

## Optical network terminals

**NTU-RG-1421G-Wac   NTU-RG-1431G-Wac**  
**NTU-RG-1421GC-Wac   NTU-RG-1421G-WZ**

---

Operation Manual, version 1.4 (June 2018)  
Firmware version 3.32.0

IP address: 192.168.1.1  
User name: user  
password: user

Document version	Suitable firmware version	Issue date	Revisions
Version 1.3	3.30.0		Fourth issue
Version 1.2	3.28.2	July 2017	Third issue
Version 1.1	3.28.1	December 2016	Second issue
Version 1.0	3.28.0	August 2016	First issue

## NOTES AND WARNINGS



Notes contain important information, tips or recommendations on device operation and setup.



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

## CONTENTS

1 INTRODUCTION .....	5
2 PRODUCT DESCRIPTION .....	6
2.1 Purpose .....	6
2.2 Models.....	7
2.3 Device Specification .....	7
2.4 Main Specifications .....	10
2.5 Design.....	12
2.5.1 NTU-RG-1421G-Wac/NTU-RG-1421G-WZ/NTU-RG-1431G-Wac.....	12
2.5.2 NTU-RG-1421GC-Wac .....	13
2.6 LED Indication.....	14
2.6.1 NTU-RG-1421G-Wac, NTU-RG-1421G-WZ, NTU-RG-1431G-Wac .....	14
2.6.2 NTU-RG-1421GC-Wac .....	15
2.6.3 Indication of LAN Interfaces .....	16
2.7 Reboot/Reset to factory defaults .....	16
2.8 Delivery Package .....	16
3 ARCHITECTURE OF DEVICES .....	17
3.1 NTU-RG architecture .....	17
4 CONFIGURATION OF NTU-RG-1421G-WAC, NTU-RG-1421G-WZ, NTU-RG-1431G-W AND NTU-RG-1421GC-W VIA WEB INTERFACE. USER ACCESS.....	19
4.1 The “Device Info” menu .....	20
4.1.1 The “Summary” submenu .....	20
4.1.2 The “WAN” submenu. The Status of Services.....	20
4.1.2.1 The “General” submenu. General information.....	20
4.1.2.2 The “Detail” submenu. Detailed Information .....	21
4.1.3 The “LAN” submenu. Monitoring of LAN Ports. Monitoring of Wi-Fi Interface Status .....	21
4.1.4 The “Statistics” submenu. Traffic flow information for device ports .....	21
4.1.5 The “Route” submenu. Routing table preview .....	22
4.1.6 The “ARP” submenu. Display of the ARP Protocol Cache .....	23
4.1.7 The “DHCP” submenu. Active DHCP leases.....	23
4.1.8 The “Wireless Stations” submenu. Connected wireless devices .....	24
4.1.9 The “Wireless Monitor” submenu. Discovered Wi-Fi networks .....	24
4.1.10 The “Voice” submenu. Monitoring of telephone ports .....	25
4.2 The “Advanced Setup” menu. Advanced configuration.....	25
4.2.1 The “LAN” submenu. Configuration of Main Parameters.....	25
4.2.2 The “NAT” submenu. NAT Settings .....	26
4.2.2.1 The “Virtual Servers” submenu. Virtual server settings .....	26
4.2.2.2 The “Port Triggering” submenu. Port Triggering Settings.....	27
4.2.2.3 The “DMZ Host” submenu. Demilitarized Zone Settings .....	29
4.2.3 The “Security” submenu. Security Settings.....	29
4.2.3.1 The “IP Filtering” submenu. Address Filtering Settings .....	29
4.2.3.2 The “MAC Filtering Setup” submenu. Filtering Settings for MAC Addresses .....	31
4.2.4 The “Parental Control” submenu: restriction settings.....	32
4.2.4.1 The “Time Restriction” submenu. Session Time Restriction Settings .....	32
4.2.4.2 The “Url Filter” submenu. Internet Access Restriction Settings .....	33
4.2.5 The “Dynamic DNS” submenu. Dynamic DNS Configuration .....	34
4.2.6 The “Print Server” submenu. Print Server Configuration .....	37
4.2.7 The “DLNA” submenu. DLNA server configuration .....	37
4.2.8 The “Z-Wave” menu .....	38
4.2.9 The “UPnP” submenu. Autoconfiguration of network devices.....	38
4.3 The “Wireless” menu. Wireless network configuration.....	39
4.3.1 The “Basic” submenu. General settings .....	39

