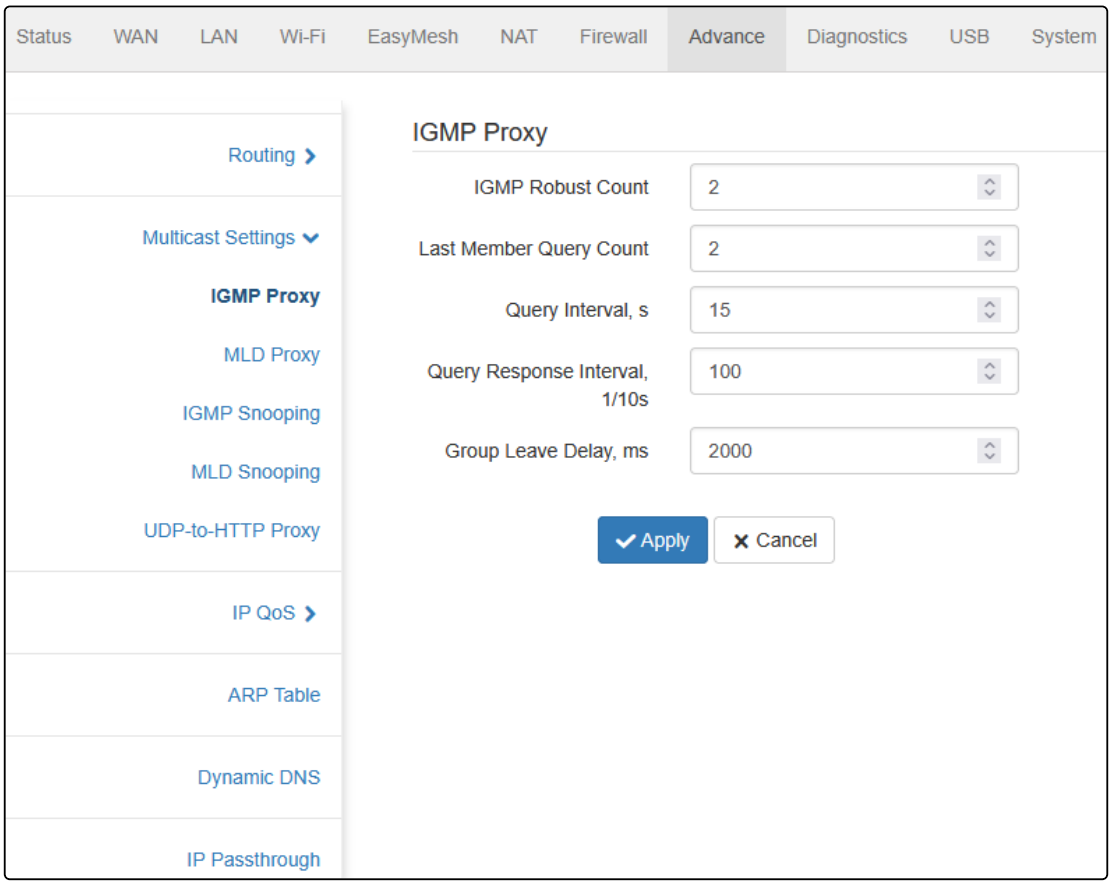
RIP — when the flag is set, the dynamic routing function over the RIP protocol is enabled.

Interface — selection of the interface for RIP operation.

Receive Mode/Send Mode — selection of the dynamic routing protocol RIP1 or RIP2 for the appropriate direction.

4.6.11.4 Multicast Settings. IGMP Proxy submenu

This submenu configures the IGMP Proxy feature more precisely.



IGMP Robust Count — the number of attempts to send an IGMP message in case of packet loss.

Last Member Query Count — the number of Group-Specific messages sent after the last client leaves the group.

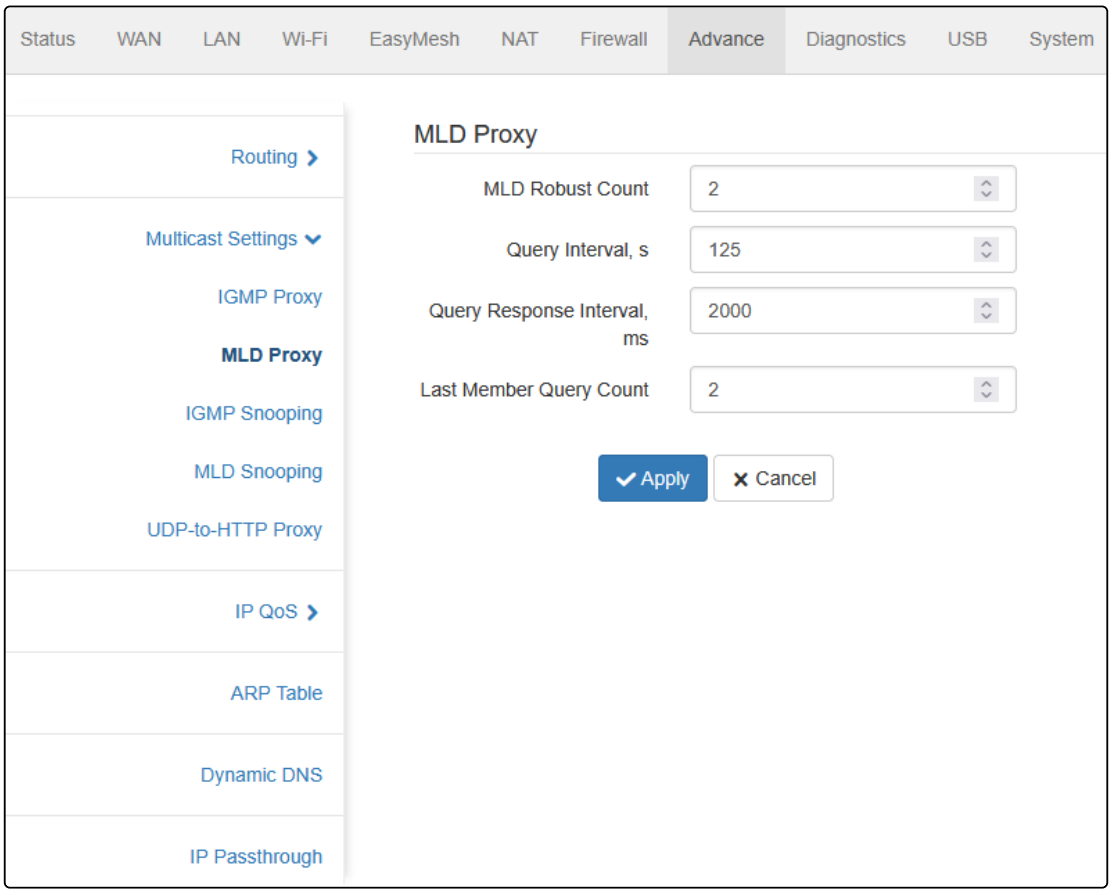
Query Interval, s — the time interval indicating the frequency of sending Query messages.

Query Response Interval, 1/10 s — the time interval indicating the delay in responding to the Query message from the client.

Group Leave Delay, ms — the time interval indicating the delay between sending Group-Specific messages after the last client leaves the group.

4.6.11.5 MLD Proxy submenu

This submenu configures the MLD Proxy feature more precisely.



MLD Robust Count — the number of attempts to send an MLD message in case of packet loss.

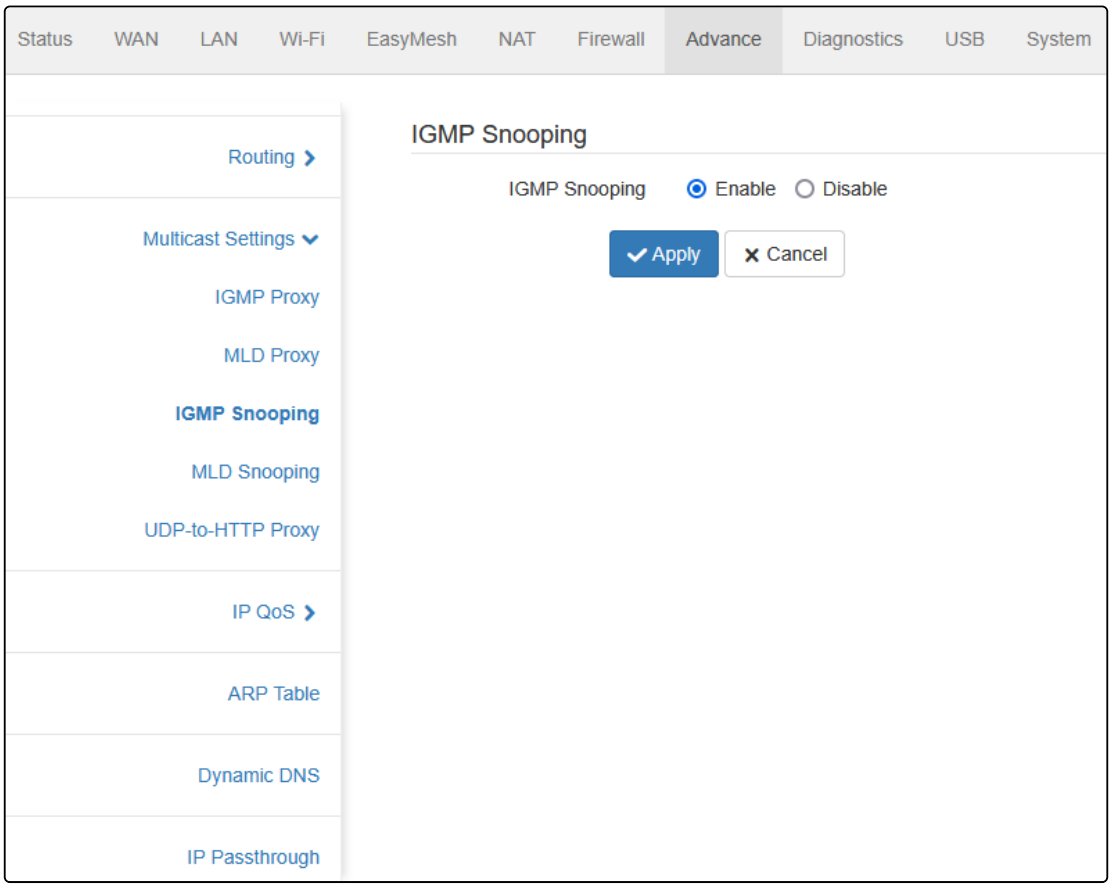
Query Interval, s — the time interval indicating the frequency of sending Query messages.

Query Response Interval, ms — the time interval indicating the delay in responding to the Query message from the client.

Last Member Query Count — the number of Group-Specific messages sent after the last client leaves the group.

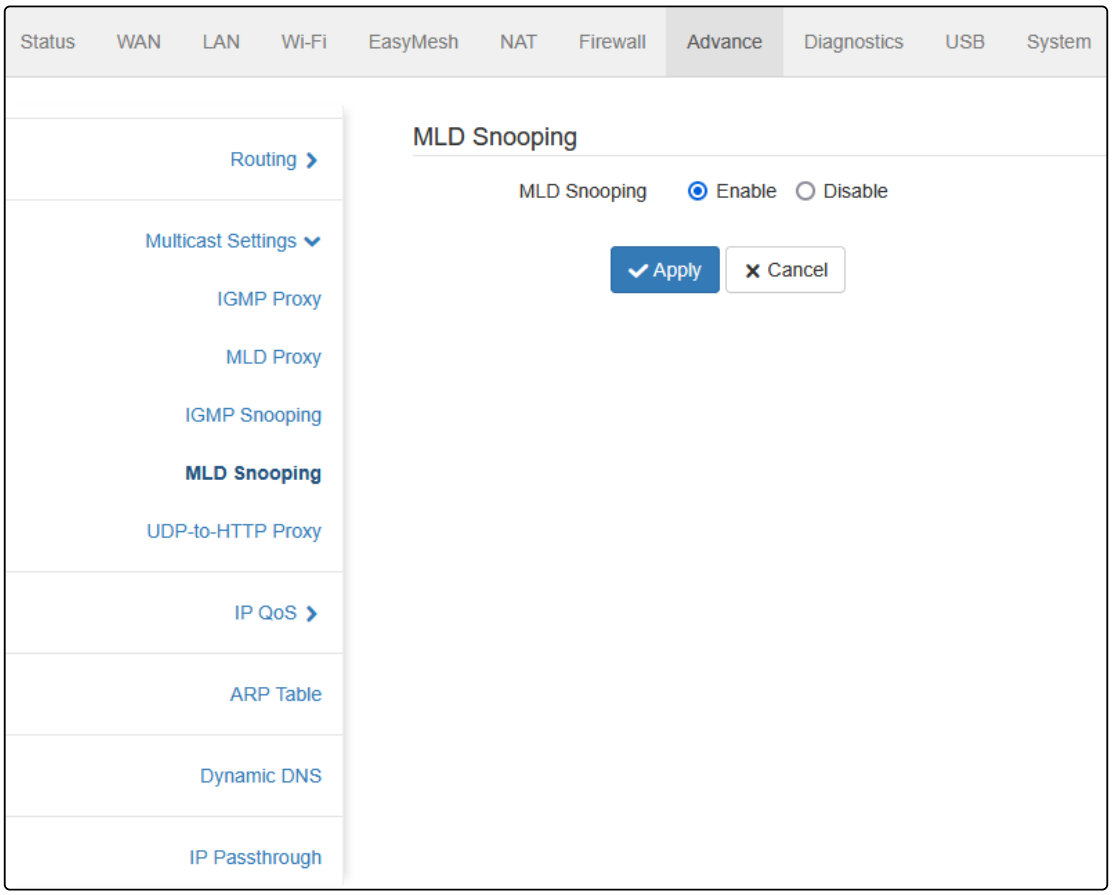
4.6.11.6 IGMP Snooping submenu

ΠThe "IGMP Snooping" submenu enables multicast traffic filtering over the IPv4 protocol.



