

Optical network terminals

# NTU-RG-55xx

User manual

Firmware version 3.4.2

IP address: 192.168.1.1

Username: user

Password: user

## Contents

<b>1</b>	<b>Introduction .....</b>	<b>4</b>
<b>2</b>	<b>Product Description .....</b>	<b>5</b>
2.1	Purpose.....	5
2.2	Models .....	6
2.3	Device Specification.....	6
2.4	Key Specifications.....	8
2.5	Design .....	12
2.6	Light Indication .....	14
2.7	Indication of LAN Interfaces .....	17
2.8	Reboot and Reset to Factory Settings.....	17
2.9	Delivery Package.....	17
<b>3</b>	<b>Installation and connection .....</b>	<b>18</b>
3.1	Operating conditions .....	18
3.2	Installation recommendations.....	18
3.3	Connecting an optical terminal.....	18
3.4	Connecting devices to an optical terminal .....	19
3.4.1	Wired connection .....	19
3.4.2	Wireless connection .....	19
3.4.3	WPS connection .....	19
<b>4</b>	<b>NTU-RG architecture .....</b>	<b>20</b>
<b>5</b>	<b>Device configuration via Web interface. User Access .....</b>	<b>21</b>
5.1	The "Status" menu.....	23
5.1.1	The "Status" submenu.....	23
5.2	The "LAN" menu. LAN interface status information.....	27
5.3	The "WLAN" menu. Wireless network settings .....	28
5.3.1	The "Basic Settings" submenu .....	28
5.3.2	The "Advanced settings" submenu.....	29
5.3.3	The "Security" Submenu. Security Settings .....	30
5.3.4	The "Access Control" Submenu. Access settings .....	31
5.3.5	The "Wi-Fi radar" submenu. Wireless network scanning.....	32
5.3.6	The "WPS" submenu. Easy connection to Wi-Fi network .....	32
5.3.7	The "Status" submenu. Current WLAN status .....	33
5.3.8	The "Wi-Fi Isolation" submenu. Wi-Fi isolation mode setting.....	34
5.4	The "VPN" menu. Virtual private network configuration.....	35

5.4.1	The "L2TP" submenu. L2TP VPN configuration.....	35
5.5	The "Services" menu. Service configuration .....	36
5.5.1	The "Service" menu .....	36
5.5.2	The "Firewall" submenu. Firewall configuration .....	39
5.5.3	The "Samba" submenu.....	44
5.6	The "VoIP" menu. IP telephony settings.....	46
5.6.1	The "VoIP" submenu.....	46
5.7	The "Advance" menu .....	58
5.7.1	The "Advance" submenu .....	58
5.7.2	The "IPv6" submenu. IPv6 configuration.....	61
5.8	The "Diagnostics" menu .....	66
5.8.1	The "Diagnostics" submenu .....	66
5.9	The "Admin" submenu .....	67
5.9.1	The "Admin" submenu. Configuration restore and reset .....	67
5.10	The "Statistics" menu .....	71
5.10.1	The "Statistics" submenu .....	71
<b>6</b>	<b>List of changes.....</b>	<b>73</b>

## 1 Introduction

A GPON is a network of passive optical networks (PON) type. It is one of the most effective state-of-the-art solutions of the last mile issue that enables cable economy and provides information transfer downlink rate up to 2.5 Gbps and uplink rate up to 1.25 Gbps. Being used in access networks, GPON-based solutions allow end users to have access to new services based on IP protocol in addition to more common ones.

The key GPON advantage is the use of one optical line terminal (OLT) for multiple optical network terminals (ONT). OLT converts Gigabit Ethernet and GPON interfaces and is used to connect a PON network with data communication networks of a higher level. ONT device is designed to connect user terminal equipment to broadband access services. It can be used in residential areas and office buildings.

The range of ONT NTU equipment produced by ELTEX comprises of terminals with four UNI interfaces of 10/100/1000Base-T and supports for FXS <sup>1</sup>, Wi-Fi, USB:


- NTU-RG-5520G-Wax, NTU-RG-5521G-Wax.

This user manual describes intended use, main specifications, configuration, monitoring, and firmware update for NTU-RG optical terminals.

### Notes and warnings

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

 Notes contain additional information on device operation or setup.

 Warnings inform users about hazardous conditions which may cause injuries or device damage and may lead to the device malfunctioning or data loss.

 <sup>1</sup> For NTU-RG-5521G-Wax.

## 2 Product Description

### 2.1 Purpose

*NTU-RG GPON ONT* (Gigabit Passive Optical Network) devices represent high-performance user terminals designed to establish a connection with upstream passive optical network equipment and to provide broadband access services to the end user. GPON connection is established through the PON interface, while Ethernet interfaces are used for connection of terminal equipment.

The key GPON advantage is the optimal use of bandwidth. This technology is considered as the next step in provisioning of new high-speed Internet applications at home and office. Being developed for network deployment inside houses or buildings, these ONT devices provide robust connection with high throughput and at long distances for users living and working at remote apartment and office buildings.

An integrated router allows local network equipment to be connected to a broadband access network. The terminals protect PCs from DoS and virus attacks with the help of firewall and filter packets to control access based on ports and MAC/IP addresses of source and target. Users can configure a home or office web site by adding a LAN port into DMZ. Parental Control enables filtration of undesired web sites and blocks domains. Virtual private network (VPN) provides mobile users and branch offices with a protected communication channel for connection to a corporate network.

FXS port enables IP telephony and provides various useful features such as display of caller ID, three-way conference call, phone book, and speed dialling. This makes dialling and call pick-up user friendly.

USB ports can be used for USB-enabled devices (USB flash drives, external HDD).

NTU-RG-5520G-Wax, NTU-RG-5521G-Wax allow Wi-Fi clients to be connected using IEEE 802.11a/b/g/n/ac/ax standard. 802.11ax standard support ensures data transfer rate of 2402 Mbps and allows wireless network to be used for delivery of modern high-speed services to client equipment. Two integrated Wi-Fi network controllers enable simultaneous 2.4 GHz and 5 GHz dual-band operation.

## 2.2 Models

NTU-RG series devices are designed to support various interfaces and features, see [Table 1](#) .

Table 1 – Models

Model name	WAN	LAN	FXS	Wi-Fi	USB
NTU-RG-5520G-Wax	1× GPON	4 × 1Gigabit	-	802.11ax, 2*2 – 574 Mbps – 2.4 GHz 802.11ax, 2*2 – 2402 Mbps – 5 GHz	1 × USB 3.0
NTU-RG-5521G-Wax	1 × GPON	4 × 1Gigabit	1	802.11ax, 2*2 – 574 Mbps – 2.4 GHz 802.11ax, 2*2 – 2402 Mbps – 5 GHz	1 × USB 3.0

## 2.3 Device Specification

**Device is equipped with the following interfaces:**

- 1 × RJ-11 port to connect network devices (FXS) for NTU-RG-5521-Wax;
- 1 × PON SC/APC port for connection to provider's network (WAN);
- Ethernet RJ-45 LAN ports for connection of network devices (LAN):
  - 4 ports of RJ-45 10/100/1000Base-T.
- Wi-Fi transceiver:
  - 802.11a/b/g/n/ac/ax.
- 1 × USB 3.0 port for external USB or HDD storages.

The terminal uses an external 220 V/12 V, 2 A power adapter.

**The device supports the following functions:**

- *Network functions:*
  - bridge or router operation mode;
  - PPPoE (auto, PAP, CHAP, MSCHAP authorization);
  - IPoE (DHCP-client and static);
  - static IP address and DHCP (DHCP client on WAN side, DHCP server on LAN side);
  - Multicast traffic transmission via Wi-Fi;
  - DNS (Domain Name System);
  - DynDNS (Dynamic DNS);
  - UPnP (Universal Plug and Play);
  - IPsec (IP Security);
  - NAT (Network Address Translation);
  - Firewall;
  - NTP (Network Time Protocol);
  - QoS;
  - IGMP snooping;
  - IGMP proxy;
  - Parental Control;
  - Storage service;
  - SMB, FTP;
  - Print Server (supported only for LAN);
  - VLAN in accordance with IEEE 802.1Q.
- *Wi-Fi:*
  - Support for IEEE 802.11a/b/g/n/ac/ax standards;
  - Simultaneous dual-band operation: 2.4 GHz and 5 GHz;
  - Support for EasyMesh.

- *VoIP*<sup>1</sup>:
  - SIP protocol;
  - Audio codecs: G.729 (A), G.711(A/U), G.723.1;
  - ToS for RTP packets;
  - ToS for SIP packets;
  - Echo cancellation (G.164 and G.165 guidelines);
  - Voice activity detection (VAD);
  - Comfort noise generator (CNG);
  - DTMF signal detection and generation;
  - DTMF transmission (INBAND, RFC2833, SIP INFO);
  - Fax transmission: G.711, T.38;
  - Caller ID display.
- *Value added services (VAS)*<sup>1</sup>:
  - Call Hold;
  - Call Transfer;
  - Call Waiting;
  - Forward unconditionally;
  - Forward on "no answer";
  - Forward on "busy";
  - Caller ID Display for ETSI FSK;
  - Anonymous calling;
  - MWI;
  - Anonymous call blocking;
  - Call Barring;
  - DND (Do not disturb).
- *Firmware update*:
  - web interface, TR-069, OMCI.
- *Remote monitoring, configuration, and setup*:
  - TR-069; web interface; OMCI; Telnet.

 <sup>1</sup> Only for NTU-RG-5521G-Wax.

The figure below illustrates the application scheme of NTU-RG.

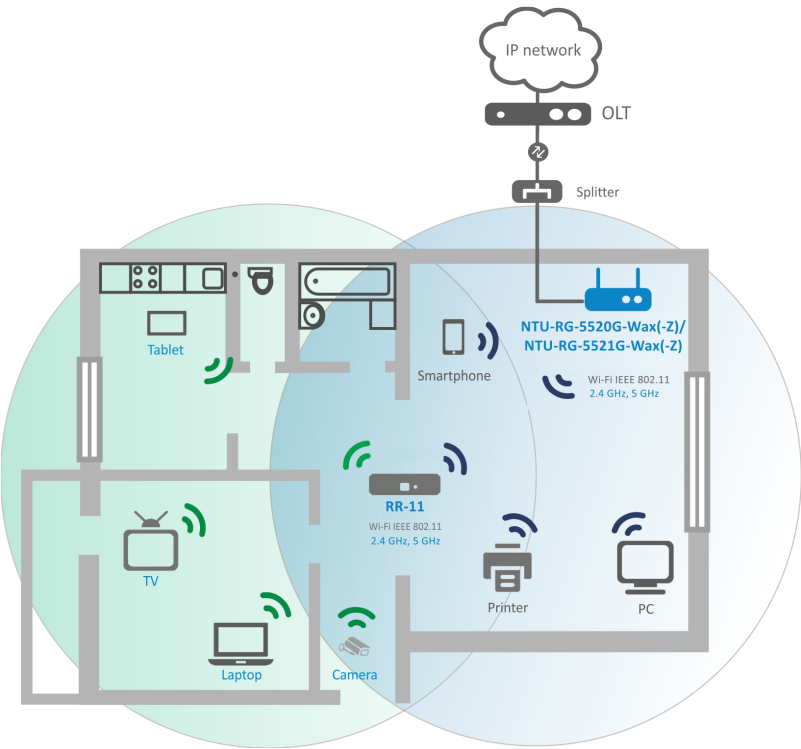


Figure 1 – NTU-RG-5520G-Wax, NTU-RG-5521G-Wax application diagram

2.4 Key Specifications

Table 2 shows main specifications of the terminals:

Table 2 – Main Specifications

VoIP protocols

Supported protocols	SIP
---------------------	-----

Audio codecs

Codecs	G.729, annex A G.711(A/μ) G.723.1 (5.3 Kbps) Fax transmission: G.711, T.38
--------	---

Parameters of Ethernet LAN interfaces

Number of interfaces	4
Connector type	RJ-45
Data transfer rate, Mbps	Autonegotiation, 10/100/1000 Mbps, duplex/half-duplex



Standards	IEEE 802.3i 10Base-T Ethernet IEEE 802.3u 100Base-TX Fast Ethernet IEEE 802.3ab 1000Base-T Gigabit Ethernet IEEE 802.3x Flow Control IEEE 802.3 NWay auto-negotiation
-----------	---

### Parameters of PON interface

Number of interfaces	1
Standards	ITU-T G.984.x Gigabit-capable passive optical networks (GPON) ITU-T G.988 ONU management and control interface (OMCI) specification IEEE 802.1Q Tagged VLAN IEEE 802.1P Priority Queues IEEE 802.1D Spanning Tree Protocol
Connector type	SC/APC in accordance with ITU-T G.984.2, ITU-T G.984.5 Filter, FSAN Class B+, SFF-8472
Transmission medium	Fiber optical cable SMF: 9/125, G.652
Splitting ratio	Up to 1:128
Maximum range of coverage	20 km
Transmitter:	1310 nm
• Upstream connection speed	1244 Mbps
• Transmitter power	from +0,5 to +5 dBm
• Optical spectrum width (RMS)	1 nm
Receiver:	1490 nm
• Downstream connection speed	2488 Mbps
• Receiver sensitivity	from -8 to -28, BER $\leq 1.0 \times 10^{-10}$
Receiver optical congestion	-8 dBm

**Parameters of subscriber analogue ports**

Number of ports	NTU-RG-5521G-Wax
	1 FXS port
Loop resistance	Up to 1800 $\Omega$
Call reception	Pulse/frequency (DTMF)
Caller ID display	Yes

**Wi-Fi interface parameters**

Standard	802.11a/b/g/n/ac/ax
Frequency range	2400 ~ 2483,5 MHz, 5150 ~ 5350 MHz, 5650 ~ 5850 MHz Simultaneous Dual Band
Modulation	CCK, BPSK, QPSK, 16 QAM, 64 QAM, 256 QAM
Data transfer rate, Mbps	<ul style="list-style-type: none"> <li>– 802.11b: 1; 2; 5.5 and 11 Mbps</li> <li>– 802.11a: 6, 9, 12, 18, 24, 36, 48 and 54 Mbps</li> <li>– 802.11g: 6, 9, 12, 18, 24, 36, 48 and 54 Mbps</li> <li>– 802.11n: 300 Mbps (20 MHz)</li> <li>– 802.11ac: 866 Mbps (80 MHz)</li> <li>– 802.11ax: 2402 Mbps (160 MHz)</li> </ul>
Maximum transmitter output power	<ul style="list-style-type: none"> <li>– 802.11b (11 Mbps): 21 dBm</li> <li>– 802.11a (54 Mbps): 18 dBm</li> <li>– 802.11g (54 Mbps): 18 dBm</li> <li>– 802.11n (MCS7): 18 dBm</li> <li>– 802.11ac (MCS0): 19 dBm</li> <li>– 802.11ax (MCS0): 20 dBm</li> <li>– 802.11ax (MCS11): 16 dBm</li> </ul>
MAC protocol	CSMA/CA model of ACK 32 MAC
Security	64/128-bit WEP encryption; WPA, WPA2 802.1x AES & TKIP
MIMO	2.4 GHz- 2x2, 5 GHz - 2x2
Operating temperature range	from +5 to +40°C

**Control**

Local control	Web interface
Remote control	Telnet, TR-069, OMCI

Firmware update	OMCI, TR-069, HTTP
Access restriction	By password

### General parameters

Power supply	12 V, 2 A power adapter
Max. power consumption	18 W
Operating temperature range	From +5 to +40°C
Relative humidity	Up to 80%
Dimensions	230 × 37 × 140 mm
Weight	0.383 kg
Lifetime	no less than 5 years

2.5 Design

Subscriber terminals are designed as desktop devices in plastic housing.