4.3.2 The “Security” submenu. Security settings .....	40
4.3.3 The “MAC Filtering” submenu. Filtering Settings of MAC Addresses .....	43
4.3.4 The “Wireless Bridge” submenu. Wireless Connection Settings in Bridge Mode.....	44
4.3.5 The “Advanced” submenu.....	45
4.3.6 The “Connection wizard” submenu .....	47
4.4 The “Storage Service” menu. File storage service .....	47
4.4.1 The “Storage Device Info” submenu. Information about connected USB devices.....	47
4.4.2 The “User Accounts” submenu. Configuration of Samba users.....	47
4.5 The “Management” menu. Device Management .....	48
4.5.1 The “Settings” submenu.....	48
4.5.1.1 The “Restore Default” submenu.....	48
4.5.2 The “PON Password” submenu. Change the PON access password .....	49
4.5.3 The “Internet time” submenu. System Time Settings .....	49
4.5.4 The “Ping” submenu. Test the Availability of Network Devices .....	50
4.5.5 The “Password” submenu. Access control configuration (setting passwords).....	50
4.5.6 The “System Log” submenu. System Log Review and Configuration .....	51
4.5.6.1 The “Configuration” submenu. System Log Configuration .....	51
4.5.6.2 The “View” submenu. System Log Display.....	52
4.5.7 The “Update Software” submenu.....	52
4.5.8 The “Reboot” submenu. Device Reboot .....	52
NTU-RG ACCEPTANCE CERTIFICATE AND WARRANTY .....	53

## 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 for the 'last mile' issue that significantly reduces the required amount of cable and provides data transfer with downlink rate up to 2.5Gbps and uplink rate up to 1.25Gbps. 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 is designed to connect terminal equipment of user to broadband access services. ONT device can be used in residential estates and offices.

The range of ONT NTU equipment produced by ELTEX comprises of the following terminals:

- NTU-RG-1421G-Wac, NTU-RG-1431 G-Wac, NTU-RG-1421GC-Wac and NTU-RG-1421G-WZ, which are designed to support four UNIs: 10/100/1000Base-T, FXS, Wi-Fi, USB, CaTV<sup>1</sup> and Z-Wave<sup>2</sup>.

This operation manual describes intended use, key specifications, configuration, monitoring, and firmware update for *NTU-RG* optical terminal series.

---

<sup>1</sup> Only for NTU-RG-1421GC-Wac

<sup>2</sup> Only for NTU-RG-1421G-WZ

## 2 PRODUCT DESCRIPTION

### 2.1 Purpose

NTU-RG GPON ONT (Gigabit Ethernet Passive Optical Network) devices represent high-performance network terminals designed for connection with upstream GPON equipment and providing end user with broadcast access services. GPON connection is established through PON interface, while Ethernet interfaces are used for connection of terminal equipment.

The key GPON advantage is the optimal use of bandwidth. The technology is the next step of high-speed Internet applications for home and office. Being designed for home or office network deployment, these ONT devices provide users, who live and work in distant flat buildings and business centres, with reliable connection with high throughput at large distances.

With built-in router, these devices enable connection of local network equipment to 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, blocks domains and allows for compilation of a schedule of Internet use. 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 connection of USB devices (USB flash drives, external HDD).

NTU-RG-1421G-Wac, NTU-RG-1431G-Wac, NTU-RG-1421GC-Wac and NTU-RG-1421G-WZ network routers allow Wi-Fi clients to be connected using IEEE 802.11a/b/g/n/ac standard. 802.11ac standard support ensures data transfer rate of 1.3 Gbps 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 2.4GHz and 5GHz dual-band operation.

NTU-RG-1421GC-Wac has a built-in RF port to connect digital and analogue TV (if the service is provided by your service operator).

NTU-RG-1421G-WZ comes with Z-Wave module, which is used for “Smart Home” service providing.

Z-Wave is a wireless radio technology with low power consumption, which was designed specially for remote control. In contrast with Wi-Fi and others IEEE 802.11 data transmission standards, that were designed for large data streams, Z-Wave operates within frequency range up to 1 GHz and is optimized for the transmission of simple control commands with low delays (for example, turn on/off, modify the volume, brightness, etc.). The choice of low radio-frequency range for Z-Wave is caused by a small quantity of potential interfering sources (in contrast with the high-usage 2.4 GHz band, which requires measures reducing possible interferences from different home wireless appliances - Wi-Fi, ZigBee, Bluetooth).

Z-Wave is designed for creation of affordable and power-efficient consumer electronics, including battery-operated devices such as remote controllers, smoke sensors, temperature sensors, humidity sensors, motion sensors and other protective sensors.

## 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	Z-Wave	RF	Wi-Fi 802.11 b/g/n	Wi-Fi 802.11 b/g/n/ac	USB
NTU-RG-1421G-Wac	1xGPON	4x1Gigabit	1	-	-	+	802.11n, 2*2 -300Mbps –2.4GHz 802.11ac, 3*3 -1.3Gbps – 5 GHz+	2
NTU-RG-1431G-Wac	1xGPON	4x1Gigabit	1	-	-	+	802.11n, 3*3 -450Mbps - 2.4GHz 802.11ac, 3*3 -1.3Gbps – 5 GHz	2
NTU-RG-1421GC-Wac	1xGPON	4x1Gigabit	1	-	1	+	802.11n, 2*2 -300Mbps –2.4GHz 802.11ac, 3*3 -1.3Gbps – 5 GHz+	1
NTU-RG-1421G-WZ	1xGPON	4x1Gigabit	1	1	-	+	802.11n, 2*2 -300Mbps –2,4GHz 802.11ac, 3*3 -1.3Gbps – 5 GHz+	2