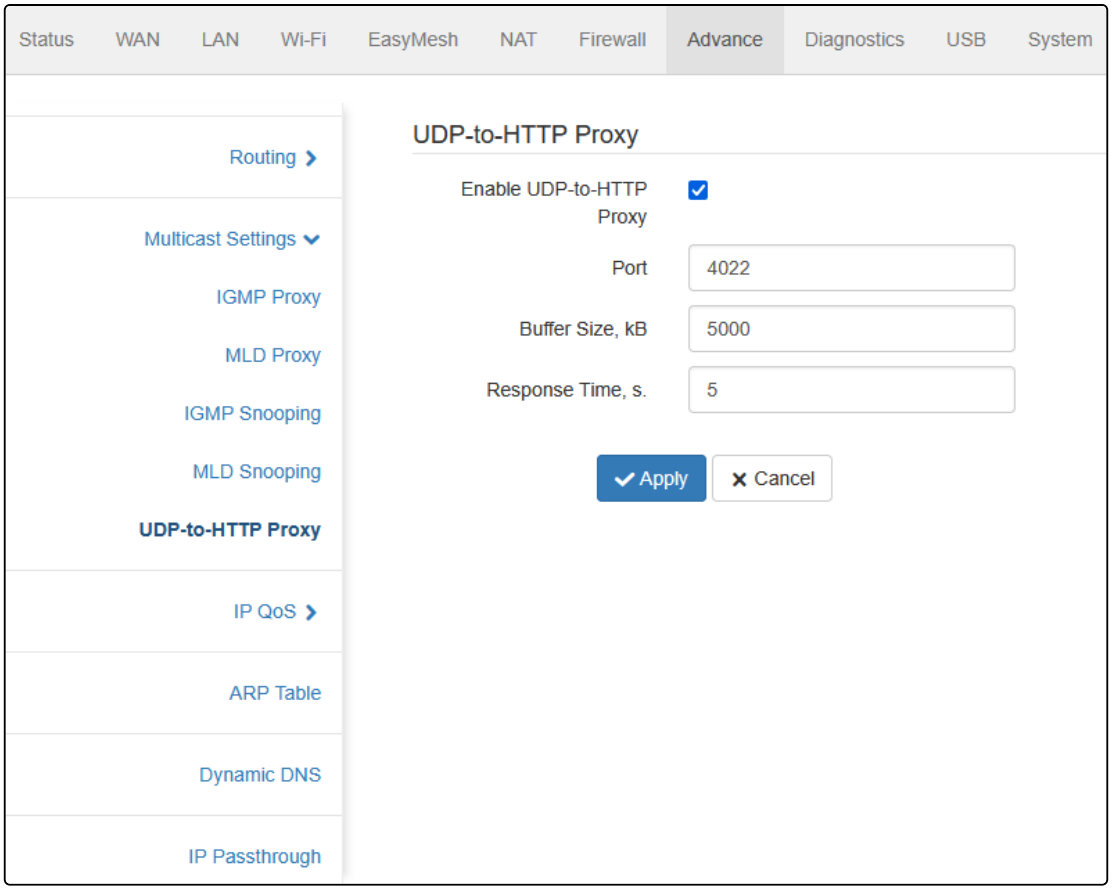
4.6.11.7 MLD Snooping submenu

The "MLD Snooping" submenu enables multicast traffic filtering over the IPv6 protocol.



4.6.11.8 UDP-to-HTTP Proxy submenu

The UDP-to-HTTP Proxy function is designed for watching IPTV on devices and players that do not support multicast transmitted over the UDP protocol. The IPTV channel requested by such a player will be broadcast to it via an HTTP connection.



Enable UDP-to-HTTP Proxy — when the flag is set, the UDP-to-HTTP Proxy function is enabled.

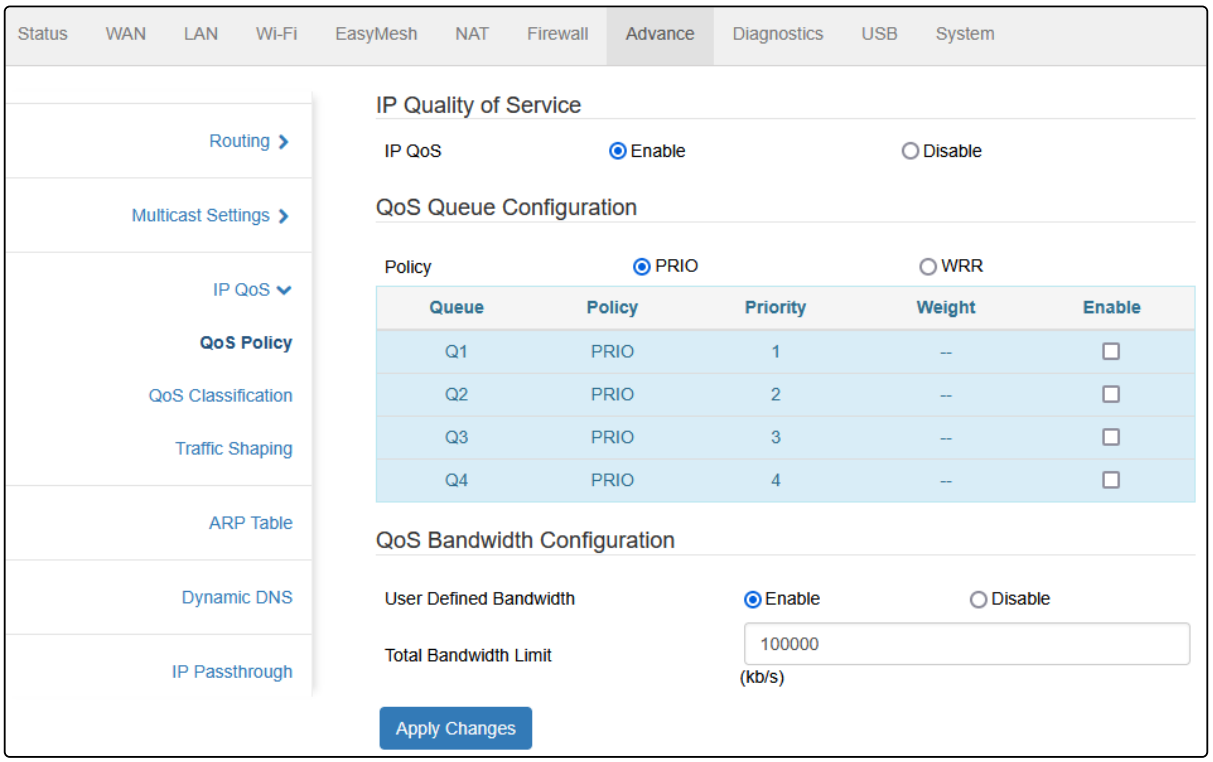
Port — the TCP port number that clients will access.

Buffer Size, kB — the size of the buffered stream in kilobytes.

Response Time, s. — value in seconds after which the device must unsubscribe from the group in case of termination of the TCP connection.

4.6.11.9 IP QoS. QoS Policy submenu

This submenu enables and configures the Quality of Service (QoS) feature.



IP QoS — when the flag is set, the QoS policy and queue settings are enabled.

Policy — definition of a way to label queue scheduling:

- *PRIO* — strict priority;
- *WRR* — a weighted cyclic algorithm.

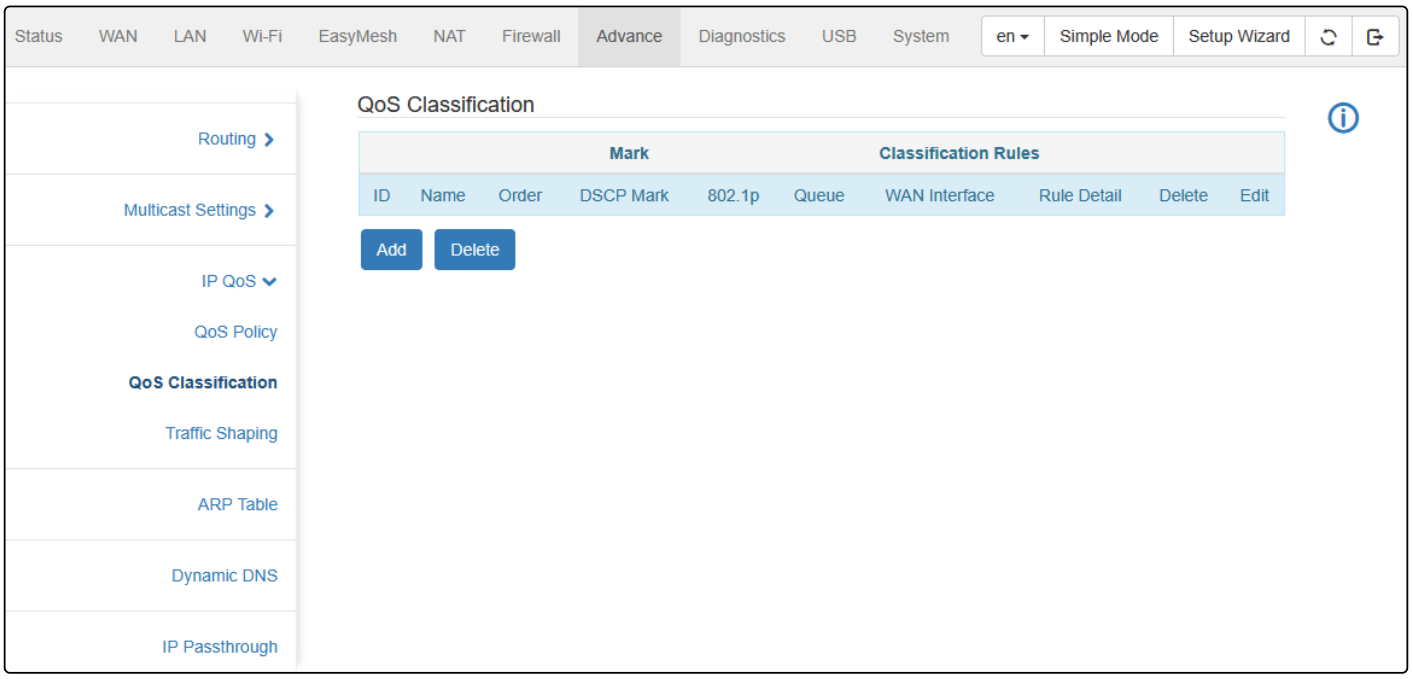
QoS Bandwidth Configuration

User Defined Bandwidth — when the flag is set, the user's bandwidth limit setting is enabled.

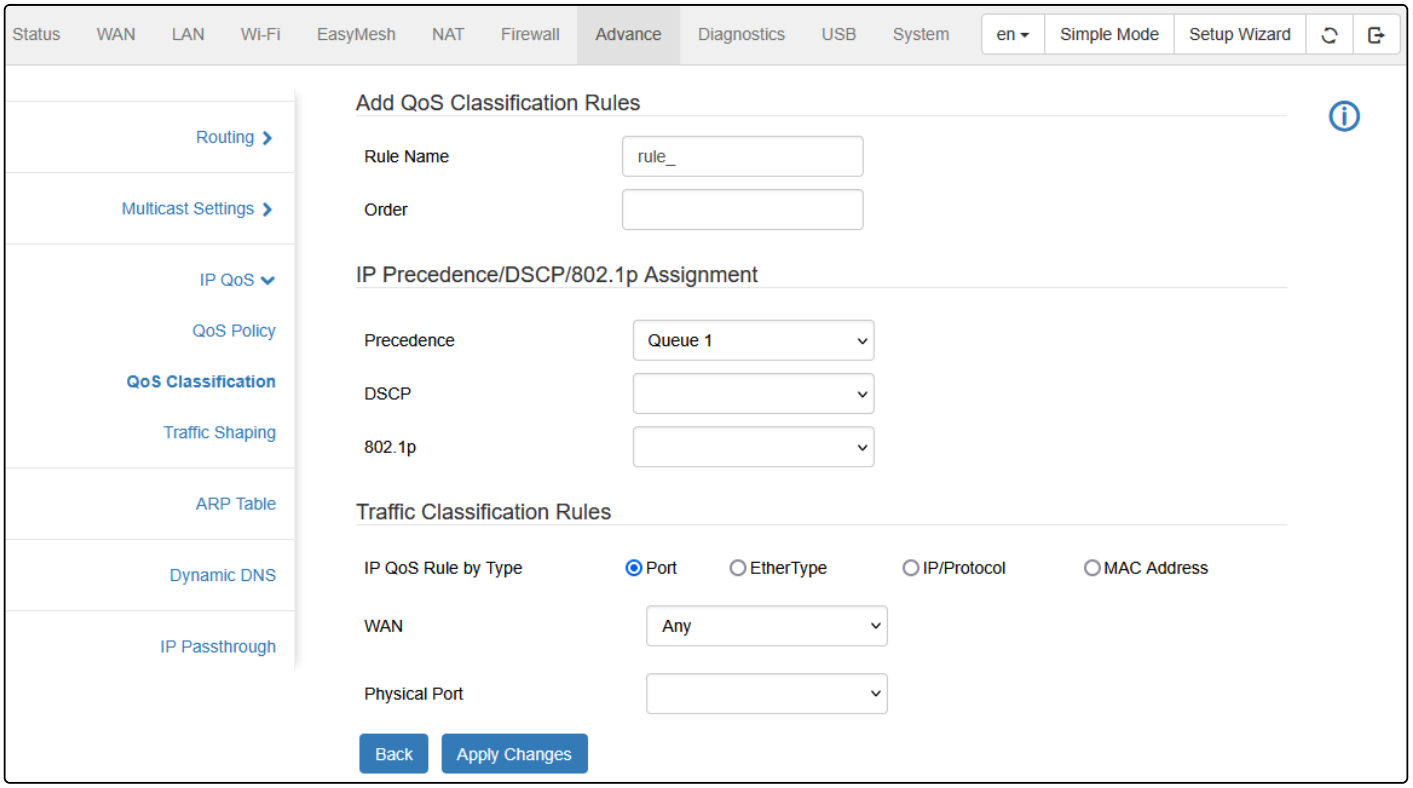
Total Bandwidth Limit — adjusting the bandwidth by the user.