The rear panel layout of NTU-RG-5520G-Wax is depicted in Figure 2 below.

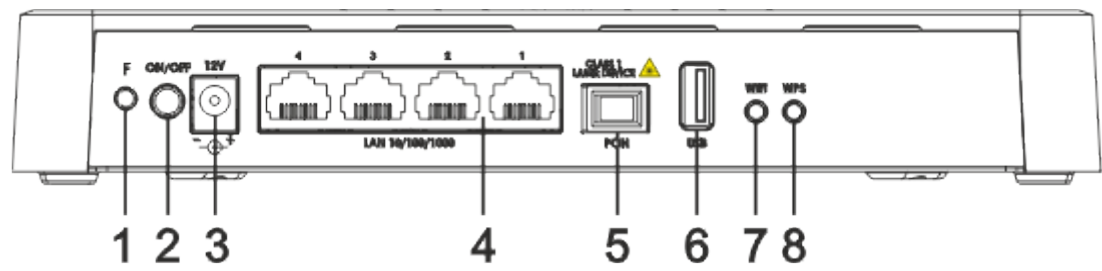


Figure 2 – NTU-RG-5520G-Wax rear panel layout

The connectors and controls located on the NTU-RG-5520G-Wax rear panel are listed in Table 3 below.

Table 3 – Description of the connectors and controls on the rear panel

Nº	Rear panel element	Description
1	F	Function button to reboot the device and reset to factory settings
2	On/Off	Power button
3	12V	Power adapter connector
4	LAN 10/100/1000 1..4	4 RJ-45 ports for connection to network devices
5	PON	SC port (socket) for PON with GPON interface
6	USB	Connector for external drives and other USB devices
7	Wi-Fi	Wi-Fi on/off button
8	WPS	Button for automatic secure connection to Wi-Fi network on the device

The rear panel layout of NTU-RG-5521G-Wax is depicted in Figure 3 below.

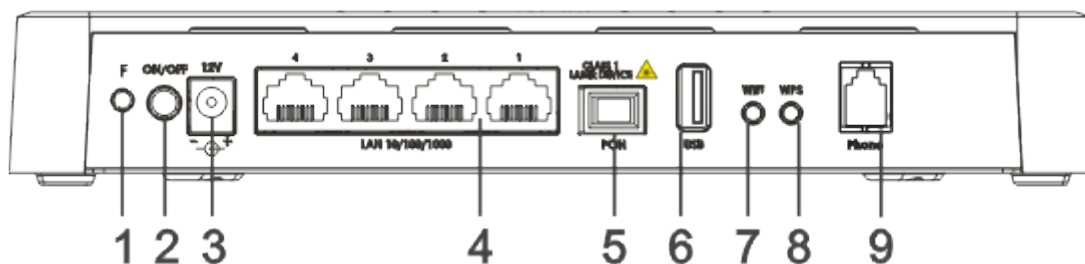


Figure 3 – NTU-RG-5520G-Wax rear panel layout

The connectors and controls located on the NTU-RG-5520G-Wax rear panel are listed in Table 4 below.

Table 4 – Description of the connectors and controls on the rear panel

Nº	Rear panel element	Description
1	<b>F</b>	Function button to reboot the device and reset to factory settings
2	<b>On/Off</b>	Power button
3	<b>12V</b>	Power adapter connector
4	<b>LAN 10/100/1000 1..4</b>	4 RJ-45 ports for connection to network devices
5	<b>PON</b>	SC port (socket) for PON with GPON interface
6	<b>USB</b>	Connector for external drives and other USB devices
7	<b>Wi-Fi</b>	Wi-Fi on/off button
8	<b>WPS</b>	Button for automatic secure connection to Wi-Fi network on the device
9	<b>Phone</b>	RJ-11 connector for analogue phone connection

## 2.6 Light Indication

Figure 4 shows NTU-RG-5520G-Wax top panel layout.

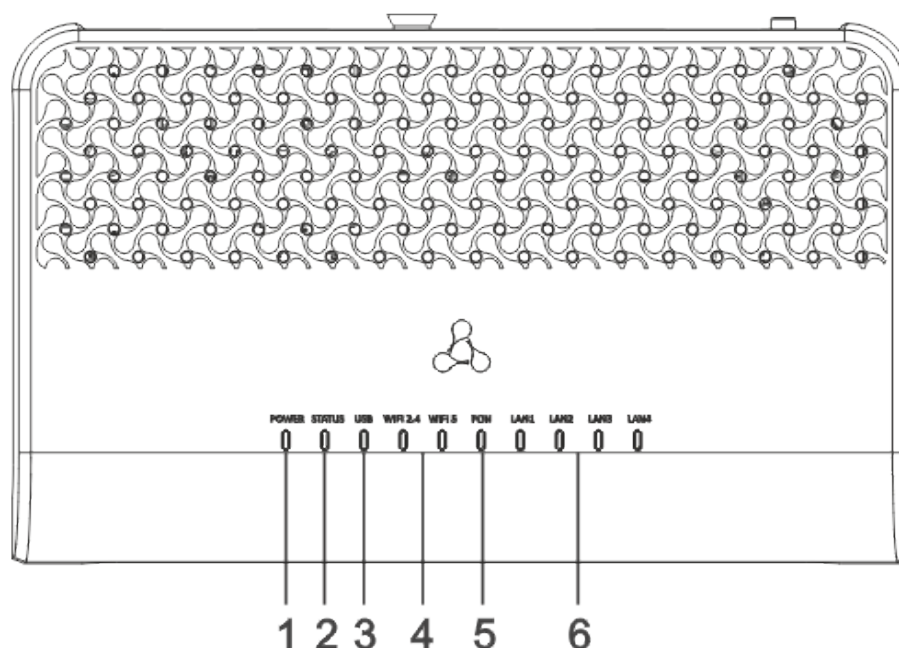


Figure 4 – NTU-RG-5520G-Wax top panel layout

The LED indicators located on the front panel show the current state of the device. The list of indicator states is shown in Table 5 below.

Table 5 – Description of NTU-RG-5520G-Wax top panel LEDs

Nº	Top panel element	LED status	Description
1	<b>Power</b> – device power and activity status indicator	off	device is disconnected from the power source or faulty
		red	device startup is in progress
		green	device startup is completed, the current device configuration differs from the default one
		orange	device startup is completed, the default configuration is set
2	<b>Status</b> – status indicator	off	Internet interface is not configured
		green	device is ready for operation, Internet connection is established
		flashes green slowly	device firmware update is in progress
		flashes green rapidly	device booting/connection to the Internet is being established

No	Top panel element	LED status	Description
3	<b>USB</b> – USB port activity indicator	off	USB device is not connected
		on	USB device is connected
		flashes	transmitting data via USB
4	<b>Wi-Fi 2.4</b> – Wi-Fi activity indicator for 2.4 GHz <b>Wi-Fi 5</b> – Wi-Fi activity indicator for 5 GHz	green	Wi-Fi network is active
		flashes	transmitting data via Wi-Fi
		off	Wi-Fi network is inactive
5	<b>PON</b> – optical interface activity indicator	off	device booting
		green	connection between optical line terminal and the device has been established
		flashes green	connection between optical line terminal and the device has been established (the device is not activated)
		flashes red	no signal from optical line terminal
6	<b>LAN1..4</b> – Ethernet port activity indicator	green	established 10/100 Mbps connection
		orange	established 1000 Mbps connection
		flashes	transferring data packets

The front panel of NTU-RG-5521G-Wax is shown in Figure 5 below.

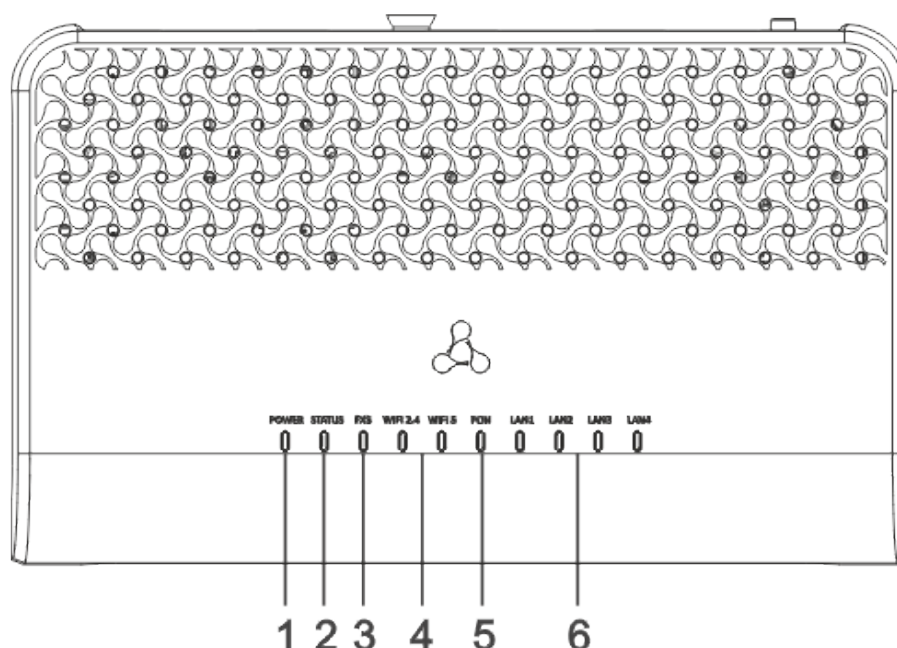


Figure 5 – NTU-RG-5521G-Wax front panel layout

The LED indicators located on the front panel show the current state of the device. The list of indicator states is shown in Table 6.

Table 6 – Description of NTU-RG-5521G-Wax front panel LEDs

No	Front panel element	LED status	Description
1	<b>Power</b> – device power and activity status indicator	off	device is disconnected from the power source or faulty
		red	device startup is in progress
		green	device startup is completed, the current device configuration differs from the default one
		orange	device startup is completed, the default configuration is set
2	<b>Status</b> – status indicator	off	Internet interface is not configured
		green	device is ready for operation, Internet connection is established
		flashes green slowly	device firmware update is in progress
		flashes green rapidly	device booting/connection to the Internet is being established
3	<b>FXS</b> – FXS port activity indicator	off	SIP agent is not configured/not registered/off
		on	SIP agent is successfully registered
		flashes	off hook/phone call
4	<b>Wi-Fi 2.4</b> – Wi-Fi activity indicator for 2.4 GHz	green	Wi-Fi network is active
	<b>Wi-Fi 5</b> – Wi-Fi activity indicator for 5 GHz	flashes	transmitting data via Wi-Fi
		off	Wi-Fi network is inactive
5	<b>PON</b> – optical interface activity indicator	off	device booting
		green	connection between optical line terminal and the device has been established
		flashes green	connection between optical line terminal and the device has been established (the device is not activated)
		flashes red	no signal from optical line terminal
6	<b>LAN1..4</b> – Ethernet port activity indicator	green	established 10/100 Mbps connection
		orange	established 1000 Mbps connection
		flashes	transferring data packets



## 2.7 Indication of LAN Interfaces

Table 7 below lists operation modes shown by LAN ports LEDs located on the rear panel of the device.

Table 7 – Light Indication of LAN Interfaces

Operation modes	Yellow LED	Green LED
Port operates in 1000BASE-T mode, data transfer is inactive	solid on	off
Port operates in 1000BASE-T mode, data transfer is active	flashes	off
Port operates in 10/100BASE-TX, data transfer is inactive	off	solid on
Port operates in 10/100BASE-TX, data transfer is active	off	flashes

## 2.8 Reboot and Reset to Factory Settings

For device reboot, press the "F" button on the device rear panel once.

In order to reset the device to the factory settings, press the "F" button and hold it for 7-10 seconds until the indicator **Power** glows red and all other LEDs go out.

Factory settings for IP address are: LAN – 192.168.1.1, subnet mask – 255.255.255.0. Access can be provided from LAN 1, LAN 2, LAN 3 and LAN 4 ports.

## 2.9 Delivery Package


NTU-RG-5520G-Wax, NTU-RG-5521G-Wax standard delivery package includes:

- NTU-RG optical network terminal;
- 220V/12V, 2A 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 2.4 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 an optical terminal

1. Connect the optical cable provided by your Internet provider to the PON connector.
2. Connect the optical terminal to a 220 V network via a power adapter. Turn on the device by pressing the "On/Off" button. Wait until the device is fully loaded, which may take 30–120 seconds.
3. Make sure that the following indicators are constantly on: POWER, WLAN5, WLAN2.4, PON, and Status. This means that the device is connected correctly and running.

## 3.4 Connecting devices to an optical terminal

### 3.4.1 Wired connection

1. Using an Ethernet cable, connect the LAN port Port1/Port2 of the optical terminal and the Ethernet port of the computer.
2. Using an Ethernet cable, connect the LAN port Port3/Port4 (defined by your provider) of the optical terminal and the Ethernet port of the set-top box or other devices.

### 3.4.2 Wireless connection

Connect device (laptop, smartphone, etc.) to the terminal'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 terminal.
3. Select this network and enter the password specified on the bottom panel of the terminal.

### 3.4.3 WPS connection

The device supports connecting the client to the terminal'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 or side panel of the terminal (depending on the model) for one second.

The client will connect to the terminal automatically.

Connecting the client device to the terminal 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 terminal.

- ✓ The WPS feature is enabled by default. One can disable the feature in the web interface in the "WLAN" → "WPS" submenu.