## 2.3 Device Specification

**The device is equipped with the following interfaces:**

- 1 x RJ-11 port for analogue phone units;
- 1 x PON SC/APC port for connection to operator's network;
- Ethernet RJ-45 LAN ports for connection of network devices:
  - 4 x RJ-45 10/100/1000Base-T ports.
- 802.11a/b/g/n/ac Wi-Fi transceiver;
- 2<sup>1</sup> x USB 2.0 ports for external USB or HDD storage;
- Z-Wave submodule<sup>2</sup>;
- 1 RF port for CaTV connection<sup>3</sup>.

The terminal uses an external adapter for 220V/12V power supply.

**The device supports the following functions:**

- **Network functions:**
  - Operation in 'bridge' or 'router' mode;
  - PPPoE support (PAP, CHAP, MSCHAP authentication);
  - Static IP address and DHCP support (DHCP client on WAN, DHCP server on LAN);
  - UPnP;
  - IPSec;
  - NAT support;
  - Firewall support;
  - NTP support;
  - QoS support;
  - IGMP snooping support;
  - IGMP proxy support;
  - Parental Control;
  - Storage Service support;
  - UPNP, SMB, FTP, DLNA, Print Server support;
  - VLAN complying with IEEE 802.1Q.

<sup>1</sup> NTU-RG-1421GC-Wac has one USB2.0 port

<sup>2</sup> For NTU-RG-1421G-WZ

<sup>3</sup> For NTU-RG-1421GC-Wac

- *Wi-Fi:*
  - 802.11 a/b/g/n/ac standard support;
  - Simultaneous dual-band operation: 2.4GHz and 5GHz.
- *VoIP:*
  - SIP protocol support;
  - Audio codecs: G.729 (A), G.711(A/U), G.723.1;
  - ToS for RTP packets;
  - ToS for SIP packets;
  - Echo cancellation (G.164, G.165 guidelines);
  - Silence detector (VAD);
  - Comfortable noise generator;
  - DTMF signals detection and generation;
  - DTMF transmission (INBAND, RFC2833, SIP INFO);
  - Fax transmission: upspeed/pass-through G.711, T.38.
- *Value Added Services:*
  - Call Hold;
  - Call Transfer;
  - Call Waiting Notification;
  - Forward Unconditionally;
  - Forward on 'No Answer';
  - Forward on 'Busy';
  - Caller ID Display for ETSI FSK;
  - Caller ID Barring (Anonymous calling);
  - Warmline;
  - Flexible numbering plan;
  - Voice mail notifications (MWI);
  - Anonymous Call Blocking;
  - Call Barring;
  - Do not Disturb (DND).
- *Firmware update via web interface, TR-069, OMCI*
- *Remote monitoring, configuration, and setup:*
  - TR-069;
  - Web interface;
  - OMCI;
  - Telnet.



Figures 1, 2 show equipment use case for NTU-RG equipment.