4.6.11.10 QoS Classification submenu

In this submenu, one can create a traffic classification rule based on the selected type.



Clicking the "Add" button opens the window for adding QoS classification rules:



Add QoS Classification Rules

Rule Name — the name of the rule to add.

Order — the order in the list of rules for a new entry.

IP Precedence/DSCP/802.1p Assignment

Precedence — selection of a queue to which packets that meet the conditions of this rule will be redirected.

DSCP — selection of a new DSCP label to packets.

802.1p — selection of the value of 802.1p.

Traffic Classification Rules

IP QoS Rule by Type — selection of the criterion by which packets will be classified. The following criteria are available:

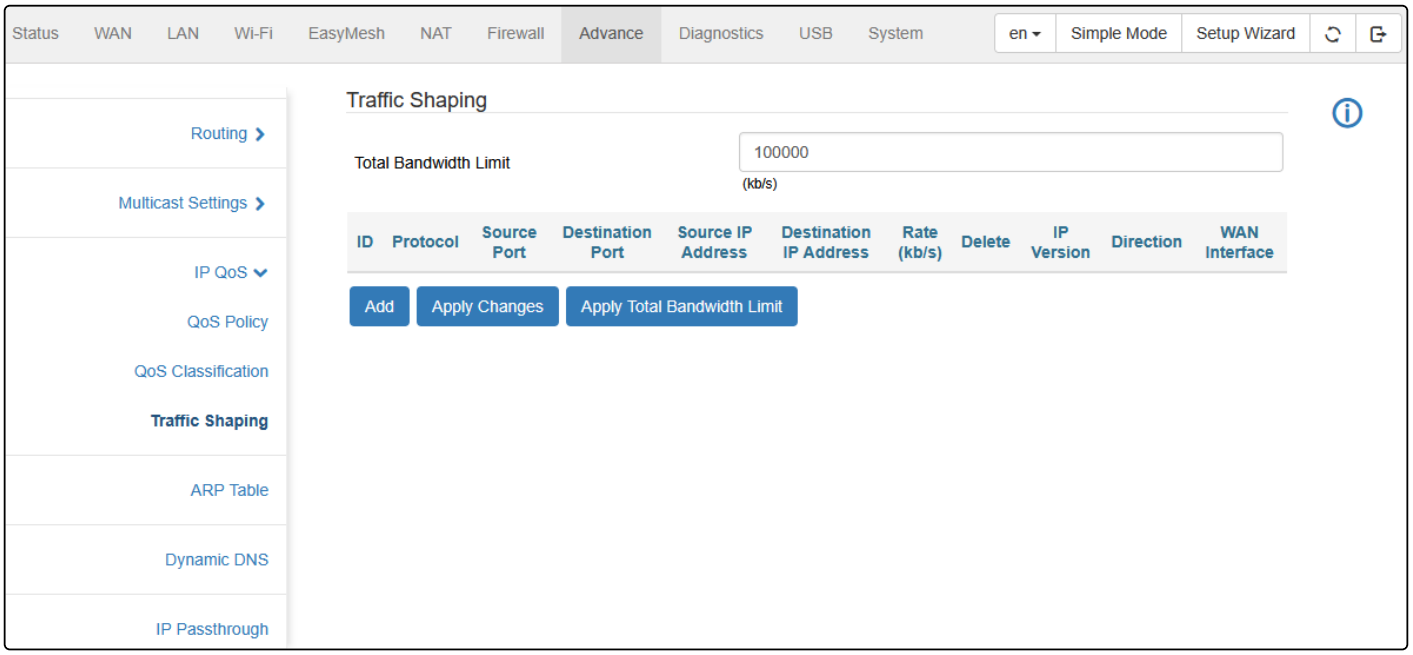
- *Port:*
  - *Physical Port* — the physical LAN port selection field.
- *EtherType:*
  - *Ethernet Type* — the type of traffic encapsulated in the Ethernet frame. The input is in hexadecimal format.
- *IP/Protocol:*
  - *Protocol* — the protocol selection for classification. TCP, UDP, ICMP or TCP/UDP;
  - *DSCP* — selecting of the DSCP label for classification;
  - *Source IP Address* — the IP address of the sender of the packet (node or subnet);
  - *Source Mask* — the mask of the source IP address (in the x.x.x format);
  - *Destination IP Address* — the IP address of the packet recipient (node or subnet);
  - *Destination Mask* — the mask of the destination IP address (in the x.x.x format);
  - *Source Port* — the port from which packets are sent (available only when TCP or UDP protocol is selected);
  - *Destination Port* — the port to which packets are sent (available only when TCP or UDP protocol is selected).
- *MAC Address:*
  - *Source MAC Address* — the MAC address of the sender;
  - *Destination MAC* Address — the MAC address of the recipient.

WAN — the WAN interface for which the rule is being added.

To enable QoS and specify the WAN interface for these connections, select the checkbox "Enable Qos" on the WAN menu → Ethernet WAN submenu.

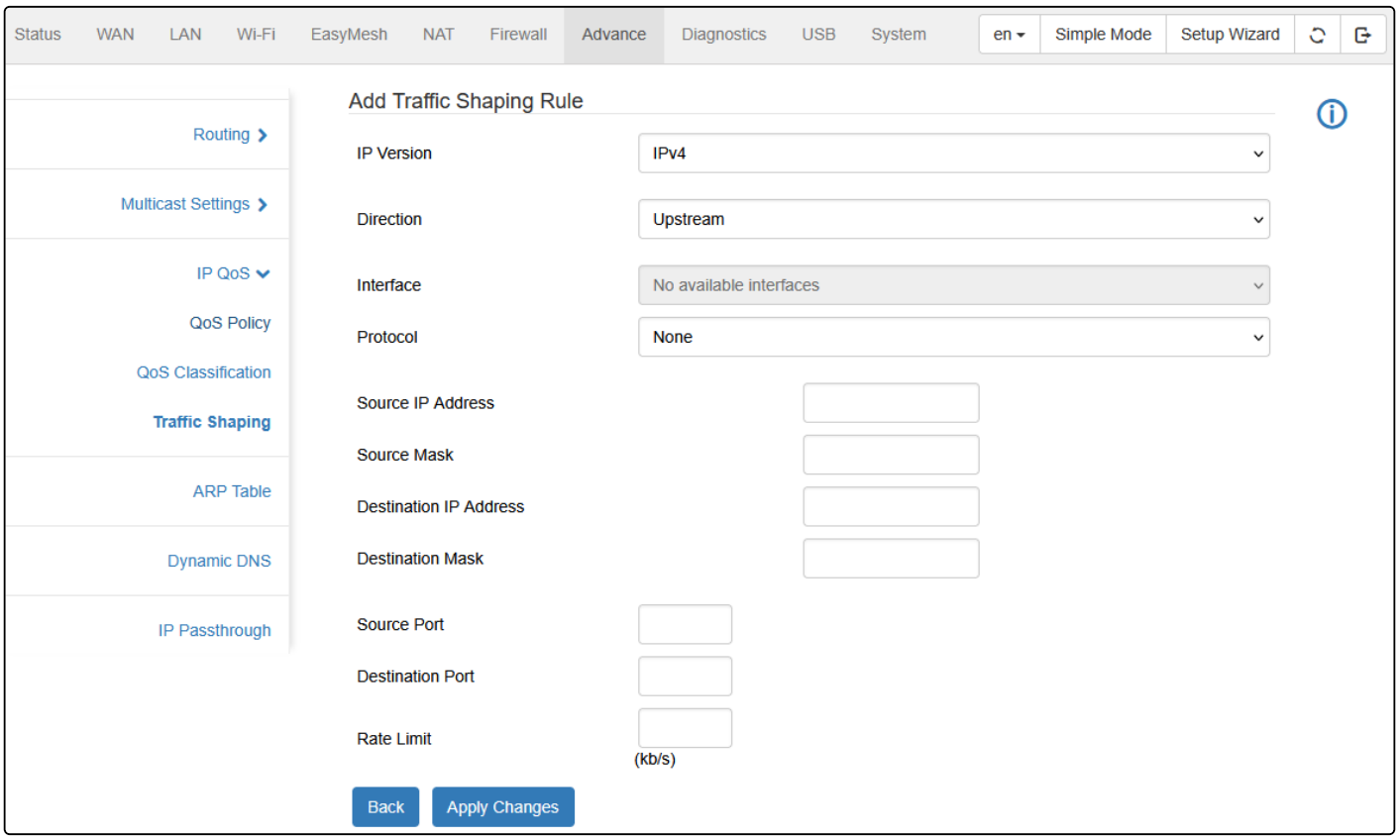
4.6.11.11 Traffic Shaping submenu

In this submenu, one can add a limit on the total bandwidth, as well as on a certain type of traffic according to a given rule.



Add Traffic Shaping Rule

Click the "Add" button to open a window for adding traffic shaping rules.



IP Version — the version of the selected IP;

Direction — traffic direction (Upstream);

Interface — an interface for adding traffic shaping rules;

Protocol — a type of TCP, UDP, or ICMP traffic protocol;

Source IP Address — the IP address of the sender of the packet (node or subnet);

Source Mask — the mask of the source IP address (in the x.x.x.x format);

Destination IP Address — the IP address of the packet recipient (node or subnet);

Destination Mask — the mask of the destination IP address (in the x.x.x.x format);

Source Port — the port from which packets are sent (available only when TCP or UDP protocol is selected);

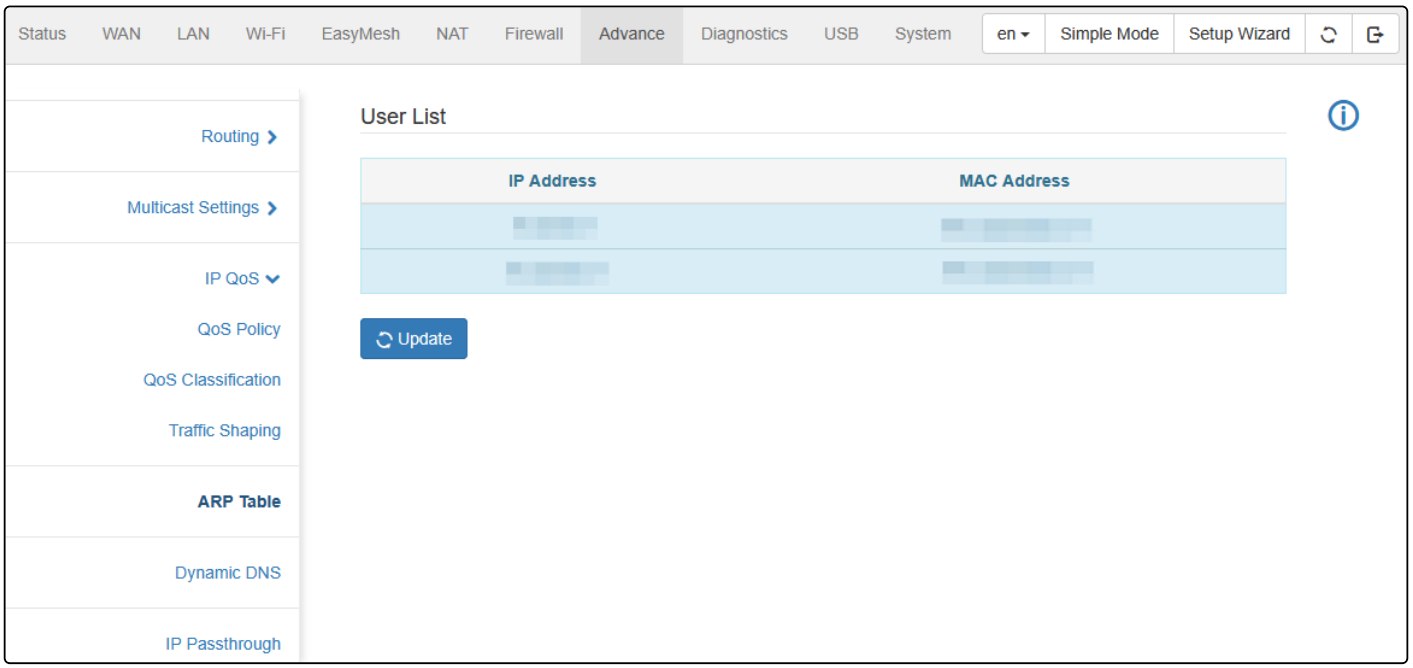
Destination Port — the port to which packets are sent (available only when TCP or UDP protocol is selected);

Rate Limit — bandwidth limitation in Kbps.

To enable traffic shaping, select the checkbox "Enable Qos" on the WAN menu → Ethernet WAN submenu for the needed WAN-connection. After that, the connections will be available in the interface selection list.