## 4 NTU-RG architecture

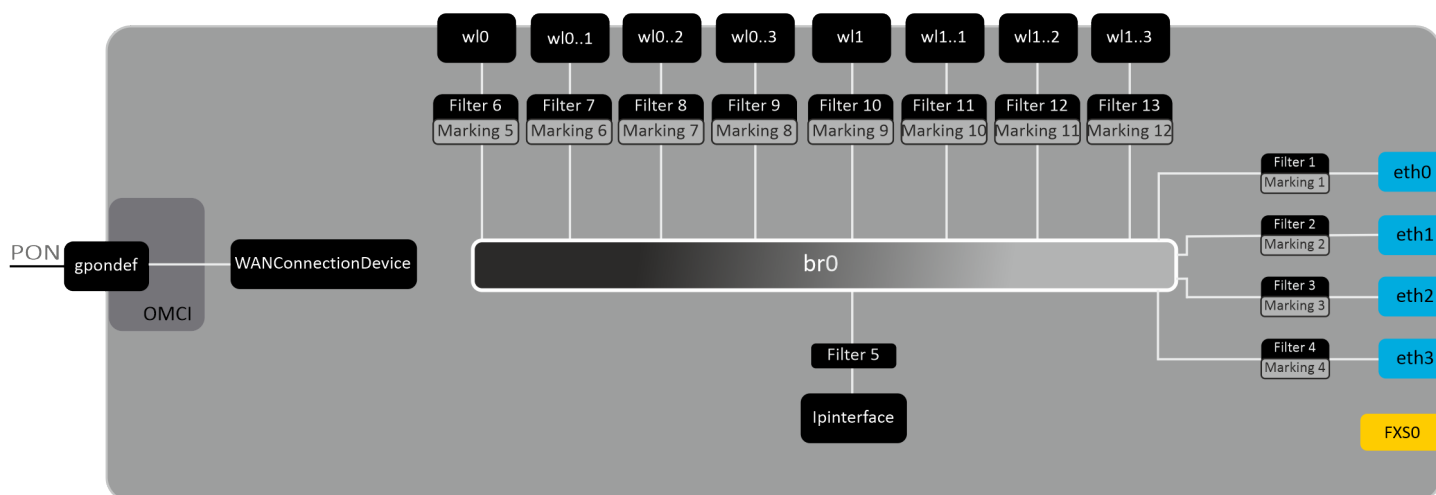


Figure 6 – Logical Architecture of a Device with Factory Settings<sup>1</sup>

 <sup>1</sup> FXS0 interface is available for NTU-RG-5521G-Wax only.

### Main Components of the Device:

- **Optical receiver/transmitter (SFF module)** for conversion of an optical signal into an electric one;
- **Processor (PON chip)** which converts Ethernet and GPON interfaces;
- **Wi-Fi modules** for wireless interfaces of the device.

A device with factory (initial) settings have the following logical blocks (see Figure 6):

- Br0;
- eth0...3;
- FXS0;
- wl0, wl0.1, wl0.2, wl0.3, wl1, wl1.1, wl1.2, wl1.3;
- IPInterface.

**Br0** block here is used to combine LAN ports into a single group.

**Eth0..3** blocks physically represent Ethernet ports with RJ-45 connector for connection of PC, STB, and other network devices. They are logically included into **br0** block.

**FXS0** block is a port with RJ-11 connectors for connection of analogue phone. It is logically included into the Voice block. The Voice block can be controlled through web interface or remotely with ACS server via TR-069 standard. The block specifies VoIP service parameters (SIP server address, phone number, VAS, etc.).

**wl0, wl0.1...wl1.3** blocks for Wi-Fi modules connection. wl0 blocks are interfaces for 2.4 GHz operation, wl1 ones – for 5 GHz operation.

**Filter** and **Marking** blocks enable inclusion of local interfaces into a single group (to **br0** block). They deal with the traffic transmission rules, **Filter** blocks are responsible for the incoming traffic on the interface, **Marking** blocks are responsible for the outgoing one.

**IPInterface** block is a logical entity on which IP address providing the access in LAN and DHCP server distributing addresses to clients are located.

## 5 Device configuration via Web interface. User Access

### Getting Started

To configure the device, it is necessary to connect to it through Web browser:

1. Open a web browser (program for viewing hypertext documents), for example, Firefox, Google Chrome etc.
2. Enter the device IP address in the browser address line.

✓ Default IP address of the device – **192.168.1.1**, subnet mask – **255.255.255.0**

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

3. Enter your username and password.

✓ Username: **user**, password: **user**.

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

### Password changing

To prevent unauthorized access to device, it is recommended to change password. To change the password go to the "Admin" menu, "Password" submenu. Enter the current password in the "Old Password" field and the new password in the "New Password" and "Confirmed password" fields. To save the changes, click the "Apply Changes" button.

Status	LAN	WLAN	WAN	Services	Advance	Diagnostics	Admin	Statistics								
<div> <div> <b>Admin</b> <ul style="list-style-type: none"> <li>&gt; GPON Settings</li> <li>&gt; OMCI Information</li> <li>&gt; Commit/Reboot</li> <li>&gt; Multi-lingual Settings</li> <li>&gt; Backup/Restore</li> <li>&gt; <b>Password</b></li> </ul> </div> <div> <h3>Password Configuration</h3> <table> <tr> <td>Username:</td> <td>admin ▾</td> </tr> <tr> <td>Old Password:</td> <td>••••••••••</td> </tr> <tr> <td>New Password:</td> <td><input type="password"/></td> </tr> <tr> <td>Confirmed Password:</td> <td><input type="password"/></td> </tr> </table> <div> <input type="button" value="Apply Changes"/> <input type="button" value="Reset"/> </div> </div> </div>									Username:	admin ▾	Old Password:	••••••••••	New Password:	<input type="password"/>	Confirmed Password:	<input type="password"/>
Username:	admin ▾															
Old Password:	••••••••••															
New Password:	<input type="password"/>															
Confirmed Password:	<input type="password"/>															

## Main elements of the web interface

General view of the device configuration window is depicted below.

The screenshot displays the web interface for the ELTEX NTU-RG-5520G-Wax device. The top header shows the ELTEX logo, the device model, and the firmware version (3.4.2.4560). The interface is divided into four numbered parts:

- 1**: The top navigation tabs (Status, LAN, WLAN, WAN, Services, Advance, Diagnostics, Admin, Statistics).
- 2**: The left sidebar navigation tree (Status, Device, IPv6, PON).
- 3**: The main settings window for the selected submenu (Device Status).
- 4**: Reboot and log out buttons in the top right corner.

The **Device Status** page shows the current status and some basic settings of the device. The table below lists the system information:

System	
Manufacturer	ELTEX
Model	NTU-RG-5520G-Wax
Uptime	1 day, 46 min
Hardware Version	...
Serial Number	...
PON Serial	...
Bootloader Version	...
Bootloader CRC32 sum	...
Current FW CRC32 sum	...
Backup FW CRC32 sum	...
CPU Usage	4%
Memory Usage	34%
Image 1 Firmware Version	...
Image 2 Firmware Version	...
IPv4 Default Gateway	...
IPv6 Default Gateway	...
DNS	...

The user interface window can be divided into 4 parts:

1. The device settings menu tabs.
2. The navigation tree on the device settings submenus.
3. The main settings window for the selected submenu.
4. Reboot and log out buttons.

## 5.1 The "Status" menu

### 5.1.1 The "Status" submenu

#### 5.1.1.1 The "Device" submenu. Device general information

This section displays general information about the device, the main parameters of the LAN and WAN interfaces.

*Status → Status → Device status*

Device Status	
This page shows the current status and some basic settings of the device.	
System	
Manufacturer	ELTEX
Model	NTU-RG-5520G-Wax
Uptime	1 day, 46 min
Hardware Version	1.0
Serial Number	12345678901234567890
PON Serial	12345678901234567890
Bootloader Version	1.0.0.0
Bootloader CRC32 sum	12345678901234567890
Current FW CRC32 sum	12345678901234567890
Backup FW CRC32 sum	12345678901234567890
CPU Usage	4%
Memory Usage	34%
Image 1 Firmware Version	1.0.0.0
Image 2 Firmware Version	1.0.0.0
IPv4 Default Gateway	
IPv6 Default Gateway	
DNS	

### System

- *Manufacturer* – manufacturer;
- *Model* – device model;
- *Uptime* – device uptime;
- *Hardware Version* – hardware version;
- *Serial Number* – device serial number;
- *PON Serial* – device serial number in the PON network;
- *Bootloader Version* – firmware bootloader version;
- *Bootloader CRC32 sum* – firmware bootloader checksum;
- *Current FW CRC32 sum* – current firmware image checksum;
- *Backup FW CRC32 sum* – backup firmware image checksum;
- *CPU Usage* – CPU utilization percent;
- *Memory Usage* – memory utilization percent;
- *Image 1 Firmware Version* – current firmware version;
- *Image 2 Firmware Version* – backup firmware version;
- *IPv4 Default Gateway* – IPv4 default gateway;
- *IPv6 Default Gateway* – IPv6 default gateway;
- *DNS* – DNS server name.

LAN Configuration							
IP Address		192.168.1.1					
Subnet Mask		255.255.255.0					
DHCP Server		Enabled					
MAC Address		XXXXXXXXXX					

LAN Port Status			
Name	Status	Speed	Mode
LAN1	NoLink	Auto	Auto
LAN2	Up	100	Full
LAN3	NoLink	Auto	Auto
LAN4	NoLink	Auto	Auto

Wi-Fi Status						
SSID	Band	Channel	Bandwidth	Encryption	Standards	Clients
ELTX-2.4GHz_WiFi_321A	2.4G	1	40MHz	WPA2 Mixed	b/g/n/ax	0
ELTX-5GHz_WiFi_321A	5G	36	160MHz	WPA2 Mixed	a/n/ac/ax	0

WAN Configuration							
Interface	VLAN ID	MAC	Connection Type	Protocol	IP Address / Subnet Mask	Gateway	Status

OMCI VLAN	
GEM Port	VLAN ID

L2TP Configuration				
Interface	Protocol	Local IP Address	Remote IP Address	Status

Refresh

### LAN Configuration

- *IP Address* – device IP address;
- *Subnet Mask* – device subnet mask;
- *DHCP Server* – DHCP server state;
- *MAC Address* – device MAC address.

### LAN Port Status

- *Name* – LAN port name;
- *Status* – LAN port status;
- *Speed* – connection speed of an external network device to a port;
- *Mode* – port operation mode (half/full/auto).

### Wi-Fi Status

- *SSID* – name of the access point wireless network;
- *Band* – band;
- *Channel* – channel number;
- *Bandwidth* – bandwidth;
- *Encryption* – encryption method;
- *Standarts* – network standards;
- *Clients* – connected clients quantity;

### WAN Configuration

- *Interface* – interface name;
- *VLAN ID* – interface VLAN ID;
- *MAC* – interface MAC address;
- *Connection Type* – connection type;
- *Protocol* – protocol used;
- *IP Address/Subnet Mask* – interface IP address/subnet mask;



- *Gateway* – gateway;
- *Status* – interface status.

### OMCI VLAN

- *GEM Port* – virtual interface used to transmit service traffic;
- *VLAN ID* – VLAN identifier.

### L2TP Configuration

- *Interface* – interface name;
- *Protocol* – used protocol;
- *Local IP Address* – L2TP interface IP address;
- *Remote IP Address* – server IP address;
- *Status* – interface status.

Click the "Refresh" button to update the page.

#### 5.1.1.2 The "IPv6 Status" submenu. Information about IPv6 system

The tab displays the current status of IPv6 system.

*Status → IPv6*

**IPv6 Status**

LAN Configuration	
IPv6 Address	
IPv6 Link-Local Address	fe80::eeb1:e0ff:fe31:321a/64

Prefix Delegation	
Prefix	

IPv6 address LAN GUA	
Prefix	

WAN Configuration					
Interface	VLAN ID	Connection Type	Protocol	IP Address	Status
Refresh					

### LAN Configuration

- *IPv6 Address* – IPv6 address;
- *IPv6 Link-Local Address* – local IPv6 address.

### Prefix Delegation

- *Prefix* – IPv6 address prefix.

### WAN Configuration

- *Interface* – interface name;
- *VLAN ID* – interface VLAN ID;
- *Connection Type* – connection type;
- *Protocol* – protocol used;
- *IP Address* – interface IP address;
- *Status* – interface status.

Click the "Refresh" button to update the page.

### 5.1.1.3 The "PON" submenu. Optical module status information

The tab displays the current status of PON interface system.

Status → PON

PON Status	
Temperature	38.480469 C
Voltage	3.346400 V
Tx Power	No signal
Rx Power	-36.989698 dBm
Bias Current	6.250000 mA
GPON Status	
ONU State	O1
ONU ID	255
LOID Status	Initial Status
Refresh	

#### PON Status

- *Temperature* – current temperature;
- *Voltage* – voltage;
- *Tx Power* – transmission power;
- *Rx Power* – reception power;
- *Bias Current* – bias current;
- Video Power – video signal power<sup>1</sup>.

#### PON Status

- *ONU State* – status of authorization on OLT (O1 -> O2 -> O3 -> O4 -> O5);
- *ONU ID* – device identifier on OLT;
- *LOID Status* – status of authorization on OLT (Initial -> Standby -> Serial Number -> Ranging -> Operation).

Click the "Refresh" button to update the page.

---

<sup>1</sup> Only for NTU-RG-5421GC-Wac

5.2 The "LAN" menu. LAN interface status information

In the "LAN" section you can view the status of LAN ports of the device and Wi-Fi interfaces.

Status → LAN

LAN Interface Settings

Interface name:	br0
IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
IPv6 Address:	fe80::eeb1:e0ff:fe31:321a
IPv6 DNS Mode:	HGWPProxy
Prefix Mode:	WANDelegated
IGMP Snooping:	<input checked="" type="checkbox"/> Enabled
Ethernet to Wireless Isolation:	<input type="checkbox"/> Enabled
LAN1:	<input checked="" type="checkbox"/> Enabled
LAN2:	<input checked="" type="checkbox"/> Enabled
LAN3:	<input checked="" type="checkbox"/> Enabled
LAN4:	<input checked="" type="checkbox"/> Enabled

Apply Changes

The LAN Port Status table shows:

- *Interface name* – interface name;
- *IP Address* – interface IP address;
- *Subnet Mask* – interface subnet mask;
- *IPv6 Address* – IPv6 address;
- *IPv6 DNS Mode* – configure the domain name usage mode:
  - *WANConnection* – use WAN interface for obtaining DNS server address;
  - *Static* – specify static DNS server address (IPv6 DNS1, IPv6 DNS2).
- *Prefix Mode* – configure the Prefix reception mode (from WAN interface or statically):
  - *WANDelegated* – enables the option of delegating the prefixes received from the ISP;
  - *Static* – specify static Prefix.
- *IGMP Snooping* – enable/disable IGMP Snooping;
- *Ethernet to Wireless Blocking* – enable/disable isolation of wired and wireless clients.
- *LAN1/LAN2/LAN3/LAN4* – LAN port state.

## 5.3 The "WLAN" menu. Wireless network settings

### 5.3.1 The "Basic Settings" submenu

This section contains individual settings for each of the operating bands – 2.4 GHz (wlan0 tab) and 5 GHz (wlan1 tab).