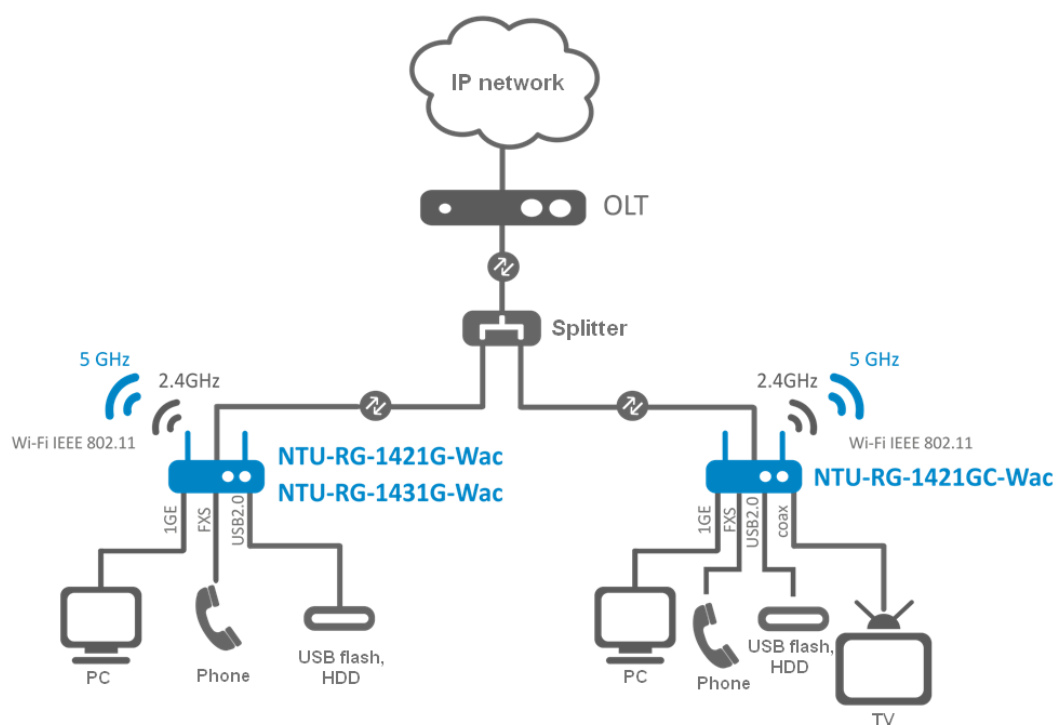


Figure 1 – Use case for NTU-RG-1421G-Wac, NTU-RG1431G-Wac, and NTU-RG-1421GC-Wac

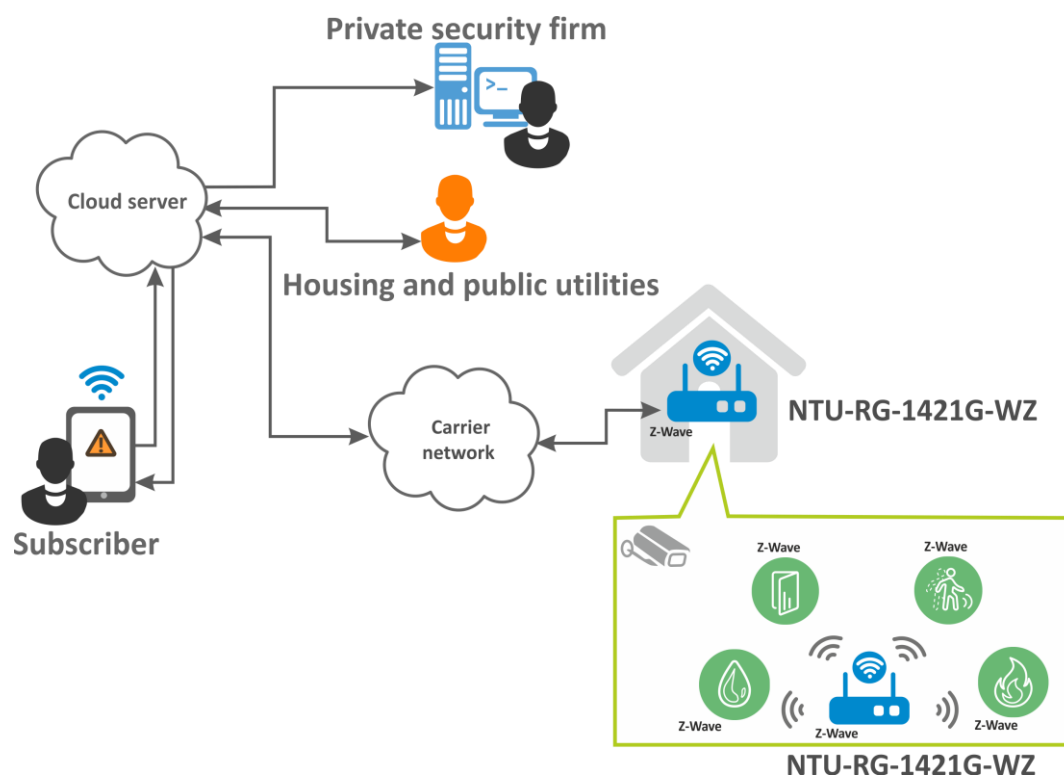


Figure 2 – Use case for NTU-RG-1421G-WZ

## 2.4 Main Specifications

Table 2 lists 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 Interface

Number of interfaces	4
Electric port	RJ-45
Data rate, Mbps	Autodetection, 10/100/1000 Mbps duplex/half-duplex
Supported 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

### PON Interface Specifications

Number of PON interfaces	1
Supported 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 Complies with ITU #T G.984.2
Transmission medium	Fibre optical cable SMF - 9/125, G.652
Splitting ratio	up to 1:128
Maximum range of coverage	20 km
Transmitter:	1310nm
Upstream connection speed	1244Mbps
Transmitter power	from +0.5 to +5 dBm
Optical spectrum width (RMS)	1 nm
Receiver	1490nm
Downstream connection speed	2488Mbps
Receiver sensitivity	from -8 to -28 dBm

### Parameters of analogue user ports

Number of ports	1
Loop resistance	up to 2kΩ
Dialling	pulse/frequency (DTMF)
Caller ID display	yes

### Wi-Fi Interface Specifications

Model	NTU-RG-1421G-Wac, NTU-RG-1421GC-Wac, NTU-RG-1421G-WZ	NTU-RG-1431G-Wac
Standard	802.11a/b/g/n/ac	802.11a/b/g/n/ac