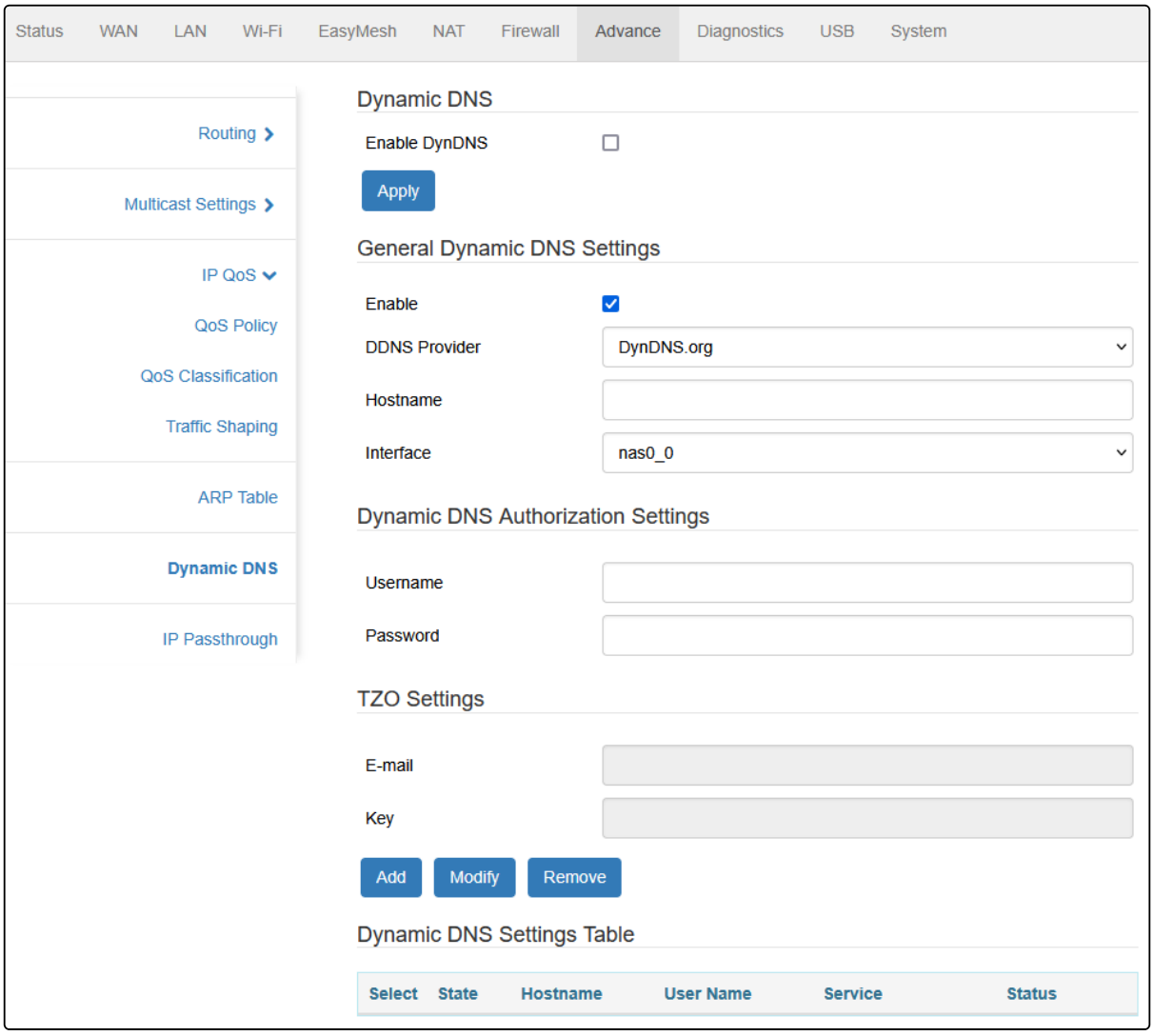
4.6.11.12 ARP Table submenu

The ARP table is an associative table of MAC and IP addresses of devices.



4.6.11.13 Dynamic DNS submenu

In this submenu, one can activate the service of providing a permanent domain name to a device with a dynamic IP address.



General Dynamic DNS Settings

Enable — when adding dynamic DNS, the service will be immediately active.

DDNS Provider — selection of a DDNS service provider.

Hostname — domain name of the service provider.

Interface — selection of an interface.

Dynamic DNS Authorization Settings

Username — *user* login on the service provider website.

Password — password.

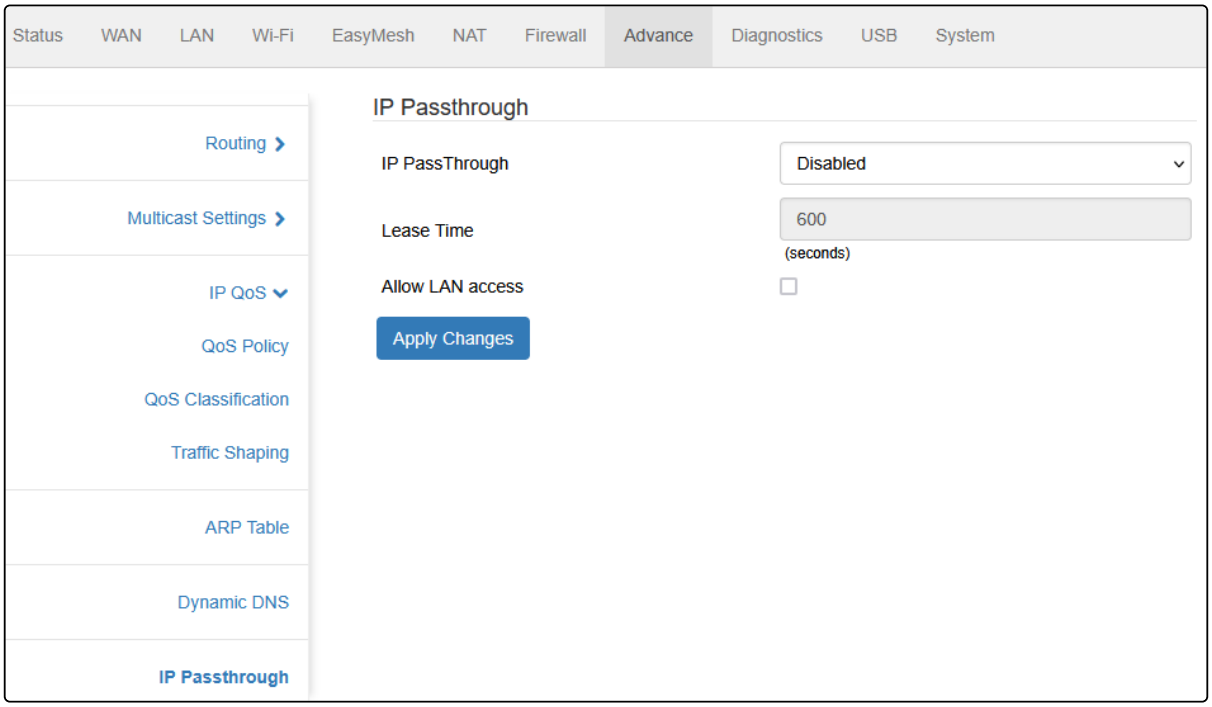
TZO Settings

E-mail — user login on the service provider's website.

Key — password.

4.6.11.14 IP Passthrough submenu

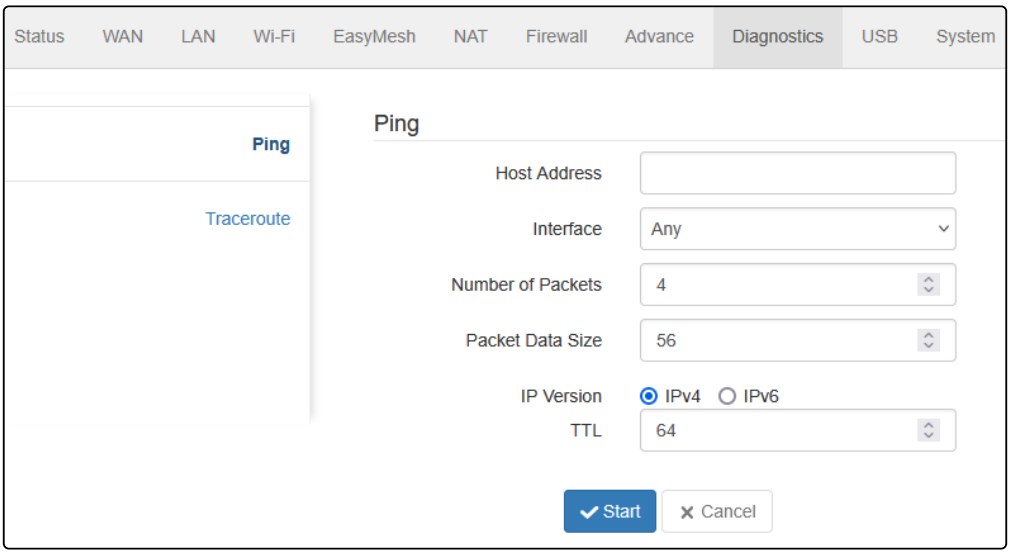
The "IP Passthrough" mode allows transparent broadcast of an external IP address from the PPPoE interface to an internal local client.



4.6.12 Diagnostics menu

4.6.12.1 Ping submenu

This submenu allows one to launch ping from any device interface to any host using the web interface.



Host Address — the address of the device to which diagnostics will be performed.

Interface — selection of the interface through which diagnostics will be performed.

Number of Packets — the number of packets being sent.

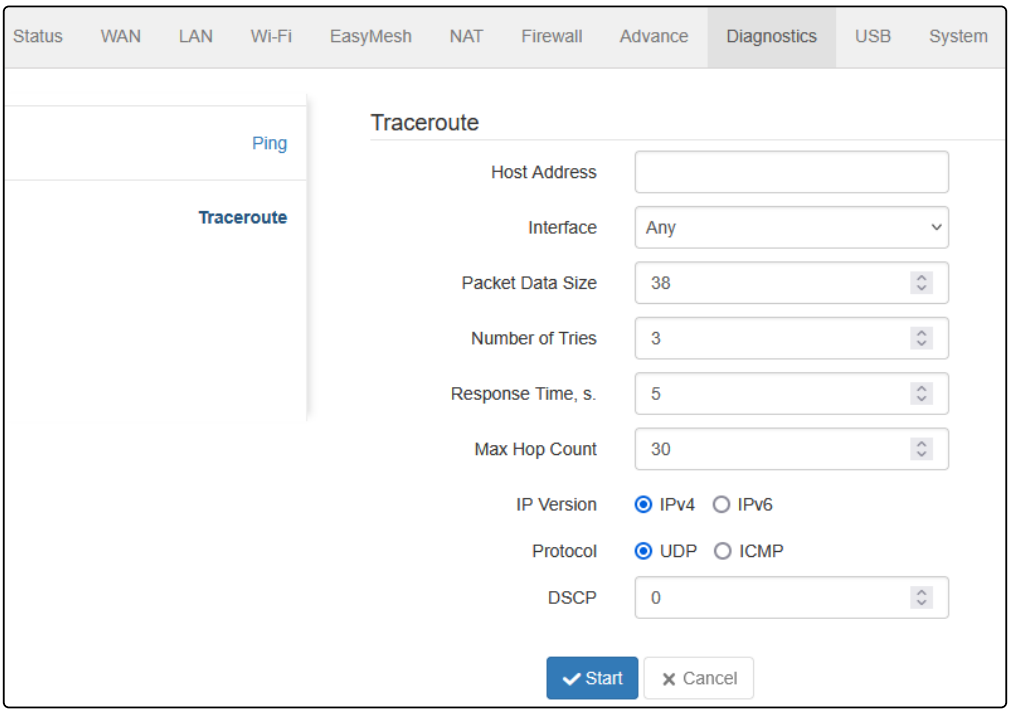
Packet Data Size — the size of the packet data in bytes.

IP Version — the version of the network protocol used.

TTL — the maximum number of nodes for packet routing.

4.6.12.2 Traceroute submenu

This submenu allows one to start tracing from any interface to any host using the traceroute utility.



Host Address — the address of the device to which tracing will be performed;

Interface — the interface through which tracing will be performed;

Packet Data Size — the size of the packet data in bytes;

Number of Tries — the number of tracing attempts;

Response Time, s. — the waiting time for a response to a packet in seconds;

Max Hop Count — the maximum number of nodes for routing a packet;

IP Version — the version of the network protocol used;

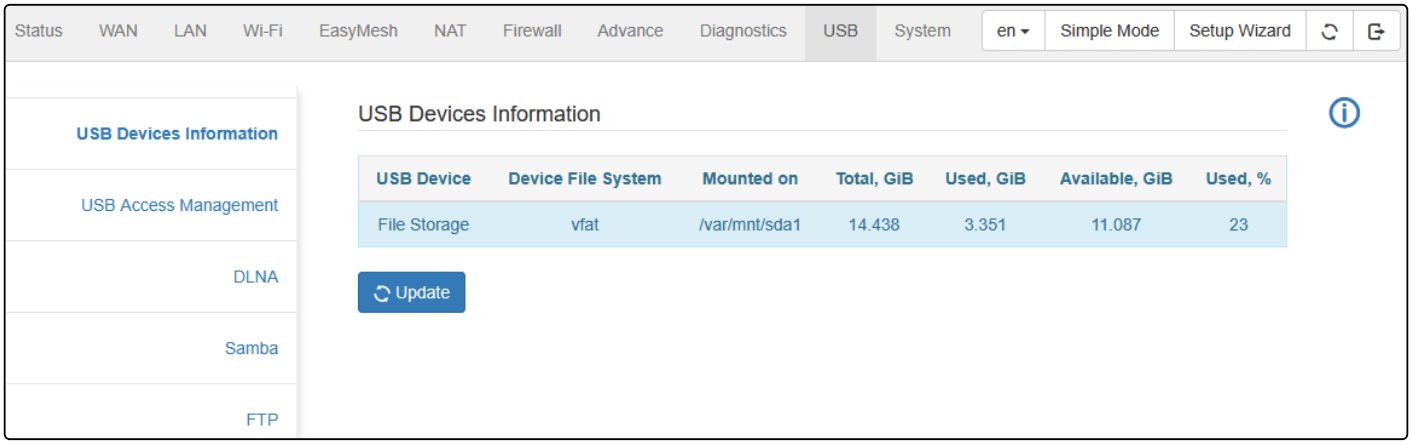
Protocol — the protocol used for tracing;

DSCP — the value of Differentiated services codepoint in the packets being sent.