*WLAN → wlan0 (2.4GHz)/wlan1 (5GHz) → Basic Settings*

**WLAN Basic Settings**  
 This page is used to configure the parameters for WLAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

<input type="checkbox"/> Disable WLAN Interface	
Band:	2.4 GHz (B+G+N+AX) ▾
Mode:	AP ▾ <span>Multiple AP</span>
SSID:	ELTX-2.4GHz_WiFi_321A
Hide:	<input type="checkbox"/> Enabled
Channel Width:	Auto ▾
Current Channel Width:	40MHz
Control Sideband:	Upper ▾
Available Channels	1 <input checked="" type="checkbox"/> 2 <input checked="" type="checkbox"/> 3 <input checked="" type="checkbox"/> 4 <input checked="" type="checkbox"/> 5 <input checked="" type="checkbox"/> 6 <input checked="" type="checkbox"/> 7 <input checked="" type="checkbox"/> 8 <input checked="" type="checkbox"/> 9 <input checked="" type="checkbox"/> 10 <input checked="" type="checkbox"/> 11 <input checked="" type="checkbox"/> 12 <input checked="" type="checkbox"/> 13 <input checked="" type="checkbox"/>
Channel Number:	Auto ▾
Radio Power (%):	100% ▾
Limit Associated Client Number:	Disabled ▾ <input type="text"/>
Associated Clients:	<span>Show Active WLAN Clients</span>
<input type="checkbox"/> Enable Universal Repeater Mode (Acting as AP and client simultaneously)	
Regdomain:	RUSSIAN(12) ▾
<span>Apply Changes</span>	

- *Disable WLAN Interface* – disable radio interface;
- *Band* – change Wi-Fi operation standard;
- *Mode* – access point (AP) operation mode;
- *SSID* – assign a wireless network name (case sensitive);

✓ **Default device SSID is ELTX-2.4GHz\_WiFi\_aaaa, where "aaaa" – the last 4 digits of WAN MAC. WAN MAC is labelled on the device housing. The network name contains a frequency band (2.4 GHz).**

- *Hide* – disable main access point;
- *Channel Width* – set channel width 20, 40 MHz (for Wi-Fi standards: 2.4 GHz (N), 2.4 GHz (G+N), 2.4 GHz (B+G+N));
- *Current Channel Width*;
- *Control Sideband* – management sideband, select the second channel (Lower or Upper) (for Wi-Fi standards: 2.4 GHz (N), 2.4 GHz (G+N), 2.4 GHz (B+G+N));
- *Available Channels* – select channel;
- *Channel Number* – select utilized channel:
  - *Auto* – automatic channel selection.
- *Radio Power (%)* – transmitter power;
- *Limit Associated Client Number* – limit the maximum amount of associated clients;
- *Associated Clients* – amount of associated clients;
- *Enable Universal Repeater Mode (Acting as AP and client simultaneously)* – enable repeater mode;
- *Regdomain* – region settings.

To save the changes, click the "Apply Changes" button.

The "Show Active WLAN Client" button outputs the table of active WLAN clients.

WLAN → wlan0 (2.4GHz) / wlan1 (5GHz) → Basic settings → Show Active WLAN Client

Active WLAN Clients					
This table shows the MAC address, transmission, reception packet counters and encrypted status for each associated WLAN clients.					
MAC Address	Tx Packets	Rx Packets	Tx Rate (Mbps)	Power Saving	Expired Time (sec)
None	---	---	---	---	---
< >					
Refresh Close					

- *MAC Address* – MAC address of the client;
- *Tx Packets* – amount of packets transmitted to the client;
- *Rx Packets* – amount of packets received from the client;
- *Tx Rate (Mbps)* – channel transmission rate, Mbps;
- *Power Saving* – power saving mode;
- *Expired Time (sec)* – address leasing expiration time, s.

To update the information in the table, click the "Refresh" button, to close the table, click "Close".

### 5.3.2 The "Advanced settings" submenu

In this submenu you can perform advanced configuration of wireless network.

WLAN → wlan0 (2.4GHz) / wlan1 (5GHz) → Advanced settings

WLAN Advanced Settings	
These settings are only for more technically advanced users who have a sufficient knowledge about WLAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.	
Beacon Interval:	100 (100-1024 ms)
DTIM Period:	1 (1-255)
Data Rate:	Auto
Preamble Type:	<input checked="" type="radio"/> Long Preamble <input type="radio"/> Short Preamble
Broadcast SSID:	<input type="checkbox"/> Enabled
Client Isolation:	<input type="checkbox"/> Enabled
Aggregation:	<input checked="" type="checkbox"/> Enabled
Short GI:	<input checked="" type="checkbox"/> Enabled
TX beamforming:	<input checked="" type="checkbox"/> Enabled
MU MIMO:	<input checked="" type="checkbox"/> Enabled
Multicast to Unicast:	<input checked="" type="checkbox"/> Enabled
Band Steering:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled Prefer 5GHz
OFDMA:	<input type="checkbox"/> Enabled
WMM Support:	<input checked="" type="checkbox"/> Enabled
802.11k Support:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Apply Changes	

- *Beacon Interval* – time period for transmission of informational packets, which indicate activity of the access point, to the wireless network;
- *DTIM Period* – interval between sending packets from buffer;
- *Data rate* – transmission rate;
- *Preamble Type (Long Preamble/Short Preamble)* – select the preamble;
- *Broadcast SSID (Enabled/Disabled)* – broadcast SSID to the network (will be hidden if *Disabled* is selected);

- *Client Isolation (Enabled/Disabled)* – enable/disable client blocking;
- *Aggregation (Enabled/Disabled)* – enable/disable frames aggregation to increase the bandwidth;
- *Short GI (Enabled/Disabled)* – enable/disable a short guard interval;
- *TX beamforming (Enabled/Disabled)* – enable/disable adaptive beamforming;
- *MU MIMO (Enabled/Disabled)* – enable/disable Multi-user MIMO mode;
- *Multicast to Unicast (Enabled/Disabled)* – enable/disable multicast-unicast conversion;
- *OFDMA (Enabled/Disabled)* – enable/disable multi-user version of digital modulation;
- *WMM Support (Enabled/Disabled)* – enable/disable the support for Wi-Fi Multimedia;
- *802.11k Support (Enabled/Disabled)* – enable/disable 802.11k support.

To save the changes, click the "Apply Changes" button.

### 5.3.3 The "Security" Submenu. Security Settings

Use this menu to configure general data encryption settings for a wireless network. The client wireless equipment can be configured either manually or automatically with the help of WPS.

WLAN → wlan0 (2.4GHz) / wlan1 (5GHz) → Security

**WLAN Security Settings**  
 This page allows you setup the WLAN security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

SSID Type:	Root AP - ELTX-2.4GHz_WiFi_321A ▾
Encryption:	WPA2 Mixed ▾
Authentication Mode:	<input type="radio"/> Enterprise (RADIUS) <input checked="" type="radio"/> Personal (Pre-Shared Key)
WPA Cipher Suite:	<input type="checkbox"/> TKIP <input checked="" type="checkbox"/> AES
WPA2 Cipher Suite:	<input type="checkbox"/> TKIP <input checked="" type="checkbox"/> AES
Group Key Update Timer:	86400
Pre-Shared Key Format:	Passphrase ▾
Pre-Shared Key:	<input type="password"/> <input type="checkbox"/> Show password

Apply Changes

- *SSID Type* – current SSID;
- *Encryption* – set the encryption mode:
  - *NONE (open)* – no wireless network protection;
  - *WEP* – WEP encryption algorithm;
  - *WPA/WPA2/WPA2 Mixed/WPA3/WPA3 Transition* – WPA/WPA2/WPA2 Mixed/WPA3/WPA3 Transition encryption algorithm;
  - *Enhanced open* – wireless network protection with Enhanced open algorithm;
  - *Enhanced open Transition* – wireless network protection with Enhanced open Transition algorithm.

When the WEP encryption mode is selected, the following settings are available:

- *802.1x Authentication* – enables 802.1x standard (enables user authentication with RADIUS server, WEP key is used for data encryption);
- *Authentication* – select authentication mode:
  - *Open system* – without authentication;
  - *Shared Key* – pre-shared key authentication;
  - *Auto* – automatic authentication.
- *Key Length (encryption strength)* – use 64- or 128-bit keys;
- *Key Format* – use ASCII or HEX format;
- *Encryption Key* – 10 hex characters key or 5 ASCII characters for 64-bit encryption. Other options are 26 hex characters or 13 ASCII characters for 128-bit encryption.

When the *WPA/WPA2/WPA2 Mixed/WPA3/WPA3 Transition* encryption mode is selected, the following settings are available:

- *Authentication Mode* – Enterprise (RADIUS) or Personal (Pre-Shared Key) authentication mode;
- *IEEE 802.11w* – enable service frame encryption;
  - *None* – disable service frame encryption;
  - *Capable* – encryption compatibility mode;
  - *Required* – encryption is required.
- *SHA256 (Enable/Disable)* – enable/disable SHA256 usage.
- *WPA Cipher Suite* – set of WPA TKIP or AES fonts;
- *Group Key Update Timer* – key update timer;
- *RADIUS Server/Backup RADIUS Server*:
  - *IP Address* – RADIUS server IP address;
  - *Port* – RADIUS server port number. The default port is 1812;
  - *Password* – Secret key for access to the RADIUS server;
  - *Show password* – show password when checkbox is selected.
- *Pre-Shared Key Format* – key format: ASCII or HEX;
- *Pre-Shared Key* – access key.

To see the encrypted access key, select the "Show password" checkbox. To save the changes, click the "Apply Changes" button.

#### 5.3.4 The "Access Control" Submenu. Access settings

The menu allows filtering configuration for MAC addresses. All added MAC addresses will be displayed in the *Current Access Control List*. When selecting the "*Allow Listed*" mode, only those MAC addresses that are in the *Current Access Control List* can connect to the access point. When the "*Deny Listed*" mode is selected, all MAC addresses except those specified in the *Current Access Control List* will have access. To change the mode, click the "Apply Changes" button.

*WLAN → wlan0 (2.4GHz) / wlan1 (5GHz) → Access control*

**WLAN Access Control**

If you choose 'Allowed Listed', only those WLAN clients whose MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these WLAN clients on the list will not be able to connect the Access Point.

Mode:

Disabled ▾

Apply Changes

MAC Address:

(ex. 00E086710502)

Add

Reset

Current Access Control List	
MAC Address	Select

Delete Selected

Delete All

- *Mode* – MAC filtering mode:
  - *Disabled* – filter is not used;
  - *Allow Listed* – filtering on the basis of allowed addresses (white list);
  - *Deny Listed* – filtering on the basis of denied addresses (black list).
- *MAC Address* – field to add MAC address to the filtering table. To enter the value, click "Add" or click "Reset" to reset the value.

To remove selected items in the list, click "Delete Selected"; click "Delete All" to remove the whole list.

### 5.3.5 The "Wi-Fi radar" submenu. Wireless network scanning

Use this menu to scan a wireless network and to detect nearby access points or IBSS.

*WLAN → wlan0 (2.4GHz) / wlan1 (5GHz) → WiFi Radar*

<b>WLAN Site Survey</b>					
This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.					
SSID	BSSID	Channel	Type	Encryption	Power (dBm)
Eltex-Devices	ec:b1:e0:0a:e6:01	11 (B+G+N+AX) 20MHz	AP	WPA-PSK/WPA2-PSK	-34
Eltex-Guest	ec:b1:e0:0a:e6:04	11 (B+G+N+AX) 20MHz	AP	no	-34
Eltex-Local	ec:b1:e0:0a:e6:00	11 (B+G+N+AX) 20MHz	AP	WPA2-1X	-34
Eltex-Local	68:13:e2:1f:76:60	1 (B+G+N+AX) 20MHz	AP	WPA2-1X	-36
RG-WiFi-403	68:13:e2:13:97:17	11 (B+G+N) 40MHz	AP	WPA2-PSK	-76
Geo_test	cc:9d:a2:c2:e1:90	6 (B+G+N+AX) 20MHz	AP	WPA-PSK	-78
Eltex-Guest	ec:b1:e0:0a:f1:e1	11 (B+G+N+AX) 20MHz	AP	no	-79
<b>Refresh</b>					

The table displays the following information:

- *SSID* – wireless access point name;
- *BSSID* – access point MAC address;
- *Channel* – channel;
- *Type* – type (AP (Access Point), Client);
- *Encryption* – encryption method;
- *Power (dBm)* – received signal power.

To scan the environment, click the "Refresh" button.

### 5.3.6 The "WPS" submenu. Easy connection to Wi-Fi network

This section configures WPS (Wi-Fi Protected Setup) connection.

*WLAN → wlan0 (2.4GHz) / wlan1 (5GHz) → WPS*

<b>Wi-Fi Protected Setup</b>	
This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your WLAN client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.	
<input type="checkbox"/> <b>Disable WPS</b>	
<b>Start WPS configuration:</b>	<b>Start PBC</b>
<b>Apply Changes</b>	

- *Disable WPS* – disable the possibility of connecting to the router using WPS technology;
- *Start WPS configuration:*
  - *Start PBC* – activate the WPS function on the router to connect subscribers.

To save the changes, click the "Apply Changes" button.



### 5.3.7 The "Status" submenu. Current WLAN status

This submenu displays the current status of the WLAN.

*WLAN* → *wlan0 (2.4GHz)* / *wlan1 (5GHz)* → *Status*

WLAN Status	
WLAN Configuration	
Mode	AP
Band	2.4 GHz (B+G+N+AX)
SSID	ELTX-2.4GHz_WiFi_321A
Channel Number	1
Channel Width	Auto
Current Channel Width	40MHz
Encryption	WPA2 Mixed
BSSID	ec:b1:e0:31:32:1b
Associated Clients	0

- *Mode* – AP (access point);
- *Band* – range, band, standards;
- *SSID* – access point network name;
- *Channel Number* – channel number;
- *Channel Width* – channel width;
- *Encryption* – encryption method;
- *BSSID* – access point MAC address;
- *Associated Clients* – number of connected clients.

To save the changes, click the "Apply Changes" button.

5.3.8 The "Wi-Fi Isolation" submenu. Wi-Fi isolation mode setting

This submenu displays isolation modes to protect a device from attacks by another device on the same network.

WLAN → Wi-Fi Isolation

Wi-Fi Isolation

WLAN Isolation

Ethernet to Wireless Isolation:

☐ Enabled

WLAN0(2.4GHz) Client Isolation:

☐ Enabled

WLAN1(5GHz) Client Isolation:

☐ Enabled

WLAN0(2.4GHz) to WLAN1(5GHz) Isolation:

☐ Enabled

wlan0 (2.4GHz) AP Isolation

Isolation:

☐ Enabled

AP Isolation:

☐ AP1 ☐ AP2 ☐ AP3

wlan1 (5GHz) AP Isolation

Isolation:

☐ Enabled

AP Isolation:

☐ AP1 ☐ AP2 ☐ AP3

Apply Changes

WLAN Isolation

- Ethernet to Wi-Fi Isolation (Enabled/Disabled) – enable/disable Isolation between LAN and wireless network;
- WLAN0(2.4GHz) Client Isolation (Enabled/Disabled) – enable/disable Isolation between clients in 2.4 GHz band;
- WLAN1(5GHz) Client Isolation (Enabled/Disabled) – enable/disable Isolation between clients in 5 GHz band;
- WLAN0(2.4GHz) to WLAN1(5GHz) Isolation (Enabled/Disabled) – enable/disable isolation between 2.4 GHz and 5 GHz bands.