Frequency range	2400 ~ 2483.5MHz, 5150 ~ 5350MHz, 5650 ~ 5850MHz Simultaneous dual-band operation	2400 ~ 2483.5MHz, 5150 ~ 5350MHz, 5650 ~ 5850MHz Simultaneous dual-band operation
Modulation	CCK, BPSK, QPSK, 16 QAM, 64 QAM, 256 QAM	CCK, BPSK, QPSK, 16 QAM, 64 QAM, 256 QAM
Data rate, Mbps	– 802.11b/g/n: 1-13 – 802.11a/ac: 36-64, 132-165  – 802.11b: 1, 2, 5.5 and 11Mbps – 802.11g: 6, 9, 12, 18, 24, 36, 48 and 54Mbps – 802.11n: 300Mbps (20MHz channel), 450Mbps (40MHz channel) – 802.11ac: 1300Mbps (80MHz)	– 802.11b/g/n: 1-13 – 802.11a/ac: 36-64, 132-165  – 802.11b: 1, 2, 5.5 and 11Mbps – 802.11g: 6, 9, 12, 18, 24, 36, 48 and 54Mbps – 802.11n: 300Mbps (20MHz channel), 450Mbps (40MHz channel) – 802.11ac: 1300Mbps (80MHz)
Maximum transmitter output power	– 802.11b (11Mbps): 17dBm – 802.11g (54Mbps): 15dBm – 802.11n (MCS7): 15dBm – 802.11ac (5GHz): 19dBm	
MAC protocol	CSMA/CA, ACK 32 MAC model	
Security	64/128 bit WEP encryption WPA, WPA2 802.1x AES & TKIP	
Supported operating systems	Windows XP 32/64, Windows Vista 32/64, Windows 2000, Windows 7 32/64 Linux, VxWorks	
MIMO	NTU-RG-1421G-Wac	2.4 GHz - 2x2, 5 GHz - 3x3
	NTU-RG-1431G-Wac	2.4 GHz - 3x3, 5 GHz - 3x3
	NTU-RG-1421GC-Wac	2.4 GHz - 2x2, 5 GHz - 3x3
	NTU-RG-1421G-WZ	2.4 GHz - 2x2, 5 GHz - 3x3
Antenna gain	5dBi	
Operating temperature range	from 0 to +70 C	

### Control

Local control	Web interface
Remote control	Telnet, TR-069, OMCI
Firmware update	OMCI, TR-069, HTTP, TFTP
Access restriction	password

### General parameters

Power supply	12V DC /220 AC power adapter	
Power consumption	NTU-RG-1421G-Wac	15 W max
	NTU-RG-1431G-Wac	15 W max
	NTU-RG-1421GC-Wac	15 W max
	NTU-RG-1421G-WZ	15 W max
Operating temperature range	from +5 to +40 C	
Relative humidity	up to 80%	
Dimensions	NTU-RG-1421G-Wac	187x120x32mm
	NTU-RG-1431G-Wac	187x120x32 mm
	NTU-RG-1421GC-Wac	217x120x49 mm
	NTU-RG-1421G-WZ	187x120x32 mm
Weight	0.3kg	

## 2.5 Design

### 2.5.1 NTU-RG-1421G-Wac/NTU-RG-1421G-WZ/NTU-RG-1431G-Wac

Network terminal is a desktop device enclosed in plastic housing.

The rear panel of the device is shown in Figure 3.

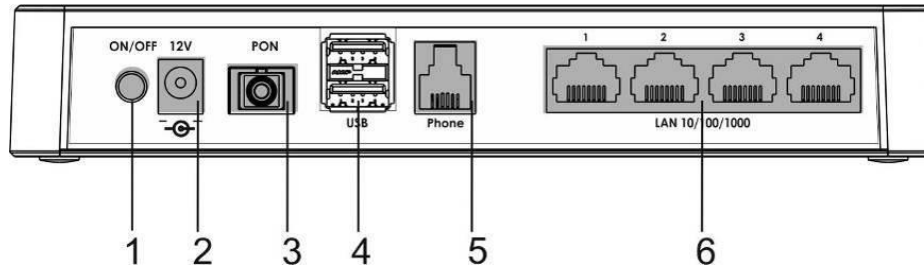


Figure 3 – NTU-RG-1421G-Wac, NTU-RG-1421G-WZ, NTU-RG-1431G-Wac rear panel layout

Connectors and controls located on the rear panel of are listed in Table 3.

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

No.	Rear Panel Element	Description
1	<b>On/Off</b>	power button
2	<b>12V</b>	power adapter connector
3	<b>PON</b>	SC port (socket) for PON with GPON interface
4	<b>USB</b>	2 ports for connecting external drives and other USB devices
5	<b>Phone</b>	RJ-11 port for connecting analogue phone
6	<b>LAN 10/100/1000 1..4</b>	4 RJ-45 ports for connecting network devices

Figures 4, 5 show NTU-2(V) side and top panels.