4.6.13 USB menu

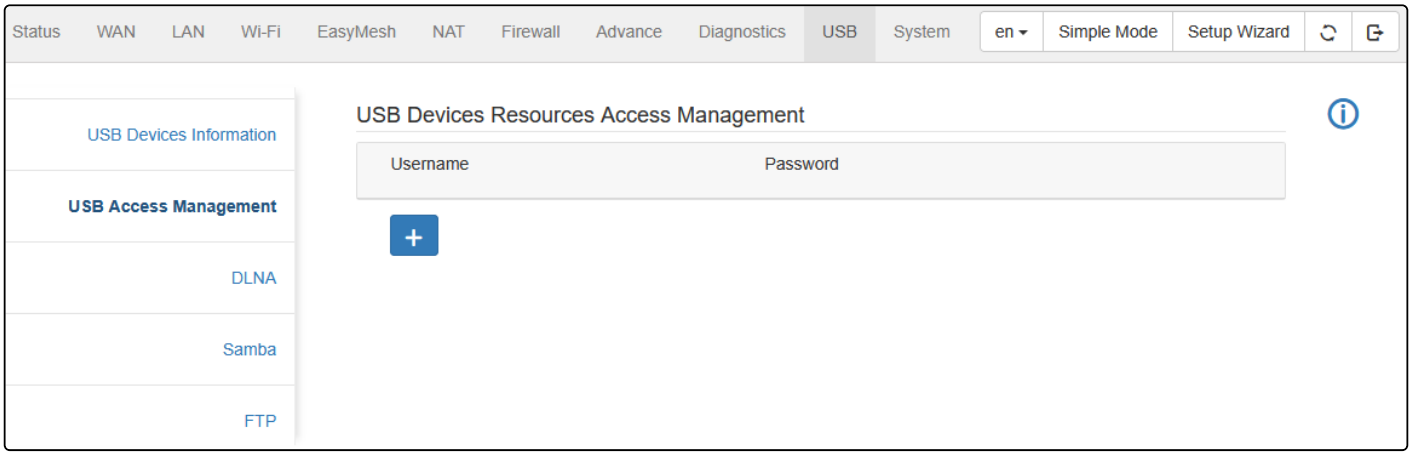
4.6.13.1 USB Devices Information submenu

Information about connected USB devices is available in this submenu.



4.6.13.2 USB Access Management

In this submenu, a user is created to access resources on the USB.



Adding a user

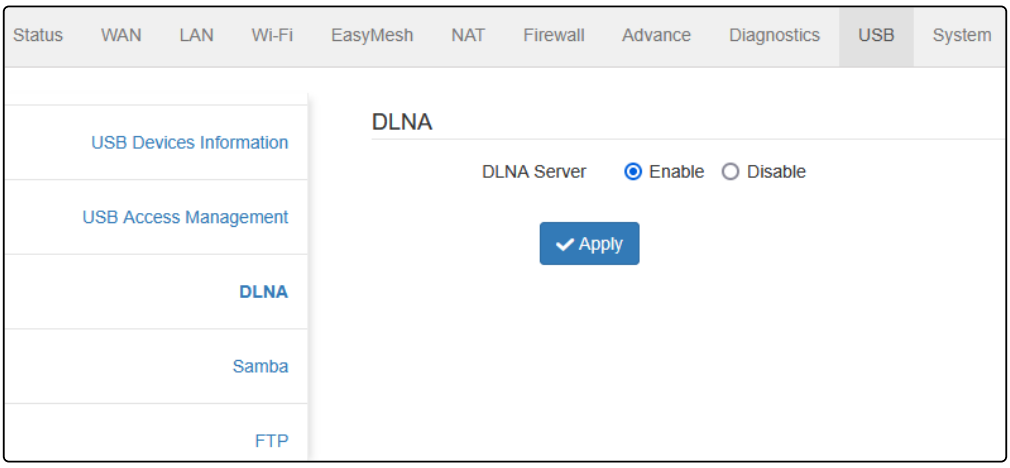
Username — the user who needs to access the resources of the USB device.

Password — the user password.

Confirm Password — confirmation of the user password.

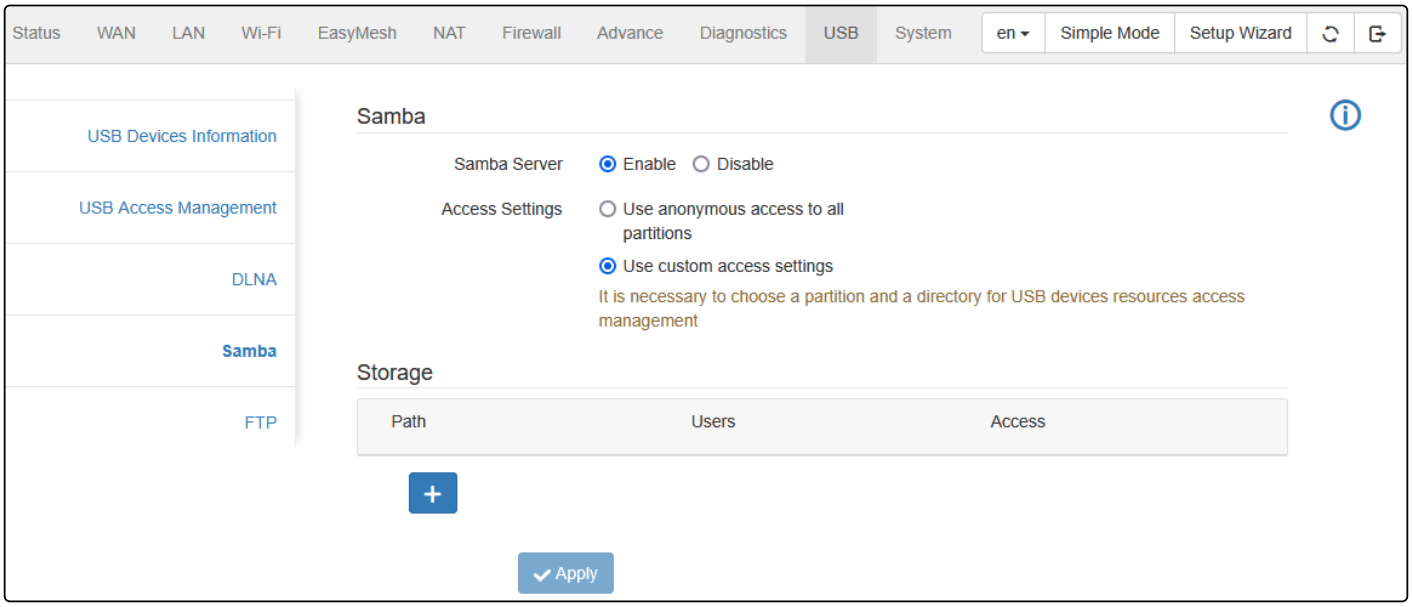
4.6.13.3 DLNA submenu

In this submenu, one can enable the feature of the DLNA server.



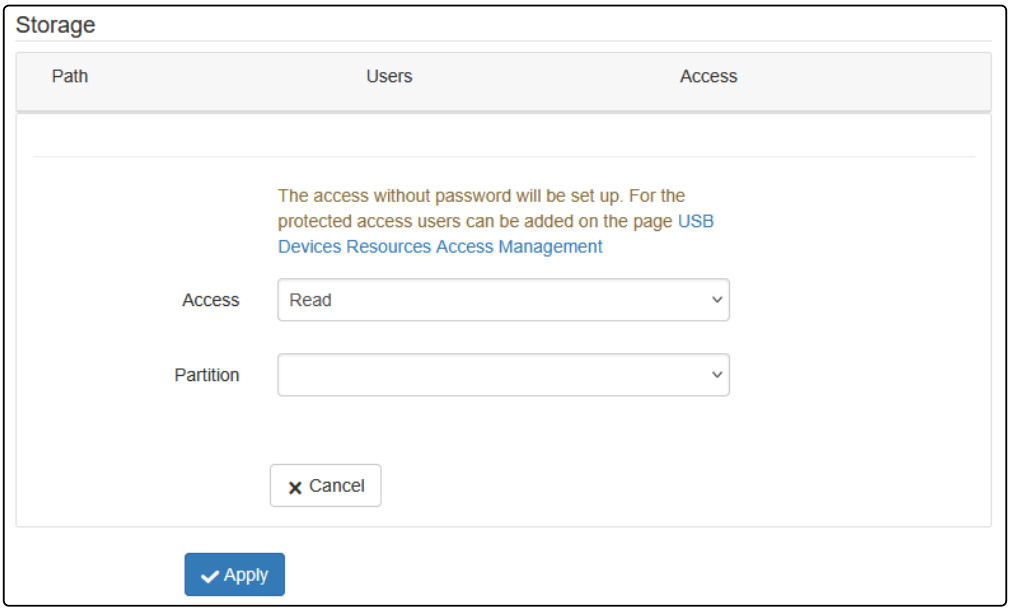
4.6.13.4 Samba submenu

In this submenu, one can enable the feature of the Samba server.



When enabling the Samba server, one can configure anonymous access.

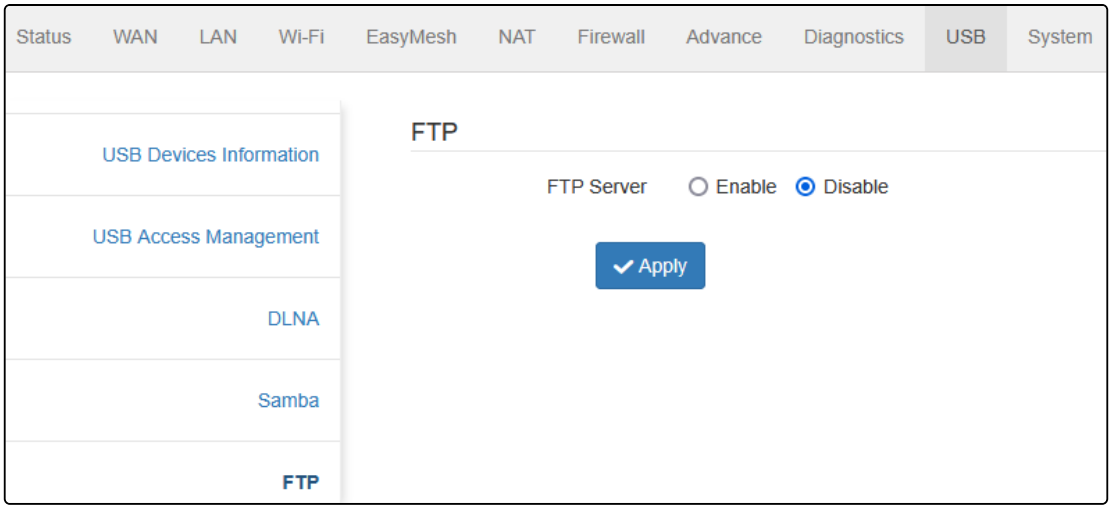
It is also possible to specify the path to the necessary resources on the USB device.



Anonymous access can only be disabled after setting up access for at least one user.

4.6.13.5 FTP submenu

In this submenu, one can enable the FTP server feature.

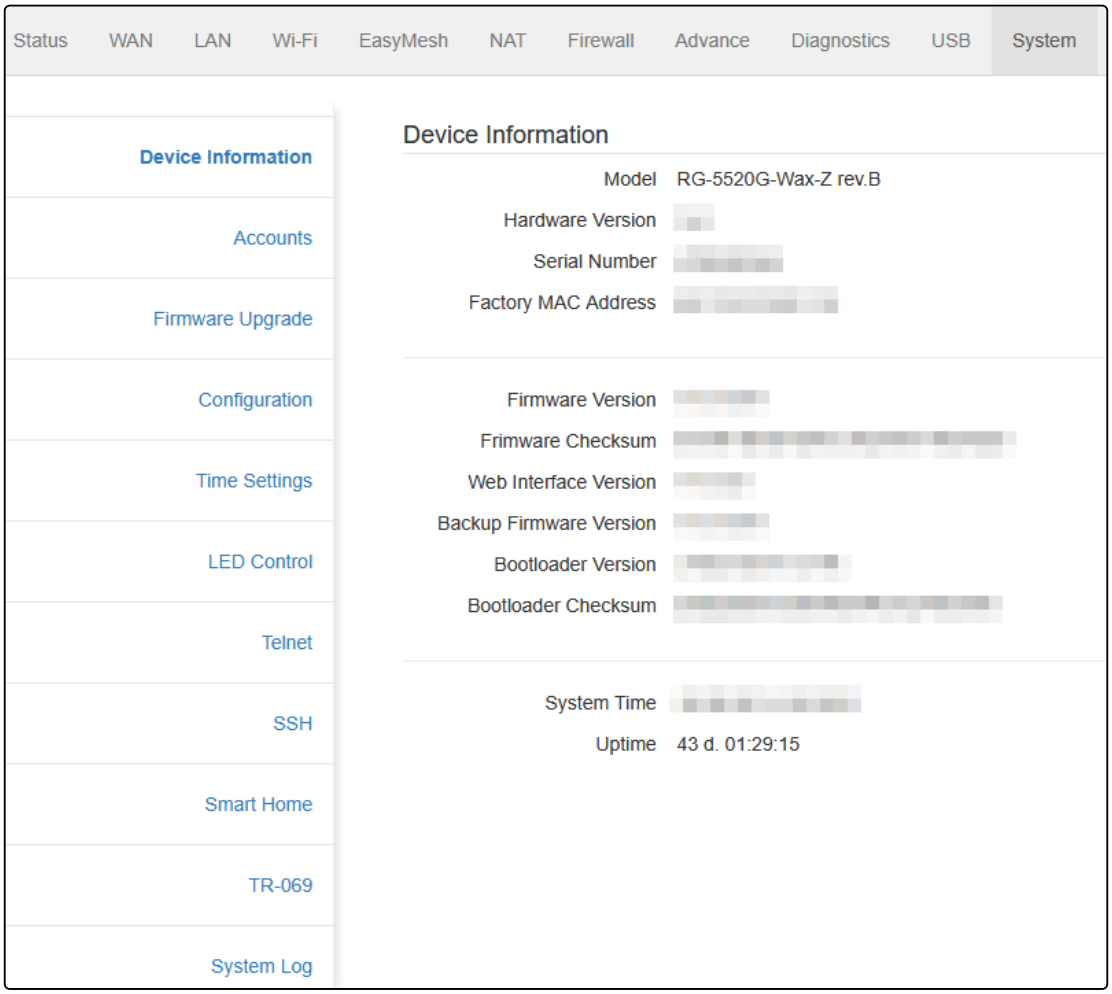


4.6.14 System menu

This menu contains configuration and firmware update options.