WLAN0 (2.4 GHz) AP Isolation/WLAN1 (5 GHz) AP Isolation

- Isolation (Enabled/Disabled) – enabling isolation in guest SSID;
- AP Isolation – selecting AP SSID, inside which isolation will be enabled.

To save the changes, click the "Apply Changes" button.

## 5.4 The "VPN" menu. Virtual private network configuration

### 5.4.1 The "L2TP" submenu. L2TP VPN configuration

This section is used to configure the parameters of L2TP VPN virtual connection. L2TP protocol is used to create a secure communication channel over the Internet between the remote user's computer and the local computer.

#### VPN → L2TP

**L2TP VPN**

**L2TP VPN:** ☒ Enable

**Server:**

**Tunnel Authentication:** ☐

**Tunnel Authentication Secret:**

**PPP Authentication:** Auto ▾

**PPP Encryption:** NONE ▾

**Username**

**Password:**

**PPP Connection Type:** Persistent ▾

**Idle Time (sec):**

**MTU:**

**Default Gateway:** ☐

Apply Changes

**L2TP Table**

Select	Interface	Server	Tunnel Authentication	PPP Authentication	MTU	Default Gateway	Action
Delete Selected							

- *L2TP VPN* – mode in which access to the Internet is provided through a special channel, a tunnel, using L2TP. When "Enable" is checked, the following parameters become available for editing:
- *Server* – L2TP server address (domain name or IP address in IPv4 format);
- *Tunnel Authentication* – enable authentication;
- *Tunnel Authentication Secret* – authentication key;
- *PPP Authentication* – selection of connection authentication protocol used on L2TP server;
- *PPP Encryption* – selection of the data encryption protocol to be used (for CHAPMSv2 method only);
- *Username* – user name for authorization on L2TP server;
- *Password* – password for authorization on L2TP server;
- *PPP Connection Type* – connection type;
- *Idle Time (min)* – idle time in seconds, breaks inactive connection after specified time (only for dial-on-demand connection);
- *MTU* – maximum block size of data transmitted over the network (recommended value – 1462);
- *Default Gateway* – selecting whether or not the created L2TP tunnel will be the default gateway.

To save the changes click the "Apply Changes" button.

In the "L2TP Table" you can view the status of L2TP VPN virtual connection. To delete a certain entry, select a position and click "Delete Selected".

## 5.5 The "Services" menu. Service configuration

### 5.5.1 The "Service" menu

#### 5.5.1.1 The "DHCP" submenu. DHCP configuration

The menu allows DHCP server and DHCP repeater configuration.

*Services → Service → DHCP (DHCP Server mode)*

### DHCP Settings

This page is used to configure DHCP Server and DHCP Relay.

**DHCP Mode:**
☐ NONE
 ☐ DHCP Relay
 ☒ DHCP Server

Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.

**LAN IP Address:** 192.168.1.1

**Subnet Mask:** 255.255.255.0

**IP Pool Range:**
 -

**Subnet Mask:**

**Max Lease Time:**  seconds (-1 indicates an infinite lease)

**Domain name:**

**Gateway Address:**

**DNS option:**
☒ Use DNS Proxy
 ☐ Set Manually

- *DHCP Mode* – select operation mode:
  - *NONE* – DHCP disabled;
  - *DHCP Relay* – operation in DHCP repeater mode;
  - *DHCP Server* – operation in DHCP server mode.
- *IP Pool Range* – range of addresses distributed among clients;
- *Show Client* – button to view clients who leased the addresses. When clicking, a table with information about DHCP clients leased by a DHCP server is displayed;
- *Max Lease Time* – maximum lease time, -1 for endless lease;
- *Domain name* – domain name;
- *Gateway Address* – gateway address;
- *DNS option* – defines DNS operation:
  - *Use DNS relay* – ONT address will be returned as DNS and all queries will be relayed via ONT;
  - *Set manually* – set DNS manually.

Click "Show Client" to see the table with information on DHCP clients, that lease the DHCP server.

*Services → Service → DHCP (DHCP Relay mode)*

### DHCP Settings

This page is used to configure DHCP Server and DHCP Relay.

**DHCP Mode:**
☐ NONE
 ☒ DHCP Relay
 ☐ DHCP Server

This page is used to configure the DHCP Server IP Address for DHCP Relay.

**DHCP Server IP Address:**

- *DHCP Server IP Address* – IP address of the remote DHCP server.

To save the changes, click the "Apply Changes" button. "Port-Based Filter" and "MAC-Based Assignment" buttons allow configuring port-based and MAC-based filtering, respectively.

#### 5.5.1.2 The "Dynamic DNS" submenu. Dynamic DNS Configuration

Dynamic DNS (domain name system) allows information to be updated on DNS server in real time and (optionally) automatically. It is applied for assignment of a constant domain name to a device (computer, router, e. g. NTP-RG) having a dynamic IP address. The IP address can be assigned by IPCP in PPP connections or in DHCP.

Dynamic DNS is frequently used in local networks where clients are obtaining IP addresses through DHCP and then are registering their names on a local DNS server.

*Services → Service → Dynamic DNS*

### Dynamic DNS

**Enable:** ☒

**DDNS Provider:**

**Hostname:**

**Interface:**

**Dynamic DNS & No-IP settings**

**Username:**

**Password:**

**Dynamic DNS table**

Select	State	Hostname	Username	Service	Status
--------	-------	----------	----------	---------	--------

- *Enable* – when selected, enable DHCP server (IP addresses from the following range will be dynamically assigned to network devices);
- *DDNS Provider* – select the type of D-DNS service (provider): org, TZO.com, No-IP.com;
- *Custom* – another provider selected by user. In this case, you need to specify the provider's name (*Hostname*) and address (*Interface*).

**Dynamic DNS & No-IP settings:**

- *UserName* – user name;
- *Password* – authorization password on the service selected for operation with D-DNS.

"Dynamic DNS table" table with the list of available DNS displayed in this section. To add a record, click the "Add" button. To remove/modify a record, click the "Remove"/"Modify" button for the selected record.

**5.5.1.3 The "UPnP" submenu. Automated Setup of Network Devices**

In this section you can configure Universal Plug and Play (UPnP™) function. UPnP ensures compatibility with network equipment, software and peripheral devices.

*Services → Service → UPnP*

- *UPnP (Enable/Disable)* – enable/disable the UPnP function.

To save the settings, click the "Apply Changes" button.

**5.5.1.4 The "RIP" submenu. Dynamic routing configuration**

This section is used to select the interfaces on your device is that use RIP, and the version of the protocol used. Enable the RIP if you are using this device as a RIP-enabled Device to communicate with others using the Routing Information Protocol (RIP).

*Services → Service → RIP*

- *Routing protocol* – enable/disable the use of dynamic routing protocol RIP.

To accept and save the settings, click the "Apply Changes" button.

- *Interface* – interface on which RIP will be started;
- *Receive Mode* – incoming packets processing mode (NONE, RIP1, RIP2, both);
- *Send Mode* – sending mode (NONE, RIP1, RIP2, RIP1 COMPAT).

Interfaces with the support for RIP are displayed in the "*RIP Config Table*". To delete all entries in the table click the "Delete All" button; to delete one position from the list select it and click "Delete Selected".

### 5.5.1.5 The "DLNA" submenu

DLNA (Digital Living Network Alliance) is a set of standards that allow compatible devices to transmit and receive various media content (images, music, video) over a home network, as well as display it in real time. That is, it is a technology for connecting home computers, mobile phones, laptops and household electronics into a single digital network. Devices that support the DLNA specification can be configured and connected to the network automatically at the user's discretion.

The media content transmission environment is usually a home local network (IP network). Connecting DLNA-compatible devices to a home network can be either wired (Ethernet) or wireless (Wi-Fi).

Services → Service → DLNA

**Digital Media Server Settings**

Digital Media Server:	<input checked="" type="checkbox"/> Enable
-----------------------	--

Apply Changes

- *Digital Media Server* – when selected, the media server is enabled.

To save the settings, click the "Apply Changes" button.

## 5.5.2 The "Firewall" submenu. Firewall configuration

### 5.5.2.1 The "ALG" submenu. Enable/disable ALG services

This section is used to enable/disable ALG services.

- ✓ **Application-level gateway (ALG)** – NAT router component that understands an application protocol, and when packets of that protocol pass through it, modifies them so that users behind the NAT can use the protocol.

Services → Firewall → ALG

**NAT ALG and Pass Through**

ALG	
FTP	<input checked="" type="checkbox"/> Enable
TFTP	<input checked="" type="checkbox"/> Enable
H323	<input checked="" type="checkbox"/> Enable
SIP	<input checked="" type="checkbox"/> Enable
PPTP	<input checked="" type="checkbox"/> Enable

Apply Changes

### 5.5.2.2 The "IP/Port Filtering" submenu. Address Filtering Settings

This section is used to configure address filtering. The IP Filtering function filters router traffic by IP addresses and ports. Using these filters can be useful to protect or restrict the local network.

Services → Firewall → IP/Port Filtering

**IP/Port Filtering**  
Entries in this table are used to restrict certain types of data packets through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

**Outgoing Default Action:**
☐ Deny
 ☒ Allow

**Incoming Default Action:**
☒ Deny
 ☐ Allow

Apply Changes

**Direction:**

Outgoing ▾

**Protocol:**

TCP ▾

**Rule Action:**
☒ Deny
 ☐ Allow

**Source IP Address:**

**Subnet Mask:**

**Port:**

-

**Destination IP Address:**

**Subnet Mask:**

**Port:**

-

**WAN Interface:**

Any ▾

Add

Current Filter Table

Select	Direction	Protocol	Source IP Address	Source Port	Destination IP Address	Destination Port	Interface	Rule Action
<div> Delete Selected           Delete All         </div>								

#### Default

- *Incoming Default Action (Deny / Allow)* – filtering for incoming packets;
- *Outgoing Default Action (Deny / Allow)* – filtering for outgoing packets.

To save the changes, click the "Apply Changes" button.

To add a filter, fill in the appropriate fields and click the "Add" button:

- *Direction* – packet direction;
- *Protocol* – filtering protocol;
- *Rule Action (Deny / Allow)* – packet processing policy (deny/allow);
- *Source IP Address* – source IP address:
  - *Subnet mask* – source subnet mask;
  - *Port* – source port.
- *Destination IP Address* – destination IP address:
  - *Subnet mask* – destination subnet mask;
  - *Port* – destination port.
- *WAN Interface* – ingress interface.

Added filters are displayed in the "Current Filter Table" located below. The entries in this table are used to restrict certain types of data packets pass through the gateway. To delete a specific filter, select the position and click the "Delete selected" button, to delete all filters click "Delete All".



5.5.2.3 The "MAC Filtering" submenu. Filtering Settings for MAC Addresses

MAC filtration allows traffic to be forwarded or blocked depending on source and destination MAC addresses. To change the mode click the "Apply Changes" button.

Services → Firewall → MAC Filtering

MAC Filtering for bridge mode

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Outgoing Default Action:

☐ Deny ☒ Allow

Incoming Default Action:

☐ Deny ☒ Allow

Apply Changes

Direction:

Outgoing ▾

Source MAC Address:

Destination MAC Address:

Rule Action:

☒ Deny ☐ Allow

Add

Current Filter Table

Select	Direction	Source MAC Address	Destination MAC Address	Interface	Rule Action
--------	-----------	--------------------	-------------------------	-----------	-------------

Delete Selected

Delete All

- Incoming Default Action (Deny / Allow) – filtering for incoming packets;
  - Outgoing Default Action (Deny / Allow) – filtering for outgoing packets;
  - Source MAC Address – MAC address for which limitation/access should be imposed;
  - Destination MAC Address – MAC address for which limitation/access should be imposed.
- Added filters are displayed in the "Current Filter Table" located below. The "Rule" field displays the type of created rule ("Allow" – allowing or "Deny" – forbidding). To delete a specific filter, select the position and click the "Delete selected" button, to delete all filters click "Delete All".



After filling the fields click the "Add" button to add the entry. To delete a selected position, click the "Delete Selected" button; to delete the whole table, click the "Delete All" button.

#### 5.5.2.5 The "URL Blocking" submenu. Internet access restriction configuration

URL filter performs complete analysis and provides access control to specific Internet resources. This section sets and displays a list of forbidden/allowed URLs to visit. Here you can add the forbidden/allowed FQDN (Fully Qualified Domain Name) with the "Add" button, filtering by keywords is also possible. The added restrictions are displayed in the "URL Blocking Table" and the "Keyword Filtering Table". To remove a specific URL or keyword from the table, click on it and then on the "Delete Selected" button. To delete all restrictions click the "Delete All" button.

Services → Firewall → URL Blocking

**URL Blocking**  
 This page is used to configure the Blocked FQDN(Such as tw.yahoo.com) and filtered keyword. Here you can add/delete FQDN and filtered keyword.

URL Blocking: ☐ Enable Apply Changes

FQDN:  Add

**URL blocking table**

Select	FQDN
<input type="checkbox"/>	

Delete Selected Delete All

Keyword:  Add

**Keyword Filtering Table**

Select	Filtered Keyword
<input type="checkbox"/>	

Delete Selected Delete All

- *URL Blocking (Enable/Disable)* – enable/disable URL Blocking operation;
- *FQDN* – Fully Qualified Domain Name;
- *Keyword* – keyword.

To save the changes, click the "Apply Changes" button.

#### 5.5.2.6 The "Domain Blocking" submenu. Domain blocking configuration

This section is used to set domain blocking.

Services → Firewall → Domain Blocking

**Domain Blocking**

Domain Blocking: ☐ Enable Apply Changes

Domain:  Add

**Domain Blocking**

Select	Domain
<input type="checkbox"/>	

Delete Selected Delete All

To block the domain check *Enable*, fill the *Domain* field and click the "Add" button

- *Domain Blocking (Enable/Disable)* – enable/disable blocking;
- *Domain* – domain name.

To save the changes, click the "Apply Changes" button. All blocked domains are listed in the "*Domain Blocking*" table, to remove a blocking for one domain, select it and click the "Delete Selected" button, to remove all restrictions, click the "Delete All" button.

#### 5.5.2.7 The "DMZ" submenu. Demilitarized Zone configuration

When an IP address is set in the "*DMZ host IP address field*", all requests from external network, that do not satisfy the "*Port Forwarding*" rules, will be redirected to a DMZ host (a trusted host with the specified address in the local network).