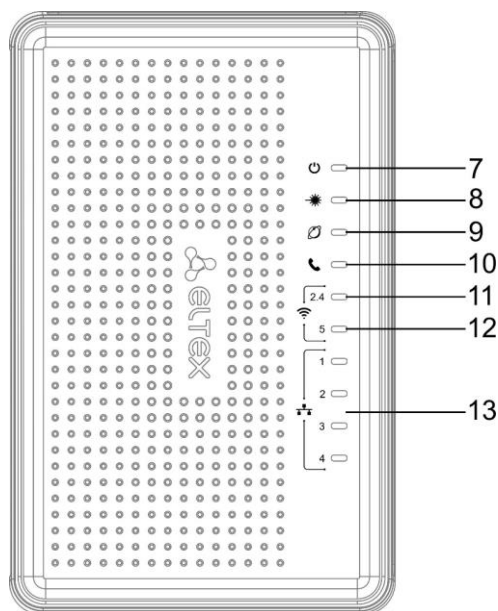


Figure 4 – NTU-RG Top Panel

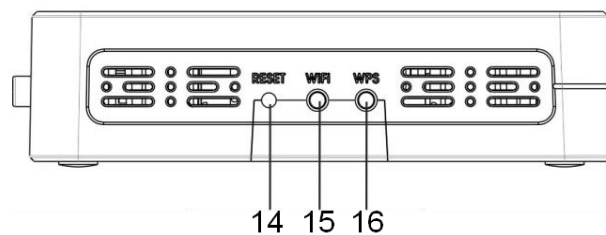









Figure 5 – NTU-RG Side Panel

Top panel LED indicators are listed in Table 4.

Table 4 – Description of Top Panel LEDs

No.	Top Panel Element	Description
7		power and activity status indicator
8		optical interface activity indicator
9		Internet service status indicator
10		FXS port activity indicator
11		Wi-Fi activity indicator for 2.4GHz
12		Wi-Fi activity indicator for 5GHz
13		Ethernet port indicator

Side panel buttons are listed in Table 5.

Table 5 – Description of Side Panel Buttons

No.	Side Panel Element	Description
14	<b>Reset</b>	functional key that reboots the device and resets it to the factory settings
15	<b>Wi-Fi</b>	Wi-Fi enabling/disabling button
16	<b>WPS</b>	enables automatically protected Wi-Fi connection for device

## 2.5.2 NTU-RG-1421GC-Wac

Subscribe terminal is designed as a desktop device in a plastic housing.

Figure 6 shows the device rear panel layout.

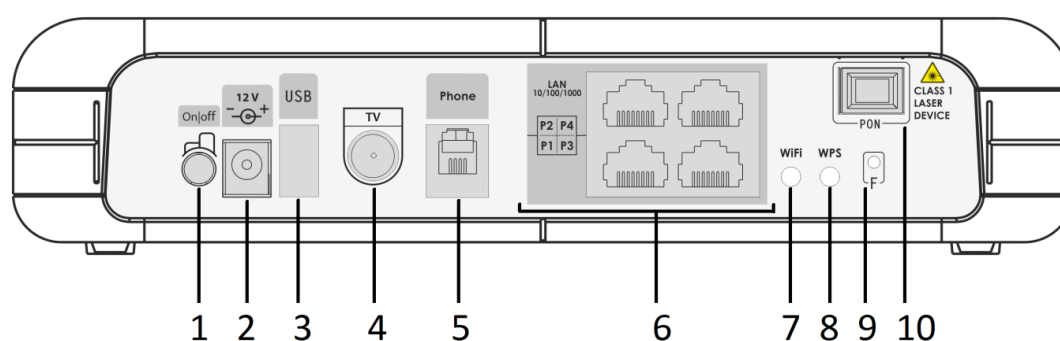


Figure 6 – The NTU-RG-1421GC-Wac rear panel layout

The connectors and controls located on the device rear panel are listed in Table 6.

Table 6 – Description of the connectors and controls of the device rear panel

No.	Rear Panel Element	Description
1	<b>On/Off</b>	power button
2	<b>12V</b>	power adapter connector
3	<b>USB</b>	port for connecting external drivers and other USB devices
4	<b>TV</b>	RF port for CaTV connection

5	<b>Phone</b>	RJ-11 port for connecting analogue phone
6	<b>LAN 10/100/1000 1..4</b>	4 RJ-45 ports for connecting network devices
7	<b>Wi-Fi</b>	Wi-Fi enabling/disabling button
8	<b>WPS</b>	enables automatically protected Wi-Fi connection for the device
9	<b>F</b>	functional key that reboots and resets the device to the factory settings
10	<b>PON</b>	SC port (socket) for PON with GPON interface

Figure 7 shows the NTU-RG-1421GC-Wac front panel layout.