4.6.14.1 Device information submenu

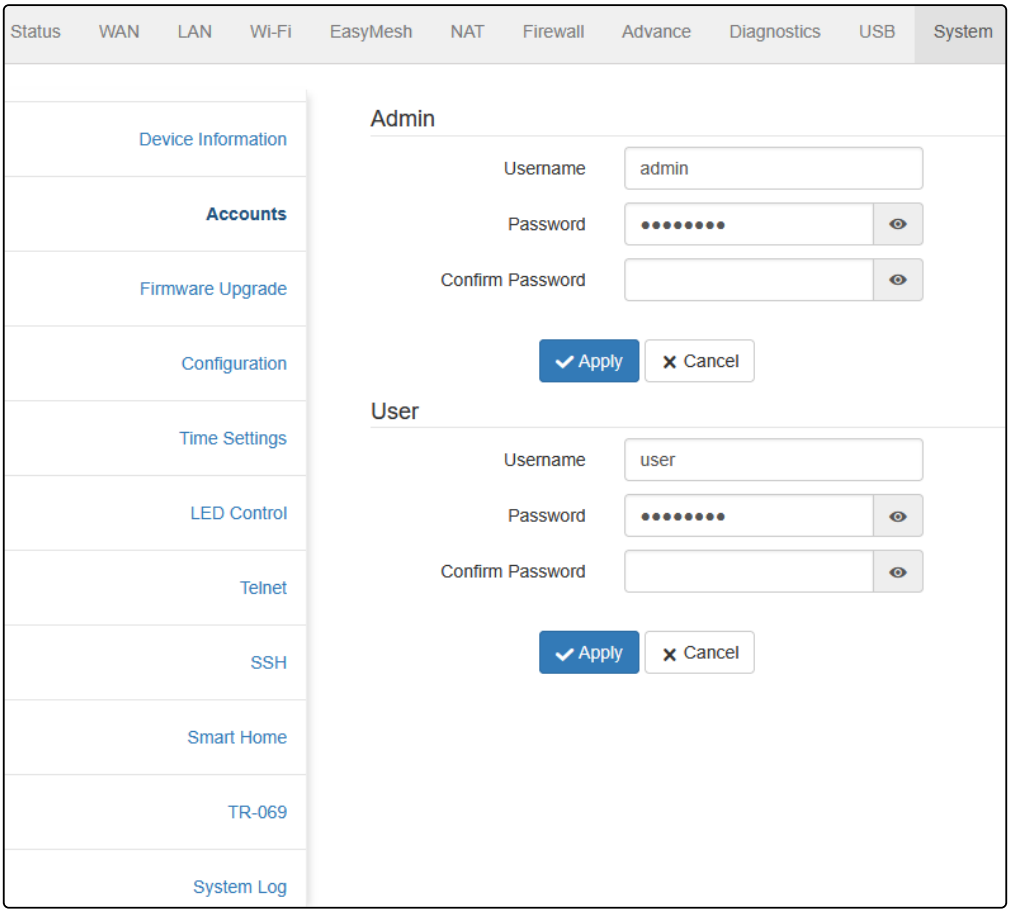
This submenu displays information about the device and basic settings.



4.6.14.2 Accounts submenu

In the "Accounts" submenu, the user name and password for accessing the device web interface for the admin and user accounts are set.

The Admin account is available for viewing and editing only when logged in under this account. The User account only allows one to change one's own account.



Admin

Username — field for changing the user name.

Password — field for changing the device password.

Confirm Password — field for re-entering a new password in order to confirm it.

User

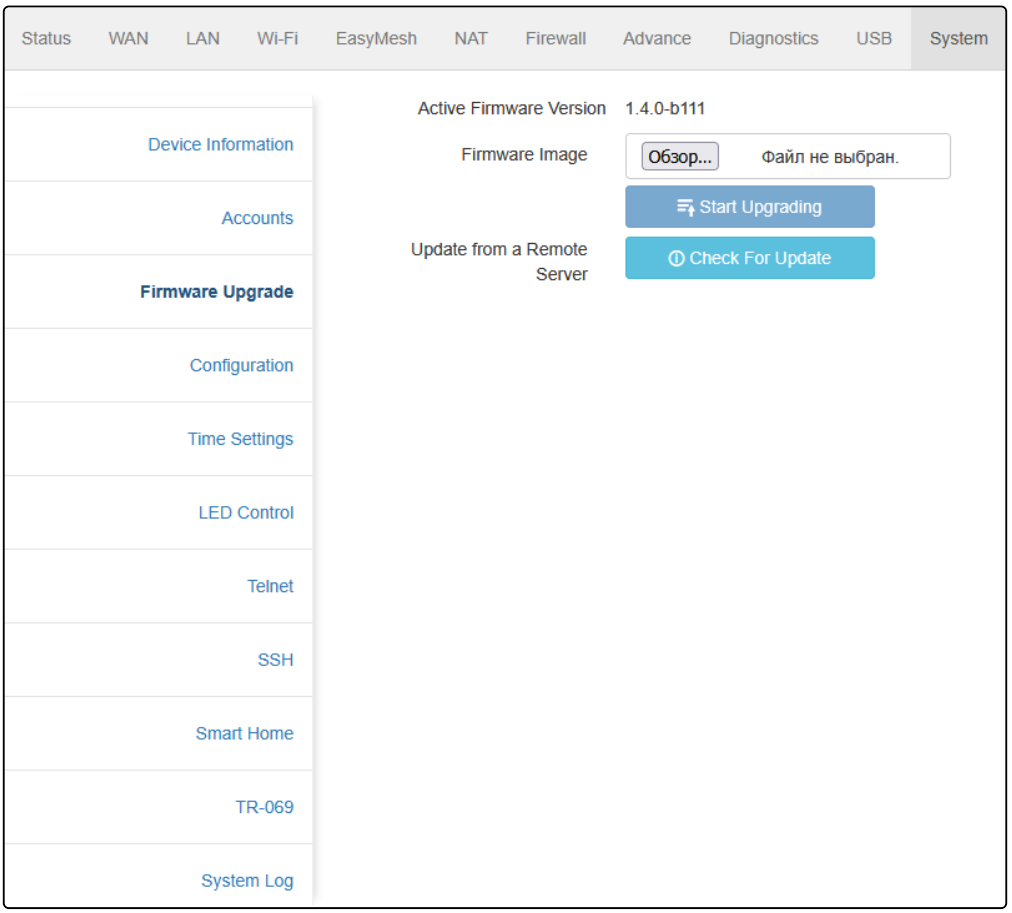
Username — field for changing the user name.

Password — field for changing the device password.

Confirm Password — field for re-entering a new password in order to confirm it.

4.6.14.3 Firmware Update submenu

Firmware Update submenu is designed to update the device's control firmware.



Active Firmware Version is the version of the firmware installed on the device.

In case of damage to the main firmware, the backup is automatically loaded.

If the firmware update is successful, the firmware backup process starts after 10 minutes.

To start the firmware update process, click the "Start Upgrading" button.

To start checking for updates, click the "Check For Update" button

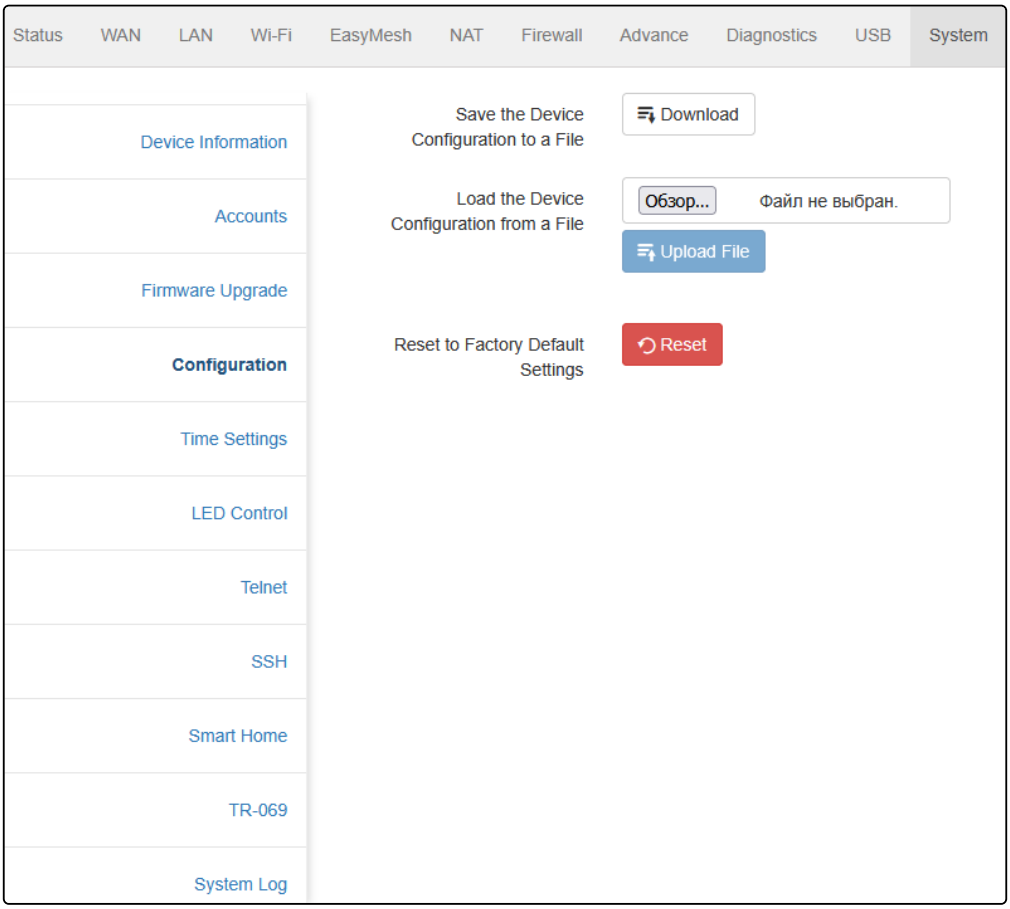
Do not turn off the device or reboot it during the firmware update process.

4.6.14.4 Configuration submenu

In the "Configuration" submenu, the current configuration is saved and updated.

If one is not sure about any settings, it is recommended to save the configuration file of the current installations to restore the configuration in an emergency.

> ⚠ **Also, if necessary, one can reset all the settings to factory settings and then configure the device again.**



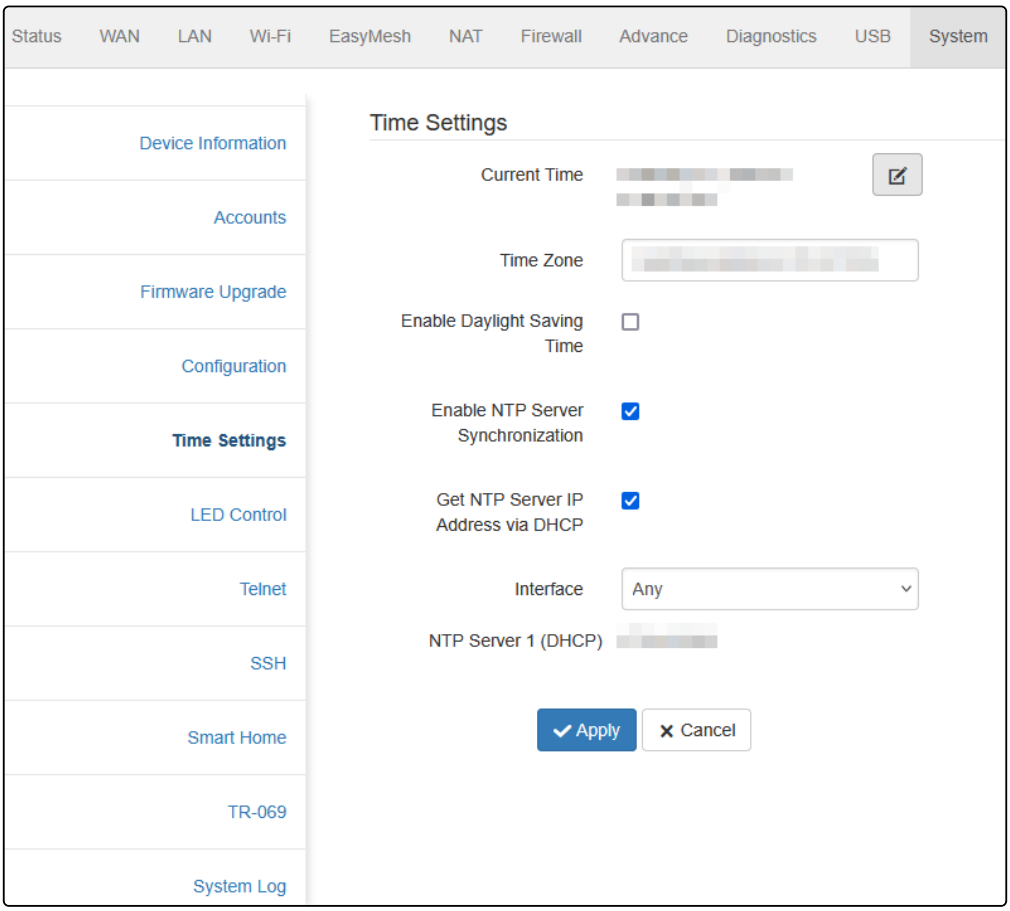
Save the Device Configuration to a File — to save the current device configuration to the local computer, click the "Download" button.