Services → Firewall → DMZ

DMZ	
A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.	
DMZ Host:	<input checked="" type="checkbox"/> Enable
DMZ Host IP Address:	<input type="text" value="0.0.0.0"/>
<input type="button" value="Apply Changes"/>	

- *DMZ Host (Enable/Disable)* – enable/disable the host;
- *DMZ Host IP Address* – IP address.

To save the changes, click the "Apply Changes" button.

### 5.5.3 The "Samba" submenu

#### 5.5.3.1 The "Configuration" submenu. Configuration of Samba

In this submenu you can configure Samba users.

Services → Samba → Configuration

Samba	
Samba:	<input type="checkbox"/> Enable
NetBIOS Name :	<input type="text"/>
Server String :	<input type="text"/>
<input type="button" value="Apply Changes"/>	

- *Samba Enable/Disable* – enable/disable Samba configuration;
- *NetBIOS Name* – domain name when identifying in a local network;
- *Server String* – server name.

The section displays the "Account information" table with a list of existing accounts. To add or edit an entry, click the "Add/Edit" button. To delete an item, select it and click "Delete". To clear the filled fields, click the "Reset" button.

To save the changes, click the "Apply Changes" button.

### 5.5.3.2 The "Accounts" submenu

In the "Accounts" section you can create personal Samba accounts.

*Services → Samba → Account*

Samba		
Username:	<input type="text"/>	
Password:	<input type="password"/>	
Confirmed Password	<input type="password"/>	
<input type="button" value="Add/Edit"/> <input type="button" value="Delete"/> <input type="button" value="Reset"/>		
Account information		
Username	Permissions	Delete Selected

- *Username* – account name;
- *New password* – password;
- *Confirmed Password* – password confirmation.

### 5.5.3.3 The "Shares" submenu

The "Shares" section is used to add Samba library.

*Services → Samba → Shares*

Samba							
Sharename:	<input type="text"/>						
Write list:	<input type="text"/>						
Read list:	<input type="text"/>						
Comment:	<input type="text"/>						
Write list:	<input type="checkbox"/>						
<input type="button" value="Apply"/> <input type="button" value="Delete"/> <input type="button" value="Reset"/>							
Shares information							
Sharename	Path	Write list	Read list	Comment	Permissions	Delete Selected	
Account information							
Username				Permissions			

- *Sharename* – library name;
- *Write list* – list of accounts who can change files in the library;
- *Read list* – list of accounts who can read files in the library;
- *Comment* – comment for the library;
- *Write list* – when selected, the library is available for reading only.

## 5.6 The "VoIP" menu. IP telephony settings

 For NTU-RG-5521G-Wax only.

### 5.6.1 The "VoIP" submenu

#### 5.6.1.1 The "Port" submenu

##### 5.6.1.1.1 Proxy

*VoIP → VoIP → Port1 → Proxy*

Default Proxy	
Select Default Proxy	Proxy0 ▾
Proxy0	
Display Name	<input type="text"/>
Number	<input type="text"/>
Login ID	<input type="text"/>
Password	<input type="password"/>
Proxy	<input type="checkbox"/> Enable
Proxy Addr	<input type="text"/>
Proxy Port	<input type="text" value="5060"/>
SIP Subscribe	<input type="checkbox"/> Enable
SIP Domain	<input type="text" value="onChange='onchange_dor"/>
Reg Expire (sec)	<input type="text" value="3600"/>
Registration Retry Timeout (sec)	<input type="text" value="20"/>
Outbound Proxy	<input type="checkbox"/> Enable
Outbound Proxy Addr	<input type="text"/>
Outbound Proxy Port	<input type="text" value="5060"/>
Enable Session timer	<input checked="" type="checkbox"/> Enable
Session Expire (sec)	<input type="text" value="1800"/>

### Default Proxy

- *Select Default Proxy* – selection of a proxy to be used by default.

### Proxy

- *Display Name* – displayed account name;
- *Number* – number;
- *Login ID* – login;
- *Password* – password;
- *Proxy* – enable server use for forwarding outgoing calls;

- *Proxy Addr* – SIP server address;
- *Proxy Port* – SIP port;
- *SIP Subscribe* – subscription to receive event notifications;
- *SIP Domain* – SIP domain name;
- *Reg Expire, (sec)* – registration time, (s);
- *Registration Retry Timeout (sec)* – registration timeout;
- *Outbound Proxy* – enable server use for forwarding outgoing calls;
- *Outbound Proxy Addr* – forwarding server address;
- *Outbound Proxy Port* – forwarding server port;
- *Enable Session timer* – enable session timer;
- *Session Expire (sec)* – session length.

## 5.6.1.1.2 SIP Advanced

VoIP → VoIP → Port1 → SIP Advanced

SIP Advanced	
SIP Port	<input type="text" value="5060"/>
Media Port	<input type="text" value="9000"/>
DTMF Relay	<input type="text" value="Inband"/>
DTMF RFC2833 Payload Type	<input type="text" value="96"/>
DTMF RFC2833 Packet Interval	<input type="text" value="10"/> (msec) (Must be multiple of 10msec)
Use DTMF RFC2833 PT as Fax/Modem RFC2833 PT	<input checked="" type="checkbox"/> Enable
Fax/Modem RFC2833 Payload Type	<input type="text" value="101"/>
Fax/Modem RFC2833 Packet Interval	<input type="text" value="10"/> (msec) (Must be multiple of 10msec)
SIP INFO Duration (ms)	<input type="text" value="250"/>
Call Waiting	<input type="checkbox"/> Enable
Call Waiting Caller ID	<input type="checkbox"/> Enable
Reject Direct IP Call	<input type="checkbox"/> Enable
Send Caller ID hidden	<input type="checkbox"/> Enable
Call transfer	<input checked="" type="checkbox"/> Enable
3 way conference	<input checked="" type="checkbox"/> Enable
Conference on server/CPE	<input type="radio"/> server <input checked="" type="radio"/> CPE
Conference-uri	<input type="text"/>

- *SIP Port* – port used for SIP operation;
- *Media Port* – port for transmission of voice traffic;
- *DTMF Relay* – DTMF transmission method;
- *DTMF RFC2833 Payload Type* – type of positive load in DTMF;
- *DTMF RFC2833 Packet Interval* – transmission interval (multiple of 10 ms);
- *Use DTMF RFC2833 PT as Fax/Modem RFC2833 PT* – enable the use of DTMF2833 PT for fax transmission;
- *Fax/Modem RFC2833 Payload Type* – load type for Fax/Modem RFC2833;
- *Fax/Modem RFC2833 Packet Interval* – Fax/Modem RFC2833 packets transmission interval (multiple of 10 ms);
- *SIP INFO Duration (ms)* – SIP INFO message duration;
- *Call Waiting* – enable call waiting;
- *Call Waiting Caller ID* – enable display of Caller ID during call waiting;
- *Reject Direct IP Call* – enable rejection of direct IP call;
- *Send Caller ID hidden* – enable hiding Caller ID;
- *Call transfer* – enable call transfer;
- *3 way conference* – enable 3-way conference;
- *Conference on server/CPE* – conference organization selection: on CPE or server;
- *Conference-uri* – conference server address.



## 5.6.1.1.3 Forward Mode

VoIP → VoIP → Port1 → Forward Mode

Forward Mode	
Immediate Forward to	<input checked="" type="radio"/> off <input type="radio"/> VoIP <input type="radio"/> PSTN
Immediate Number	<input type="text"/>
Busy Forward to	<input checked="" type="radio"/> off <input type="radio"/> VoIP
Busy Number	<input type="text"/>
No Answer Forward to	<input checked="" type="radio"/> off <input type="radio"/> VoIP
No Answer Number	<input type="text"/>
No Answer Time (sec)	<input type="text" value="0"/>

- *Immediate Forward to* – activation of unconditional forwarding;
- *Immediate Number* – number to which unconditional forwarding will be carried out;
- *Busy Forward to* – busy call forwarding activation;
- *Busy Number* – number to which call forwarding will be carried out when the line is busy;
- *No Answer Forward to* – activation of call forwarding on no answer;
- *No Answer Number* – number to which call forwarding on no answer will be carried out;
- *No Answer Time, (sec)* – no answer time until call forwarding is triggered, (s).

## 5.6.1.1.4 Dial plan

VoIP → VoIP → Port1 → Dial plan

Dial plan	
Enable Dialplan	<input type="checkbox"/> Enable
Dial plan	<input type="text" value="[*#x]."/>

- *Enable Dialplan (on/off)* – enable/disable dialplan;
- *Dial plan* – dialplan itself.

## 5.6.1.1.5 Codec

VoIP → VoIP → Port1 → Codec

Codec											
RTP Redundant (First precedence)		Codec		Disable ▾							
		Payload Type		121							
Type	Packetization	Precedence									Disable
		1	2	3	4	5	6	7	8	9	
G711-ulaw	20 ms ▾	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G711-alaw	20 ms ▾	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G729	20 ms ▾	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G723	30 ms ▾	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
G726-16k	20 ms ▾	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G726-24k	20 ms ▾	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G726-32k	20 ms ▾	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G726-40k	20 ms ▾	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G722	10 ms ▾	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Option	G726 Packing Order		Right ▾								
	G723 Bit Rate		6.3k ▾								

- *RTP Redundant Codec (First precedence)* – select redundant codec;
- *Payload Type* – positive load type;
- *Type* – codec type;
- *Packetization* – select packetization time;
- *Precedence* – select codec priority;
- *Disable* – disable codecs;
- *Option G726 Packing Order* – select option G726 order;
- *Option G723 Bit Rate* – select G723 speed.

## 5.6.1.1.6 Hot line

VoIP → VoIP → Port1 → Hot Line

Hot Line	
Use Hot Line	<input type="checkbox"/> Enable
Hot Line Number	<input type="text"/>

- *Use Hot Line* – enable use of hotline;
- *Hot Line Number* – hotline number.

## 5.6.1.1.7 DND (Don't Disturb)

*VoIP → VoIP → Port1 → DND (Don't Disturb)*

DND (Don't Disturb)	
DND Mode	<input type="radio"/> Always <input checked="" type="radio"/> Enable <input type="radio"/> Disable
From	<input type="text" value="00"/> : <input type="text" value="00"/> (hh:mm)
To	<input type="text" value="00"/> : <input type="text" value="00"/> (hh:mm)

- *DND Mode* – activation of the Do Not Disturb service;
- *From; To* – Do Not Disturb service time.

## 5.6.1.1.8 Alarm

*VoIP → VoIP → Port1 → Alarm*

Alarm	
Enable	<input type="checkbox"/>
Time	<input type="text" value="0"/> : <input type="text" value="0"/> (hh:mm)
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

- *Enable* – activation of the service alarm;
- *Time* – set alarm time.

### 5.6.1.2 The "Advance" submenu. Advanced VoIP settings

VoIP → VoIP → Advance

Call Hold	
Call Hold	<input checked="" type="checkbox"/> Enable
V.152	
V.152	<input type="checkbox"/> Enable
V.152 Payload Type	102
V.152 codec type	PCM u-law ▾
T.38(FAX)	
T.38	<input type="checkbox"/> Enable
Fax Modem Detection Mode	AUTO_2 ▾
T.38(Customize parameters)	
Customize parameters	<input type="checkbox"/> Enable
Max buffer	500
TCF	Remote TCF ▾
Max Rate	14400 ▾
ECM	<input checked="" type="checkbox"/> Enable
ECC Signal	5 ▾
ECC Data	2 ▾
Spoofing	<input checked="" type="checkbox"/> Enable
Packet Duplicate Num	0 ▾

#### Call Hold

- *Call Hold* – enable the service.

#### V.152

- *152 Enable* – enable support for V.152;
- *152 Payload Type* – positive load type;
- *152 codec type* – select codec type.

#### T.38(FAX)

- *T38* – enable protocol T.38 (Fax);
- *Fax Modem Detection Mode* – select fax detection mode.

#### T.38 (Customize parameters)

- *Customize parameters* – enable the use of arbitrary parameters for T.38;
- *Max buffer* – maximum buffer size;
- *TCF* – select starting frame;
- *Max Rate* – select maximum speed;
- *ECM* – enable error correction;
- *ECC Signal* – select correction signal;

- *ECC Data* – corrected data;
- *Spoofing* – spoofing;
- *Packet Duplicate Num* – select number of ports.

DSP		
Jitter Buffer Control	Min delay (ms):	40 ▾
	Max delay (ms):	200 ▾
	Optimization factor:	1 ▾
LEC Tail Length	2 (ms)	2~32 ms
LEC	<input checked="" type="checkbox"/> Enable	
NLP	<input checked="" type="checkbox"/> Enable	
VAD	<input type="checkbox"/> Enable	
VAD Amp. Threshold (0 < Amp < 200)	63 (Amp.)	
SID Noise Level	<input checked="" type="radio"/> Disable configuration	
	<input type="radio"/> Fixed noise level	70 (0>Value>127 dBov)
	<input type="radio"/> Adjust noise level	0 (-127~127 dBov, 0:Not change)
CNG	<input checked="" type="checkbox"/> Enable	
CNG . Amp. (0 < Amp < 200, 0 means no limit for Max. Amp)	0 (Amp.)	
PLC	<input checked="" type="checkbox"/> Enable	

## DSP

- *Jitter Buffer Control* – jitter buffer control settings;
  - *Min delay (ms)* – set minimum delay (ms);
  - *Max delay (ms)* – set maximum delay (ms);
  - *Optimization factor* – optimization factor.
- *LEC Tail Length (ms)* – set the echo cancellation delay before disconnecting (2-32 ms);
- *LEC (Line Echo Cancellation)* – enable echo cancellation;
- *NLP (Non-Linear Processing)* – enable non-linear echo cancellation;
- *VAD (Voice Activite Detector)* – enable voice activity detector;
- *VAD Amp. Threshold (0<Amp<200)* – setting the threshold by triggering VAD within 0<A<200;
- *SID Noise Level* – set SID noise level;
  - *Disable configuration* – set default value;
  - *Fixed noise level (0>Value>127dBov)* – setting a fixed noise level from 0 to 127dBV.
  - *Adjust noise level (-127~127dBov, 0:Not change)* – noise level setting (-127 ~ 127dBV, 0: unchanged)
- *CNG (Comfort Noise Generation)* – enable comfort noise generator;
- *CNG Amp. (0<Amp<200.0 means no limit for Max.Amp.)* – setting the gain value of comfortable noise;
- *PLC (Packet loss concealment)* – enable masking of lost packets.