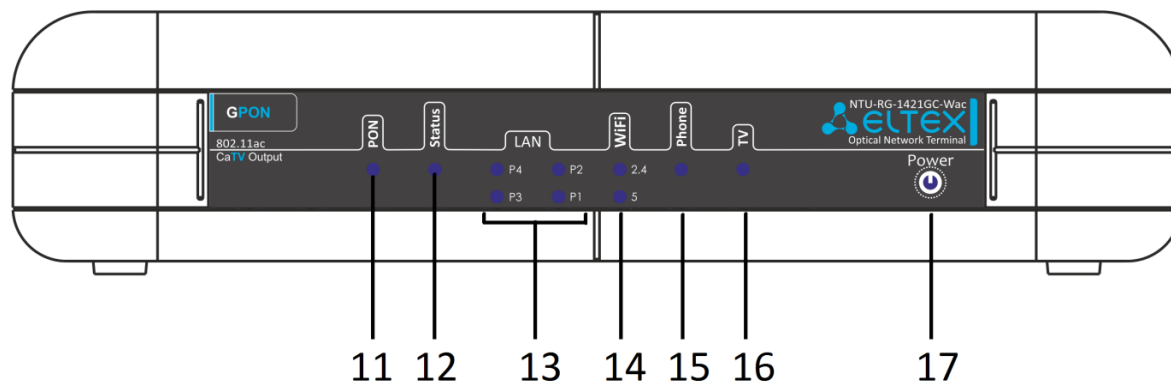


Figure 7 – NTU-RG-1421GC-Wac front panel layout

Table 7 lists LEDs located on the device front panel.

Table 7 – Description of the LEDs located on the front panel

No.	Front panel element	Description
11	<b>PON</b>	power and activity status indicator
12	<b>Status</b>	configuration and hardware status indicator
13	<b>LAN 1..4</b>	Ethernet port activity indicator
14	<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
15	<b>Phone</b>	FXS port activity indicator
16	<b>TV</b>	CaTV activity indicator
17	<b>Power</b>	power indicator


## 2.6 LED Indication






### 2.6.1 NTU-RG-1421G-Wac, NTU-RG-1421G-WZ, NTU-RG-1431G-Wac

LED indicators located on the front panel represent the current state of the device.

Possible states of the LEDs are listed in Table 8.

Table 8 – Light indication of the device

LED indicator	LED state	Device status
 <b>1..4</b>	green	10/100Mbps connection has been established
	orange	1000Mbps connection has been established

	flashes	packet data transmission is in progress
	on	phone is off-hook
	flashes	port is not registered or authorization is not completed on SIP server
	flashes slowly	receiving call signal
 2.4/5	green	Wi-Fi is active
	flashes	Wi-Fi data transfer
	off	Wi-Fi is not active
	off	interface with the Internet identifier is not configured
	green	interface with the Internet identifier is configured and IP address is obtained
	orange	interface with the Internet identifier is configured but IP address is not obtained
	flashes green	device firmware update is in progress
	off	device startup is in progress
	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
	off	device is disconnected from the power source or faulty
	red	device startup failure
	green	device startup completed, the current device configuration differs from the default one
	orange	device startup is completed, the default configuration is set

### 2.6.2 NTU-RG-1421GC-Wac

LED indicators located on the front panel represent the current state of the device.

Possible states of the LEDs are listed in Table 9.

Table 9 – Light indication of the device

LED indicator	LED state	Device state
<b>PON</b>	off	device booting
	green	connection between optical line terminal and the device has been established
	green flashes	authentication failed on the optical line terminal
	red	no signal from optical line terminal
<b>Status</b>	off	static or bridge operation mode has been established for WAN interface (PPP client is not started)
	green	The device has been successfully authorized on the optical line device (PPP session is started on WAN interface).
	orange	The device has not been authorized (PPP session is not started on WAN interface)
<b>LAN P1/P2/P3/P4</b>	green	10/100 Mbps connection has been established
	orange	1000 Mbps connection has been established
	flashes	packet data transmission is in progress
<b>Wi-Fi 2.4/5</b>	green	Wi-Fi is active
	flashes	Wi-Fi data transfer

	off	Wi-Fi is not active
<b>Phone 0</b>	green	phone is off-hook
	flashes	port is not registered or authorization is not completed on SIP server
	flashes slowly	receiving call signal
<b>TV</b>	off	RF port is disabled
	red	TV signal is not available
	orange	signal level does not correspond to the normal (more than +2 dBm)
<b>Power</b>	off	The device is disconnected from the power source or faulty
	green	The current device configuration differs from the default one
	orange	The default configuration is set
	red	device booting

### 2.6.3 Indication of LAN Interfaces

Table 10 lists operation modes shown by LAN ports LEDs located on the rear panel of the device.

Table 10 – Light Indication of LAN Interfaces

Operation Modes	Yellow LED	Green LED
Port is in 1000Base-T mode, no data transfer	solid on	solid on
The port is in the 1000Base-T mode, data transfer	solid on	flashes
Port is in 10/100Base-TX mode, no data transfer	off	solid on
The port is in the 10/100Base-TX mode, data transfer	off	flashes

## 2.7 Reboot/Reset to factory defaults

For device reboot, press the *Reset* button once on the device side panel (“F” button on a rear panel for NTU-RG-1421GC-Wac). In order to reset the device to factory settings, press the *Reset* button (“F”) and hold it for 7-10 seconds until the *POWER* LED glows red. 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.