Load the Device Configuration from a File — selection of the configuration file saved on the local computer. To update the device configuration, click the "Browse" button and specify the file (in .cfg format) and click the "Upload File" button.

Reset to Factory Default Settings — to reset all device settings to the default factory settings, click the "Reset" button.

4.6.14.5 Time Settings submenu

In this submenu, the date and system time of the device are set using synchronization with the NTP-server.



Current Time — current date and time. It is possible to copy this data from the computer instead of entering it.

Time Zone — the time zone in which the device is located. Depending on this, the time adjustment will be performed.

Enable Daylight Saving Time — when the flag is set, daylight saving time is enabled automatically.

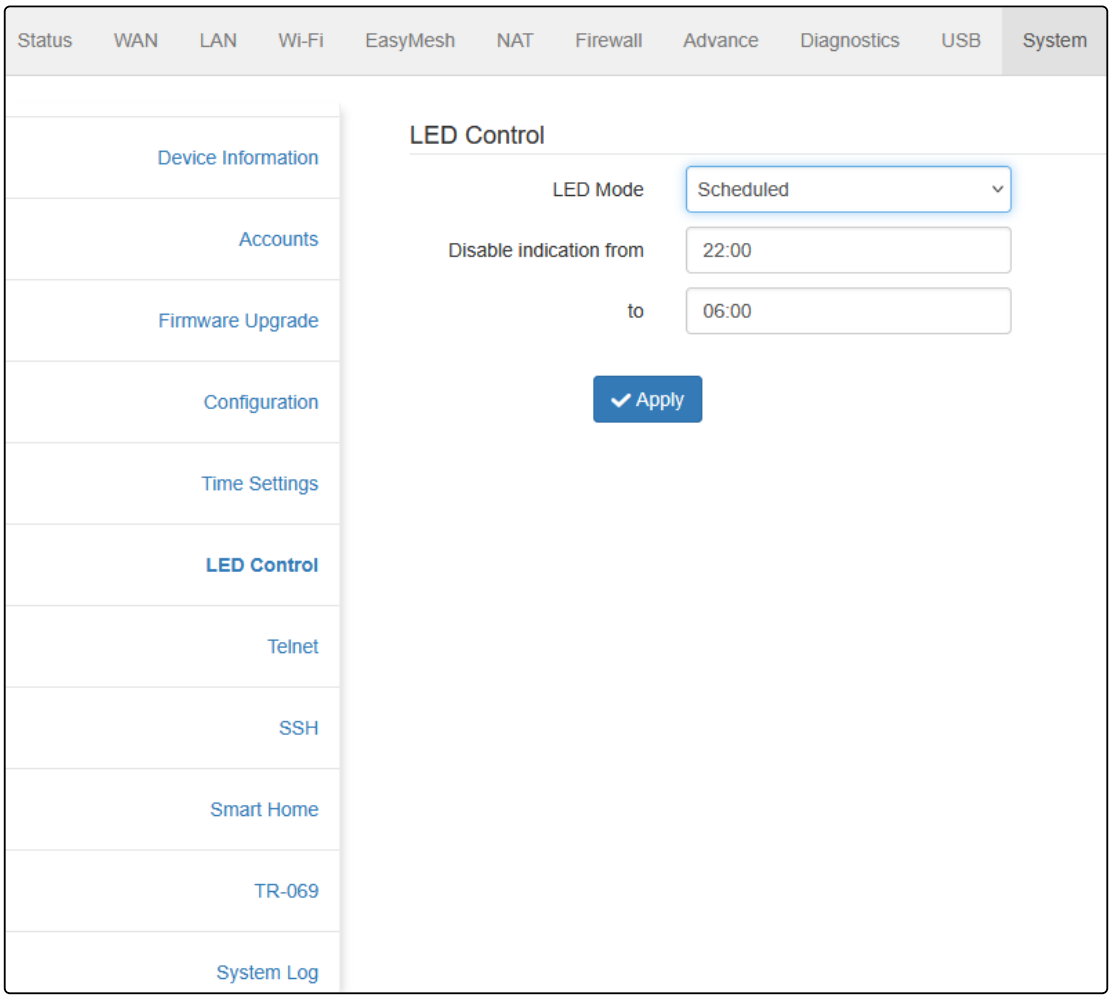
Enable NTP Server Synchronization — when the flag is set, synchronization with the exact time server is enabled.

Get NTP Server IP Address via DHCP — when the flag is set, the NTP server from the DHCP 42 option will be used.

Interface — selection of the interface when setting the time from the WAN side.

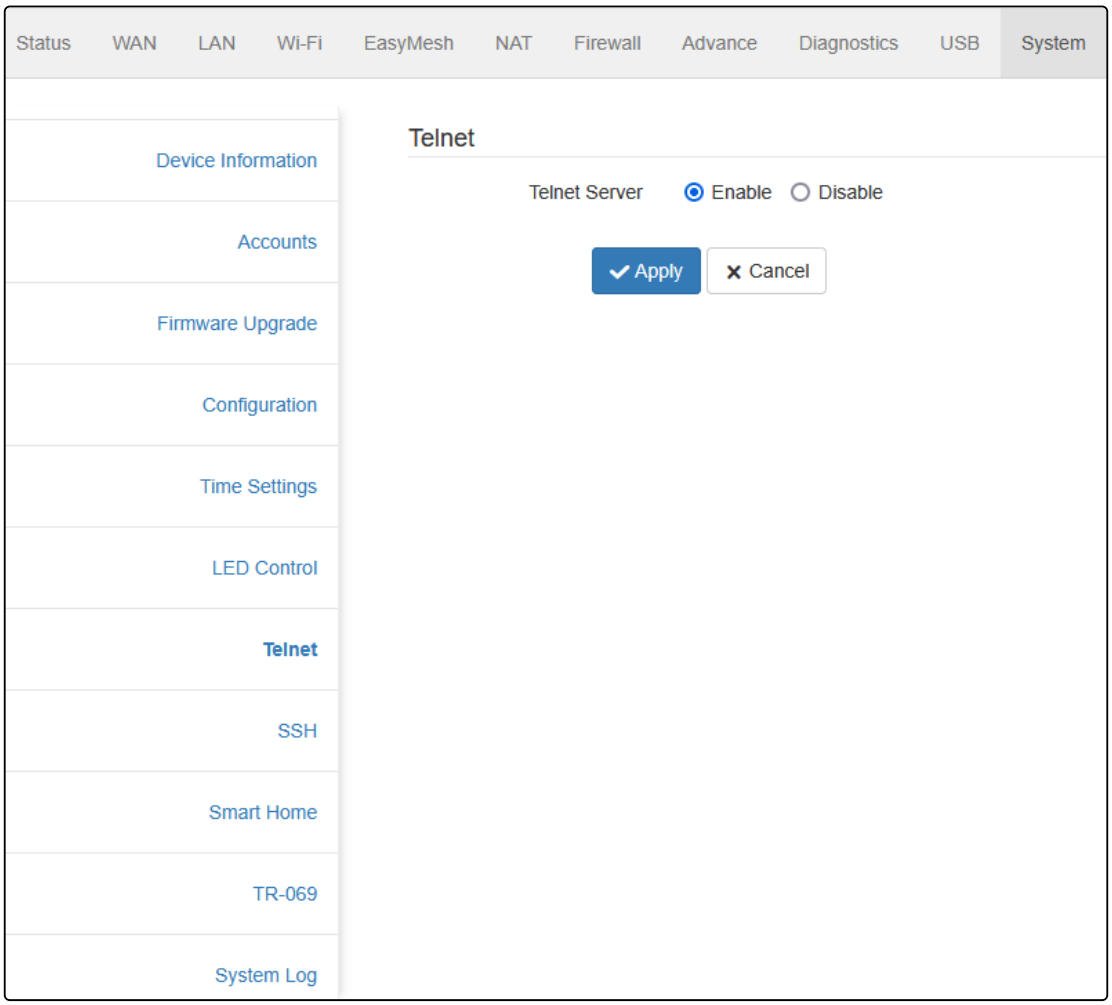
4.6.14.6 LED Control submenu

This submenu allows one to turn on/off the device LED indication or schedule the LED operation.



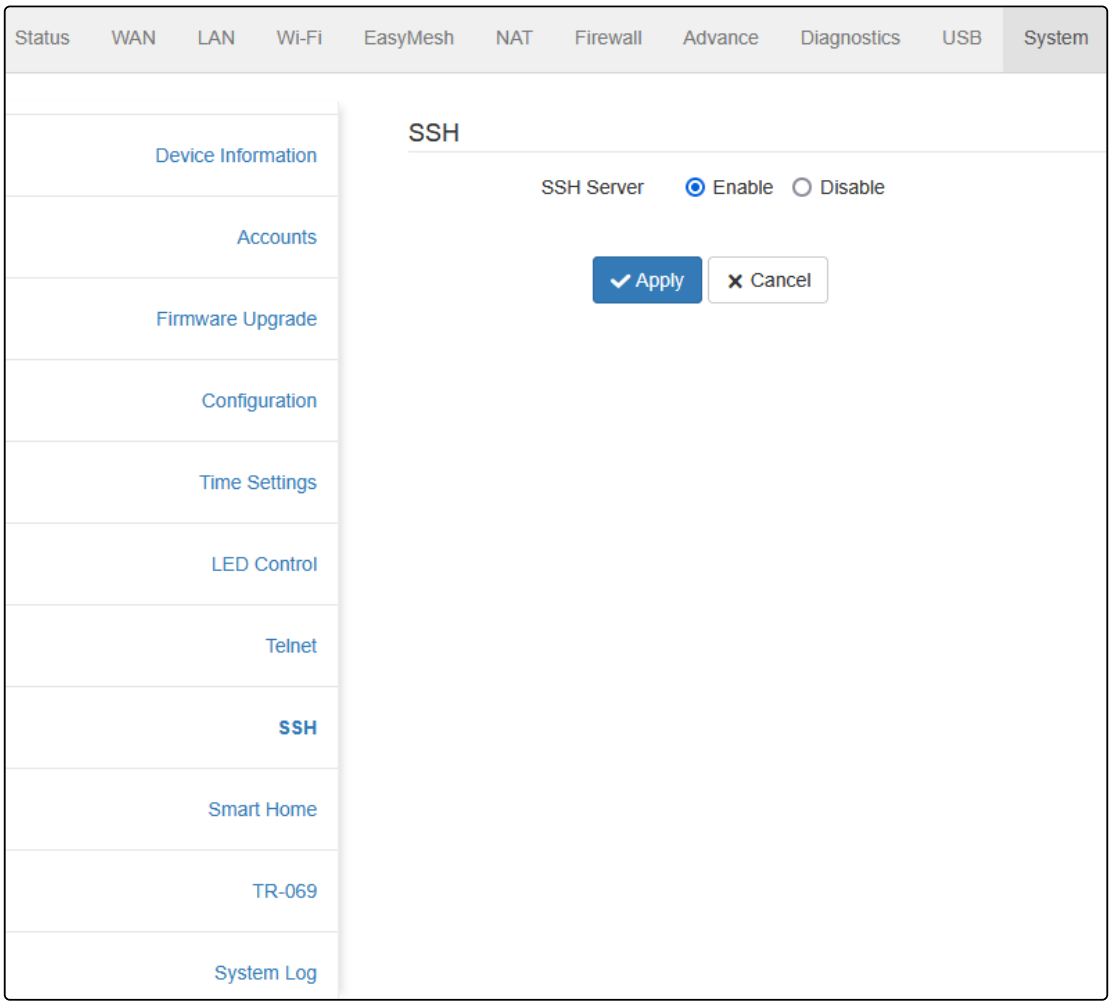
4.6.14.7 Telnet submenu

This submenu allows one to enable/disable the Telnet server feature on the device.