RTCP	<input checked="" type="checkbox"/> Enable	Interval: <input type="text" value="10"/> (Sec)
RTCP XR	<input checked="" type="checkbox"/> Enable	
Fax/Modem RFC2833 Support	<input type="checkbox"/> Enable Fax/Modem RFC2833 Relay(For TX) <input type="checkbox"/> Enable Fax/Modem Inband Removal(For TX) <input type="checkbox"/> Enable Fax/Modem Tone Play(For RX)	
Speaker AGC	<input type="checkbox"/> Enable require level: <input type="text" value="1"/> <input type="button" value="v"/> Max gain up: dB <input type="text" value="6"/> <input type="button" value="v"/> Max gain down: dB <input type="text" value="-6"/> <input type="button" value="v"/>	
MIC AGC	<input type="checkbox"/> Enable require level: <input type="text" value="1"/> <input type="button" value="v"/> Max gain up: dB <input type="text" value="6"/> <input type="button" value="v"/> Max gain down: dB <input type="text" value="-6"/> <input type="button" value="v"/>	
Caller ID Mode	<input type="text" value="DTMF"/> <input type="button" value="v"/>	
FSK Date & Time Sync	<input type="checkbox"/> Enable	
Reverse Polarity before Caller ID	<input type="checkbox"/> Enable	
Short Ring before Caller ID	<input type="checkbox"/> Enable	

- *RTCP* – inclusion and selection of the RTCP protocol usage interval, s;
- *RTCP XR* – enable advanced RTCP reports;
- *Fax/Modem RFC2833 Support* – enable support for Fax/Modem RFC2833;
- *Speaker AGC, (dB)* – automatic adjustment of volume level, dB;
- *MIG AGC, (dB)* – automatic adjustment of microphone sensitivity level, dB;
- *Caller ID Mode* – select CallerID mode;
- *FSK Date&Time Sync* – enable time synchronization via FM;
- *Reverse Polarity before Caller ID* – enable inverting CallerID polarity;
- *Short Ring before Caller ID* – enable short call CallerID field.

Dual Tone before Caller ID	<input type="checkbox"/> Enable	
Caller ID Prior First Ring	<input checked="" type="checkbox"/> Enable	
Caller ID DTMF Start Digit	<input type="text" value="DTMF_A"/> <input type="button" value="v"/>	
Caller ID DTMF End Digit	<input type="text" value="DTMF_C"/> <input type="button" value="v"/>	
Flash Time Setting (ms) [ Space:10, Min:80, Max:2000 ]	<input type="text" value="80"/> < Flash Time < <input type="text" value="500"/>	
Speaker Voice Gain (dB) [ -32~31 ],Mute:-32	<input type="text" value="0"/>	
Mic Voice Gain (dB) [ -32~31 ],Mute:-32	<input type="text" value="0"/>	

- *Dual Tone before Caller ID* – enable double call before CallerID field;
- *Caller ID Prior First Ring* – inclusion of a double beep in front of the CallerID field;
- *Caller ID DTMF Start Digit* – setting the starting DTMF symbol of the CallerID;
- *Caller ID DTMF End Degit* – setting the ending DTMF symbol of the CallerID;
- *Flash Time Setting, (ms)* – setting Flash sending duration, ms;

- *Speaker Voice Gain (dB)* – setting the speaker volume, dB;
- *Mic Voice Gain (dB)* – setting the microphone sensitivity, dB.

#### 5.6.1.3 The "Tone" submenu. Country selection

VoIP → VoIP → Tone

Select Country	
Country	RUSSIAN ▼
<input type="button" value="Apply"/>	

- *Select Country* – regional settings.

#### 5.6.1.4 The "Other" submenu. Other VoIP settings

VoIP → VoIP → Other

Dial Option	
Auto Dial Time	5 ( 3~9 Sec, 0 is disable )
Dial-out by Hash Key	<input checked="" type="checkbox"/> Enabled
Off-Hook Alarm	
Off-Hook Alarm Time	10 ( 10~60 Sec, 0 is disable )
FXS Pulse Dial Detection	
Enable	<input type="checkbox"/>
Interdigit Pause Duration	450 (msec)
SIP setting	
SIP Prack	<input type="checkbox"/> Disabled
SIP Server Rendundacy	<input type="checkbox"/> Enabled
SIP CLIR anonymouse from header	<input type="checkbox"/> Enabled
Non-SIP INBOX call	<input type="checkbox"/> Enabled
Hook Flash Relay setting:	NONE ▼
SIP Min-SE	90 (Sec)
User = phone	<input checked="" type="checkbox"/> Enabled
# to %23	<input type="checkbox"/> Enabled
SIP OPTIONS	
Enable	<input type="checkbox"/>
Options interval time	0 (Sec)
<input type="button" value="Apply"/>	

#### Dial Option

- *Auto Dial Time* – the delay before the call ranges from 3-9 seconds, a value of 0 excludes the delay.
- *Dial-out by Hash Key* – calling a number using the hash key of the numbering plan. When the flag is set, the function is disabled.

## Off-Hook Alarm Time

- Off-Hook Alarm Time – setting the response time for the off-hook alarm from 10-60 seconds, a value of 0 disables the alarm.

## FXS Pulse Dial Detection

- *Enable* – enable/disable dial tone mode;
- *Interdigit Pause Duration (msec)* – setting the duration of the intersymbol pause, ms.

## SIP Setting

- *SIP Prack* – SIP provisional response. When the flag is set, the service is disabled;
- *SIP Server Rendundacy* – enable backup SIP server;
- *SIP CLIR anonymouse from header* – enable the anti-automatic caller ID (anti-Caller ID) service;
- *Non-SIP INBOX call* – outgoing call via analogue phone;
- *Hook Flash Relay setting* – setting up a short-term call reset;
- *SIP Min-SE* – session check interval;
- *User = phone* – enable the function of assigning a phone number to a user name;
- *# to %23* – enable the function of converting the # symbol.

## SIP OPTIONS

- *Enable* – enable/disable the use of the SIP message option;
- *Options interval time* – setting the interval for sending SIP messages.

### 5.6.1.5 The "Network" submenu

VoIP → VoIP → Network

DSCP Flag	
SIP DSCP	<input type="text" value="24"/> ( 0~63 )
RTP DSCP	<input type="text" value="46"/> ( 0~63 )
<input type="button" value="Apply"/>	

- *SIP DSCP* – set DHSP priority for SIP;
- *RTP DSCP* – set DHSP priority for RTP.



### 5.6.1.6 The "Call history" submenu

*VoIP → VoIP → Call history*

Call History						
Refresh						
No.	Status	From	To	Type	Duration	DateTime

- *No.* – sequence number of the entry;
- *Status* – call status;
- *From* – caller number;
- *To* – callee number;
- *Type* – call type;
- *Duration* – call duration;
- *Date Time* – call date.

To update the information, click the "Refresh" button.

### 5.6.1.7 The "Register Status" submenu

*VoIP → VoIP → Register Status*

VoIP Register Status		
Register Status		
Port	Number	Status
1		Disabled
Refresh		

- *Port* – port number;
- *Number* – user phone number;
- *Status* – registration status.

## 5.7 The "Advance" menu

### 5.7.1 The "Advance" submenu

#### 5.7.1.1 The "ARP Table" menu

This section shows a list of learned MAC addresses. The ARP efficiency depends a lot on ARP cache presented in every host. The cache contains Internet addresses and corresponding hardware addresses. Every record created in the cache is stored for 5 minutes.

*Advance → Advance → ARP table*

User List	
IP Address	MAC Address
192.168.1.2	00:e0:5c:36:0d:4f
Refresh	

- *IP Address* – IP address of the client;
- *MAC Address* – MAC address of the client.

To update the information, click the "Refresh" button.

#### 5.7.1.2 The "Bridging" submenu. Bridging parameters configuration

In this section you can configure bridge parameters. Here you can configure aging time of addresses in MAC table as well as to enable/disable 802.1d Spanning Tree.

*Advance → Advance → Bridging*

<b>Bridging</b>	
This page is used to configure the bridge parameters. Here you can change the settings or view some information on the bridge and its attached ports.	
Ageing Time:	<input type="text" value="7200"/> (seconds)
802.1d Spanning Tree:	<input type="checkbox"/> Enabled
<input type="button" value="Apply Changes"/> <input type="button" value="Show MACs"/>	

- *Ageing Time* – address lifetime (s);
- *802.1d Spanning Tree* – enable/disable 802.1d Spanning Tree protocol.

To save the changes, click the "Apply Changes" button.

To view the information about bridge and its connected ports click the "Show MACs" button.

*Advance → Advance → Bridging → Show MACs*

Bridge Forwarding Database			
This table shows a list of learned MAC addresses.			
Port	MAC Address	Is Local?	Ageing Timer
2	00-e0-5c-36-0d-4f	no	0.00
6	ec-b1-e0-31-32-1c	yes	---
6	ec-b1-e0-31-32-1c	yes	---
5	ec-b1-e0-31-32-1b	yes	---
5	ec-b1-e0-31-32-1b	yes	---
<div> <div>Refresh</div> <div>Close</div> </div>			

- *Port* – port number;
- *MAC Address* – MAC address;
- *Is Local* – local address;
- *Ageing Timer* – address lifetime.

To update the information in the table, click the "Refresh" button, to close the table, click "Close".

#### 5.7.1.3 The "Routing" submenu. Routing configuration

This submenu is used to configure static routing.

*Advance → Advance → Routing*

Routing						
This page is used to configure the routing information. Here you can add/delete IP routes.						
Enabled:	<input checked="" type="checkbox"/>					
Destination:	<input type="text"/>					
Subnet Mask:	<input type="text"/>					
Next Hop:	<input type="text"/>					
Metric:	<input type="text"/>					
Interface:	Any ▾					
<div> <div>Add Route</div> <div>Update</div> <div>Delete Selected</div> <div>Show Routes</div> </div>						
Static Route Table						
Select	State	Destination	Subnet Mask	Next Hop	Metric	Interface

To add the static route check "Enable", fill the corresponding fields and click "Add Route".

- *Enabled* – flag for route adding;
- *Destination* – destination address;
- *Subnet Mask* – subnet mask;
- *Next Hop* – next host;
- *Metric* – metric;
- *Interface* – interface.

Added static routes are displayed in the "Static Route Table". To update the information in the table, click the "Update" button, to delete the position from the table select it and click "Delete Selected".

To view the routes that the device often accesses, click the "Show Routes" button, then the "IP Route Table" will be displayed.

*Advance → Advance → Routing → Show Routes*

**IP Route Table**  
This table shows a list of destination routes commonly accessed by your network.

Destination	Subnet Mask	Next Hop	Metric	Interface
127.0.0.0	255.255.255.0	*	0	lo
192.168.1.0	255.255.255.0	*	0	br0
239.0.0.0	255.0.0.0	*	0	br0

< >

**Refresh** **Close**

To update the information in the table, click the "Refresh" button, to close the table, click "Close".

#### 5.7.1.4 The "Link mode" submenu. LAN ports configuration

In this submenu you can set the LAN ports operation mode. LAN1/2/3/4 – operation mode configuration; available modes: 10M Half Mode, 10M Full Mode, 100M Half Mode, 100M Full Mode and Auto Mode (auto-negotiation mode).

*Advance → Advance → Link mode*

**Ethernet Link Speed/Duplex Mode**

<b>LAN1:</b>	Auto Mode ▼
<b>LAN2:</b>	Auto Mode ▼
<b>LAN3:</b>	Auto Mode ▼
<b>LAN4:</b>	Auto Mode ▼

**Apply Changes**

To save the changes, click the "Apply Changes" button.

### 5.7.1.5 The "Others" submenu. JumboFrame enabling

In this submenu you can enable/disable JumboFrame by selecting or clearing the checkbox "Enable". You can also allow access to the local network and configure the USB port.

*Advance → Advance → Others*

Advanced	
IP PassThrough:	NONE ▾
Lease Time:	600 seconds
Allow LAN access:	<input type="checkbox"/>
JumboFrame:	<input checked="" type="checkbox"/> Enable
USB Settings:	USB3.0 may affect Wi-Fi 2.4G behaviour, please consider changing it to USB2.0 <input checked="" type="radio"/> USB2.0 <input type="radio"/> USB3.0
Detected devices:	
<b>Apply Changes</b>	

To save the changes, click the "Apply Changes" button.

## 5.7.2 The "IPv6" submenu. IPv6 configuration

### 5.7.2.1 The "IPv6 Enable/Disable" submenu

In this section you can enable/disable IPv6 operation by selecting or clearing the checkbox "Enable".

*Advance → IPv6 → IPv6 Enable/Disable*

IPv6 Configuration	
This page be used to configure IPv6 enable/disable	
IPv6:	<input checked="" type="checkbox"/> Enable

To save the changes, click the "Apply Changes" button.

### 5.7.2.2 The "RADVD" submenu. RADVD configuration

In this submenu you can configure RADVD (Router Advertisement Daemon).

*Advance → IPv6 → RADVD*

RADVD	
MaxRtrAdvInterval:	20
MinRtrAdvInterval:	10
AdvManagedFlag:	<input type="checkbox"/> on
AdvOtherConfigFlag:	<input checked="" type="checkbox"/> on
<b>Apply Changes</b>	

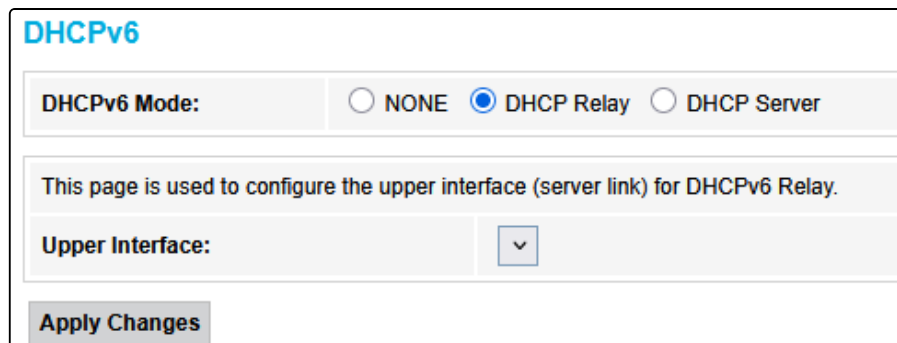
- *MaxRtrAdvInterval* – maximum RA (Router Advertisement) sending interval;
- *MinRtrAdvInterval* – minimum RA sending interval;
- *AdvManagedFlag* – enable/disable "Managed" flag sending in RA;
- *AdvOtherConfigFlag* – enable/disable Other RA flag sending.

To save the changes, click the "Apply Changes" button.

### 5.7.2.3 The "DHCPv6" submenu. DHCPv6 server configuration

This submenu is used to configure DHCPv6 server. By default, it operates in auto configuration mode (DHCPv6Server) via prefix delegation.

*Advance → IPv6 → DHCPv6*



The screenshot shows a web interface for DHCPv6 configuration. At the top, the title "DHCPv6" is displayed in blue. Below the title, there is a section labeled "DHCPv6 Mode:" with three radio button options: "NONE", "DHCP Relay" (which is selected), and "DHCP Server". A descriptive text box states: "This page is used to configure the upper interface (server link) for DHCPv6 Relay." Below this, there is a label "Upper Interface:" followed by a dropdown menu with a downward arrow. At the bottom of the form, there is a button labeled "Apply Changes".

- *DHCPv6 Mode* – enable/disable DHCPv6 server operation;
- *Upper Interface* – select interface.

To save the changes, click the "Apply Changes" button.

#### 5.7.2.4 The "MLD proxy" submenu. MLD proxy function configuration

In this section you can enable/disable MLD-proxy operation. For this you should check "Enable/Disable".

Advance → IPv6 → MLD proxy

MLD Proxy	
Robust Count:	<input type="text" value="2"/>
Query interval:	<input type="text" value="125"/> (Second)
Query response interval:	<input type="text" value="2000"/> (millisecond)
Response interval last group:	<input type="text" value="2"/> (Second)
<input type="button" value="Apply Changes"/>	

- *Robust Count* – the number of attempts to send an MLD message in case of packet loss;
- *Query Interval* – the time interval indicating the frequency of sending Query messages;
- *Query Response Interval* – the time interval indicating the delay in responding to the Query message from the client;
- *Response interval last group* – the number of Group-Specific messages sent after the last client leaves the group.

To save the changes, click the "Apply Changes" button.

#### 5.7.2.5 The "MLD snooping" submenu. MLD snooping function configuration

In this section you can enable/disable MLD-snooping operation. For this you should select "Enable".

Advance → IPv6 → MLD snooping

MLD Snooping	
MLD Snooping:	<input checked="" type="checkbox"/> Enable
<input type="button" value="Apply Changes"/>	

To save the changes, click the "Apply Changes" button.

### 5.7.2.6 The "IPv6 routing" submenu. IPv6 routes configuration

This section configures static IPv6 routes.

Advance → IPv6 → IPv6 routing

**IPv6 Static routing**  
 This page is used to configure the IPv6 static routing information. Here you can add/delete static IP routes.

Enabled:	<input checked="" type="checkbox"/>
Destination IP:	<input type="text"/>
Next Hop:	<input type="text"/>
Metric:	<input type="text"/>
Interface:	Any ▾

Add Route    Update    Delete Selected    Delete All    Show Routes

Select	State	Destination	Next Hop	Metric	Interface
--------	-------	-------------	----------	--------	-----------

- *Enable* – flag for route adding;
- *Destination IP* – destination address;
- *Next Hop* – next host;
- *Metric* – metric;
- *Interface* – interface.

To add IPv6 Routing, fill in the appropriate fields and click the "Add Route" button. Added routes are displayed in the table, to update the information click the "Update" button. To delete the whole table, click the "Delete All" button; To delete one route, select it and click the "Delete Selected" button. The "Show Routes" button displays a table of static IPv6 routes that the network typically accesses.

Advance → IPv6 → IPv6 routing → Show Routes

**IP Route Table**  
 This table shows a list of destination routes commonly accessed by your network.

Destination	Next Hop	Flags	Metric	Ref	Use	Interface
fe80::/64	::	U	256	3	0	br0
::1/128	::	U	0	4	0	lo
fe80::/128	::	U	0	3	0	br0
fe80::eeb1:e0ff:fe31:321a/128	::	U	0	5	0	br0
ff00::/8	::	U	256	4	0	br0

Refresh    Close

- *Destination* – destination network;
- *Next Hop* – next host;
- *Flags* – flags;
- *Metric* – metric;
- *Ref* – route source;
- *Use* – route usage;
- *Interface* – interface through which the specified route is available.

To update the table click "Refresh"; to close it click "Close".



### 5.7.2.7 The "IP/Port filtering" submenu. Packet filtering configuration

Use this page to configure the filtering of data packets transmitted through the gateway.

Advance → IPv6 → IP/Port filtering

## IP/Port Filtering

Entries in this table are used to restrict certain types of data packets through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Outgoing Default Action:

☐ Deny
 ☒ Allow

Incoming Default Action:

☒ Deny
 ☐ Allow

Apply Changes

Direction:

Outgoing ▾

Protocol:

TCP ▾

Rule Action:

☒ Deny
 ☐ Allow

Source IP Address:

-

Source Prefix Length:

Destination IP Address:

-

Destination Prefix Length:

Source Port:

-

Destination Port:

-

Add

Current Filter Table

Select	Direction	Protocol	Source IP Address	Source Port	Destination IP Address	Destination Port	Interface	Rule Action
<div> <div>Delete Selected</div> <div>Delete All</div> </div>								

- *Outgoing/Incoming Default Action* – default action:
  - *Deny* – when checked, traffic pass is prohibited by default;
  - *Allow* – when checked, traffic pass is allowed by default;

To save the changes, click the "Apply Changes" button.

- *Direction (Outgoing/Incoming)* – select traffic direction;
- *Protocol* – select protocol;
- *Rule Action (Deny/Allow)* – traffic processing policy;
- *Source IP Address* – source IP:
  - *Source Prefix Length*;
  - *Source Port* – source port;
- *Destination IP Address* – destination IP:
  - *Source Port* – source port;
  - *Destination Port* – destination port.

To add a filter fill the corresponding fields and click the "Add" button. Added filters are displayed in the "Current Filter Table". To delete the whole table, click the "Delete All" button; To delete one filter, select it and click the "Delete Selected" button.

## 5.8 The "Diagnostics" menu

Diagnostics section of access to various network nodes.

### 5.8.1 The "Diagnostics" submenu

#### 5.8.1.1 The "Ping" submenu. Checking the Availability of Network Devices

Use this menu to test the availability of network devices with Ping utility.

*Diagnostics → Diagnostics → Ping*

**Ping**

This page is used to send ICMP ECHO\_REQUEST packets to network host. The diagnostic result will then be displayed.

Host Address:	<input type="text"/>
WAN Interface:	Any ▾

Ping IPv4
Ping IPv6

To test the availability of the connected device, enter its IP address into the "Host Address" field and click the "Ping IPv4" or "Ping IPv6" button.

#### 5.8.1.2 The "Traceroute" submenu

This submenu is intended for network diagnostics by sending UDP packets and receiving a message about port availability/inaccessibility.

*Diagnostics → Diagnostics → Traceroute*

**Traceroute**

This page is used to print the route packets trace to network host. The diagnostic result will then be displayed.

Protocol:	ICMP ▾
Host Address:	<input type="text"/>
Number Of Tries:	<input type="text" value="3"/>
Time out:	<input type="text" value="5"/> s
Data Size:	<input type="text" value="56"/> Bytes
DSCP:	<input type="text" value="0"/>
Max HopCount:	<input type="text" value="30"/>
WAN Interface:	Any ▾

Traceroute IPv4
Traceroute IPv6

- *Protocol* – the protocol used for tracing;
- *Host Address* – the address of the device to which tracing will be performed;
- *Number of Tries* – the number of tracing attempts;
- *Time out* – packet response timeout;
- *Data Size* – the size of the packet data in bytes;
- *DSCP* – the value of Differentiated services codepoint in the packets being sent;
- *Max HopCount* – the maximum number of nodes for routing a packet;
- *WAN Interface* – the interface through which tracing will be performed.

To display the path of the information packet from its source to its destination, you should enter its IP address in the "Host Address" field, specify the other parameters and click the "Traceroute IPv4" or "Traceroute IPv6" button.

## 5.9 The "Admin" submenu

Device management section. In this menu, you can configure passwords, time, configurations, etc.

### 5.9.1 The "Admin" submenu. Configuration restore and reset

#### 5.9.1.1 The "Commit/Reboot" submenu. Saving changes and rebooting the device

Click the "Commit and Reboot" button to reboot the device or to save changes in system memory. The rebooting process takes a few minutes to complete.

*Admin → Admin → Commit/Reboot*

Commit and Reboot	
This page is used to commit changes to system memory and reboot your system.	
Commit and Reboot:	<button>Commit and Reboot</button>

#### 5.9.1.2 The "Multi-lingual Settings" submenu. Selecting the interface language

Use the "Language Select" field to set the language of the device's web interface and click the "Apply Changes" button to save the changes.

*Admin → Admin → Multi-lingual Settings*

Multi-Lingual Setting	
This page is used to set multi-lingual.	
Language Select:	<input type="text" value="English"/>
<button>Apply Changes</button>	

#### 5.9.1.3 The "Backup/Restore" submenu

*Admin → Admin → Backup/Restore*

Backup and Restore Settings	
This page allows you to backup current settings to a file or restore the settings from the file which was saved previously. Besides, you could reset the current settings to factory default.	
Backup Settings to File:	<button>Backup...</button>
Backup Settings to encrypted File:	<button>Backup...</button>
Restore Settings from File:	<div>Обзор... Файл не выбран.</div> <div><button>Restore</button></div>
Reset Settings to Default:	<button>Reset</button>

In this section, you can copy the current settings to a file by clicking the "Backup" button ("Backup Settings to File") or copy them via encryption mode ("Backup Settings to encrypted File"). It is also possible to restore the settings from a file that was saved earlier ("Restore Settings from a File") by clicking the "Restore" button and reset the current settings to factory defaults by clicking the "Reset" button.

#### 5.9.1.4 The "Password" submenu. Access control configuration (setting passwords)

In this section you can change a password to access the device.

*Admin → Admin → Password*

Password	
This page is used to set the account to access the web server of ADSL Router. Empty user name and password will disable the protection.	
Login User:	user
Old Password:	<input type="password"/>
New Password:	<input type="password"/>
Confirmed Password:	<input type="password"/>
<input type="button" value="Apply Changes"/> <input type="button" value="Reset"/>	

To change the password, enter the existing password in the "Old Password" field, then the new password in "New Password" and confirm it with "Confirmed Password".


To confirm and save changes, click the "Apply changes" button. Click the "Reset" button to reset the value.

#### 5.9.1.5 The "Firmware Upgrade" submenu. Firmware Update

To update firmware, select firmware file by clicking the "Select file" button and click "Upgrade". To reset the value, click the "Reset" button.

*Admin → Admin → Firmware Upgrade*

Firmware Upgrade	
This page allows you upgrade the firmware to the newer version. Please note that do not power off the device during the upload because this make the system unbootable.	
<input type="button" value="Обзор..."/> Файл не выбран.	
<input type="button" value="Upgrade"/> <input type="button" value="Reset"/>	

 Do not switch off or reboot the device during the update. The process may take several minutes. The device will be automatically rebooted when the update is completed.

5.9.1.6 The "Remote Access" submenu

In this section you can configure remote access rules via HTTP/ICMP protocols.

Admin → Admin → Remote Access

Remote Access

This page is used to configure the IP Address for Access Control List. If remote access is enabled, only the IP address in the remote access Table can access CPE. Here you can add/delete the IP Address.

Enabled:

☐

Interface:

LAN ▾

IP Address:

Subnet Mask:

Protocol:

▾

Add

Remote Access Table

Select	State	Interface	IP Address	Services	Port
<input type="radio"/>	Enabled	LAN	0.0.0.0/0	HTTP	80
<input type="radio"/>	Enabled	LAN	0.0.0.0/0	ICMP	N/A
<input type="radio"/>	Enabled	LAN	0.0.0.0/0	HTTPS	443

- Enabled – enabling the rule to add;
  - Interface – interface to which the rule applies;
  - IP Address – source IP address;
  - Subnet Mask – subnet mask;
  - Protocol – destination port.

To add a rule fill the corresponding fields and click the "Add" button. Added rules are displayed in the "Remote Access Table". To activate/deactivate the selected rule, click the "Toggle selected" button. To delete one rule, select it with a flag in the Select column and click the "Delete Selected" button.

### 5.9.1.7 The "Time Zone" submenu. System time configuration

In this section you can configure the device system time. Synchronization with accurate online time-servers is available.

*Admin → Admin → Time Zone*

**Time Zone Configuration**  
 You can maintain the system time by synchronizing with a public time server over the Internet.

<b>Current Time :</b>	Year <input type="text" value="1970"/> Mon <input type="text" value="1"/> Day <input type="text" value="8"/> Hour <input type="text" value="6"/> Min <input type="text" value="2"/> Sec <input type="text" value="35"/>
<b>Time Zone Select :</b>	<input type="text" value="Africa/Blantyre (UTC+02:00)"/>
<b>Enable Daylight Saving Time</b>	<input checked="" type="checkbox"/>
<b>Enable SNTP Client Update</b>	<input type="checkbox"/>
<b>WAN Interface:</b>	<input type="text" value="Any"/>
<b>SNTP Server :</b>	<input checked="" type="radio"/> <input type="text" value="clock.fmt.he.net"/> <input type="radio"/> <input type="text"/> (Manual Setting)
<b>SNTP Interval:</b>	<input type="text" value="86400"/> (seconds)

Refresh

- *Current Time* – current time;
- *Time Zone Select* – timezone;
- *Enable Daylight Saving Time* – enable daylight saving time;
- *Enable SNTP Client Update* – enable time synchronization via SNMP;
- *WAN Interface* – interface for time update;
- *SNTP Server* – preferred time server;
- *SNTP Interval* – NTP server synchronization interval.

To save the changes click the "Apply Changes" button, to update the information click "Refresh".

## 5.10 The "Statistics" menu

### 5.10.1 The "Statistics" submenu

#### 5.10.1.1 The "Interface" submenu

This section displays timers/errors for packets for each interface.

*Statistics → Statistics → Interface*

Interface Statistics						
This page shows the packet statistics for transmission and reception regarding to network interface.						
Interface Statistics						
Interface	Packets Sent			Packets Received		
	Rx pkt	Rx err	Rx drop	Tx pkt	Tx err	Tx drop
LAN1	0	0	0	0	0	0
LAN2	235466	0	0	235449	0	0
LAN3	0	0	0	0	0	0
LAN4	0	0	0	0	0	0
WLAN 2.4GHz	0	0	0	0	0	0
WLAN 5GHz	0	0	0	0	0	0
Refresh						

- *Interface* – interface;
- *Rx pkt* – packets received;
- *RX err* – errors on receive;
- *Rx drop* – rejected on receive;
- *Tx pkt* – packets sent;
- *Tx err* – transmission error;
- *Tx drop* – rejected on transmission.

### 5.10.1.2 The "PON Statistics" submenu

This section displays timers for the optical interface.

*Statistics → Statistics → PON Statistics*

PON Statistics	
Bytes Sent:	0
Bytes Received:	0
Packets Sent:	0
Packets Received:	0
Unicast Packets Sent:	0
Unicast Packets Received:	0
Multicast Packets Sent:	0
Multicast Packets Received:	0
Broadcast Packets Sent:	0
Broadcast Packets Received:	0
FEC Errors:	0
HEC Errors:	0
Packets Dropped:	0
Pause Packets Sent:	0
Pause Packets Received:	0



## 6 List of changes

Document version	Suitable firmware version	Issue date	Revisions
Version 1.2	3.4.2	03.2025	Third issue
Version 1.1	3.4.1	10.2024	Second issue
Version 1.0	3.4.0	06.2024	First issue

## TECHNICAL SUPPORT

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

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

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

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

Download Center: <http://www.eltex-co.com/support/downloads/>