4.6.14.8 SSH submenu

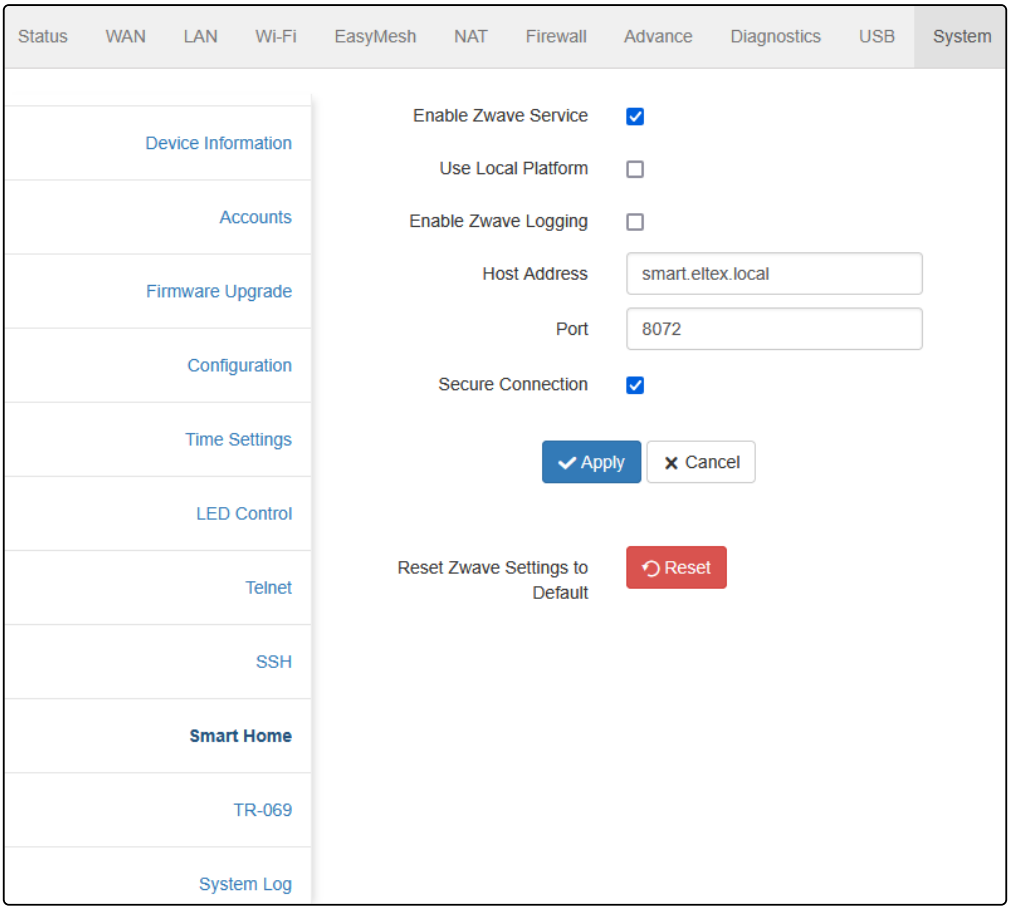
This submenu allows one to enable/disable the SSH server feature on the device.



4.6.14.9 Smart Home submenu

> **[1] Built-in Z-Wave module is supported for RG-5520G-Wax-Z only.**

In this submenu, the Smart Home hub is configured.



Enable Zwave Service[1] — when the flag is set, the Z-Wave hub function is enabled. This feature is enabled by default.

Use Local Platform — when the flag is set, the local platform connected to the device will be used. The default value is smart.eltex.local.

Enable Zwave Logging — when the flag is set, events with the Z-Wave device are saved to the system log.

Host Address — address of the Eltex Smart Control (Eltex SC) server. The default value is smart.eltex.local.

Port — port for communication with the "Eltex Smart Control" platform. The default port is 8072.

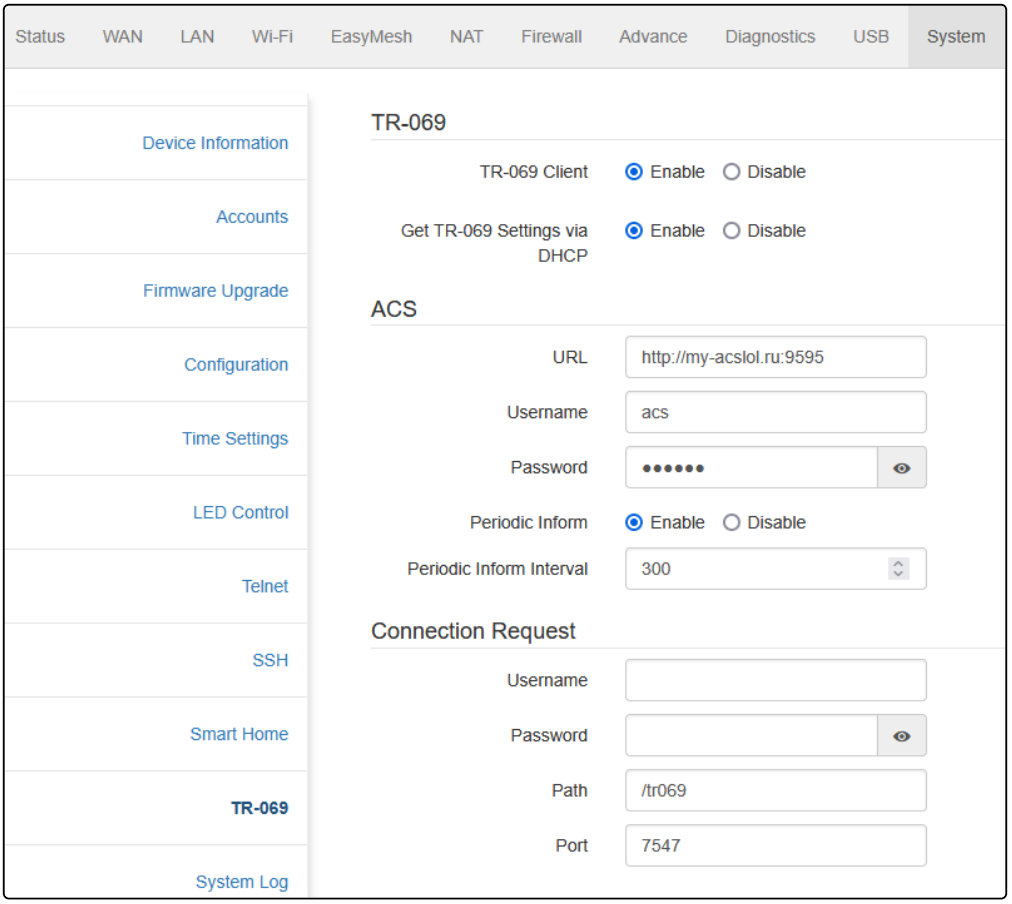
Secure Connection — when the flag is set, the SSL encryption protocol is used. Enabled by default.

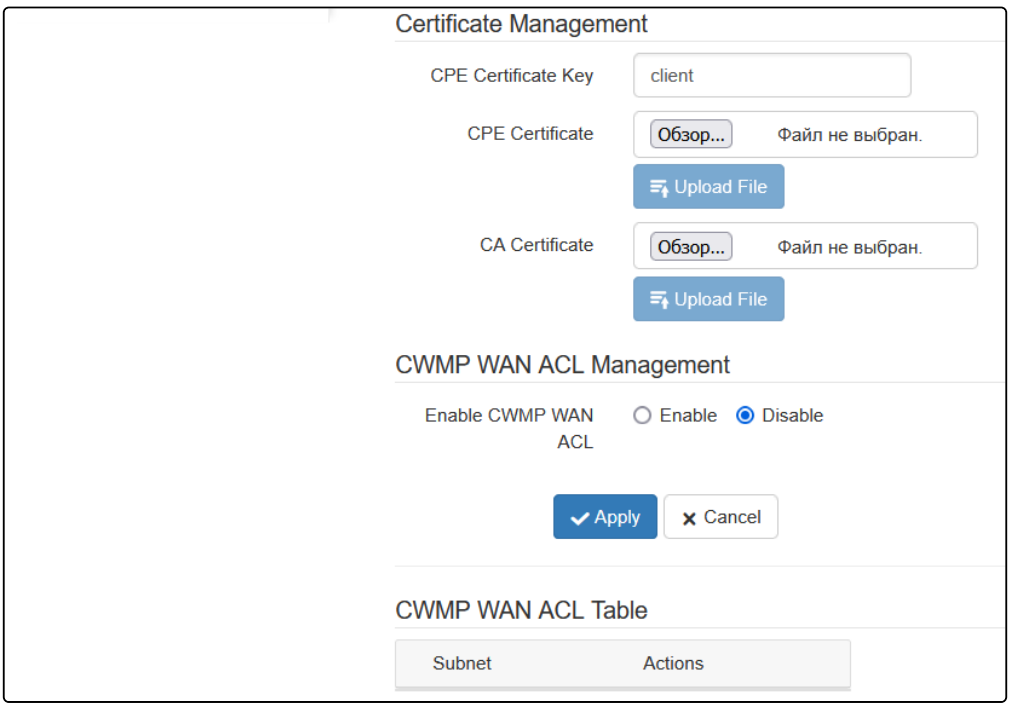
Reset Zwave Settings to Default — restarting the hub and deleting all connected devices using the Z-Wave protocol.

4.6.14.10 TR-069 submenu

> **The "TR-069" submenu is available only under the *Admin* account.**

The protocol for automatic configuration of TR-069 subscriber devices is configured in the "TR-069" submenu.





TR-069 Client — when the flag is set the built-in TR-069 protocol client is enabled, otherwise, it is prohibited (enabled by default).

Get TR-069 Settings via DHCP — when enabled, the TR-069 client will use the parameters received in the DHCP 43 option (the fields below will remain unchanged, but will be ignored by the client if the option is successfully received via DHCP).

ACS

URL — address of the auto-configuration server. The address must be entered in the http://<address>:<port> or https://<address>:<port> format (<address> is the IP address or domain name of the ACS server,

<port> is the port of the ACS server). In the second case, the client will use the secure HTTPS protocol to exchange information with the ACS server.

Username, Password — fields for entering the username and password for client access to ACS server.

Periodic Inform — when the flag is set, the built-in TR-069 client periodically polls the ACS server with an interval equal to the *Periodic Inform Interval field*, in seconds. The purpose of the pollis to detect possible changes in the device configuration.

Connection Request

Username — the user name for the connection request.

Password — password.

Path — the path added to the address for connecting to the device CWMP client.

Certificate Management

It is used to establish a secure connection with the ACS server.

CPE Certificate Key — the certificate key for uploading.

CPE Certificate — select the file to upload the CPE certificate.

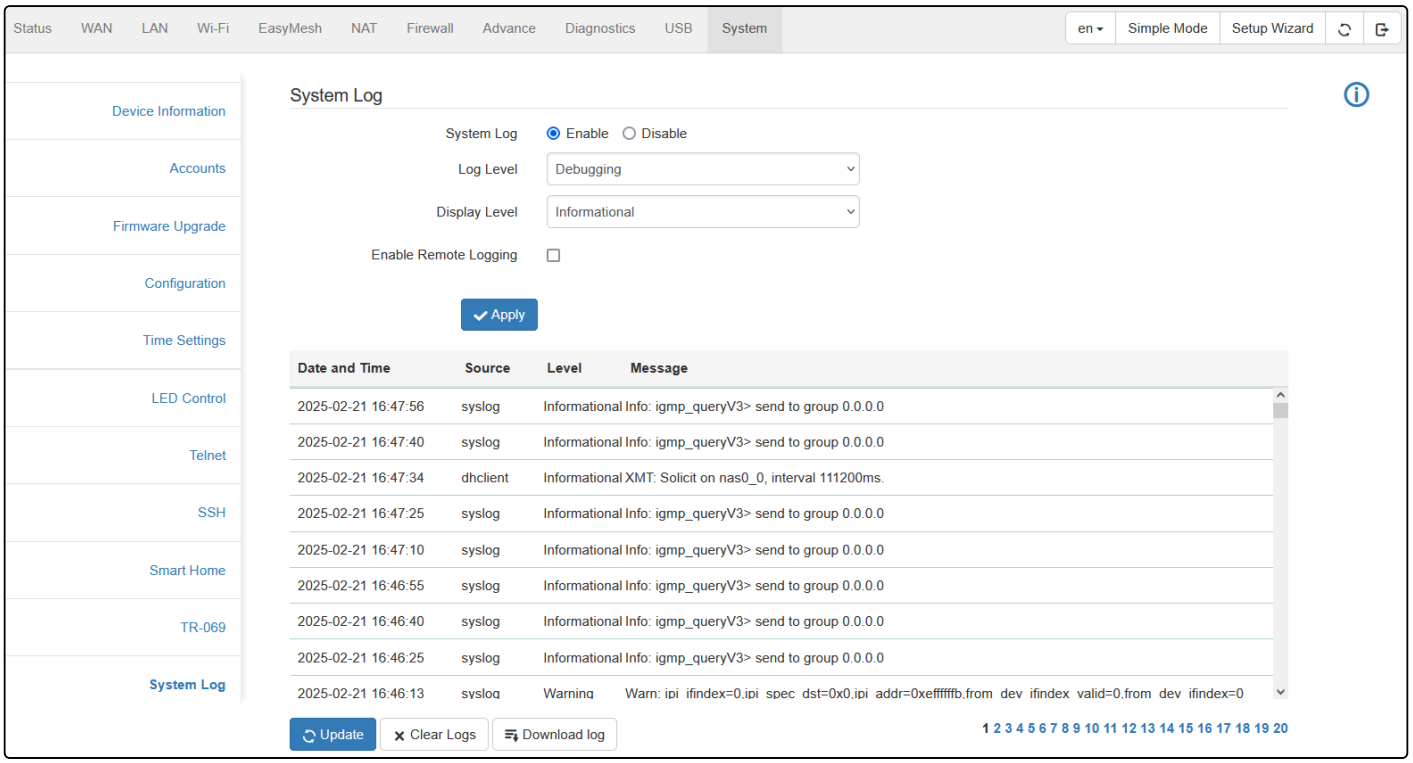
CA Certificate — select the file to upload the CA certificate.

CWMP WAN ACL Management

Enable CWMP WAN ACL — enable access control to CWMP via WAN.

4.6.14.11 System Log submenu

The "System Log" submenu is designed to configure the output of various kinds of system debugging messages in order to detect problems with the device.



System Log — when the flag is set, the logging feature is active.

Log Level — selection of the maximum logging level for system messages.

Display Level — the maximum display level of system messages on the web interface.

Enable Remote Logging — when the flag is set, logs will be downloaded remotely using the Syslog protocol.

Syslog Server — the address of the remote syslog server for downloading system messages.

Apply — click the button to display the contents of the system log at the moment on the current page.

Clear Logs[1] — clear the event log.

Download log — download the current system log to the device in text format.

> [1] **Only when logged in with an *Admin* account.**

TECHNICAL SUPPORT

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

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

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

Official site: https://eltex-co.com/

Download Center: https://eltex-co.com/support/downloads/