## 2.8 Delivery Package

NTU-RG standard delivery package includes:

- NTU-RG optical network terminal;
- 220V/12V power adapter;
- operation manual.



### 3 ARCHITECTURE OF DEVICES

#### 3.1 NTU-RG architecture

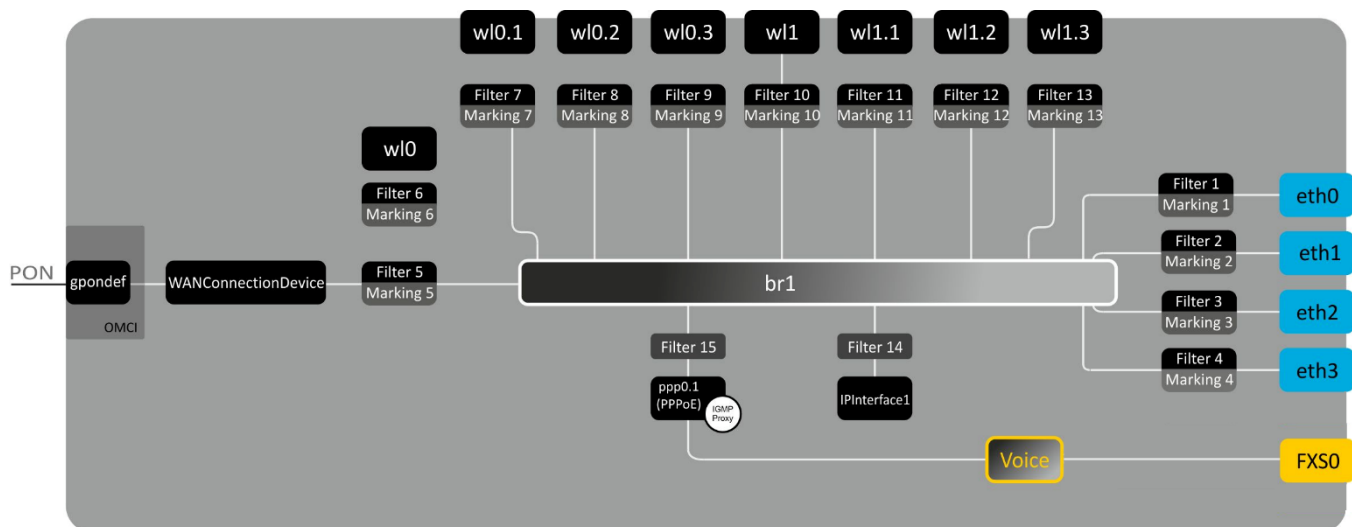


Figure 8 – Logical Architecture of a Device with Factory Settings

#### Main Components of the Device:

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

A device with factory (initial) settings have the following logical blocks (see Figure 8):

- Br1;
- Voice (IP telephony);
- eth0...3;
- FXS0;
- w0, w0.1..w0.3, w1, w1.1..w1.3;
- ppp0.1;
- IPInterface.

The **br1** block here is used to combine LAN ports into a single group.

The **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 the **br1** block.

The **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.).

The **w0, w0.1..w1.3** blocks are the Wi-Fi module connection interfaces. w0 blocks are the interfaces designed for 2.4GHz band operation and w1 blocks are designed for 5GHz band operation.

**Filter** and **Marking** blocks enable inclusion of local interfaces into a single group (to **br1** block). They deal with the traffic transmission rules, **Filter** blocks are responsible for the incoming traffic on the interface, **Marking** blocks—for the outgoing one.

**IPInterface block** is a logical entity that the IP address is provided for the access in LAN and DHCP server distributing addresses to clients.

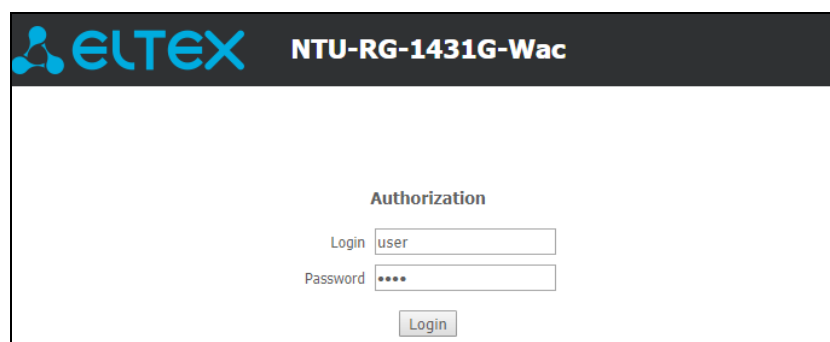
The **ppp0.1** block is WAN interface of the router. In the factory default configuration, this interface is a default interface for such services as the Internet, VoIP, TR-069 device management and IPTV.

A connection to OB device (successful connection to an OLT) additionally creates the **gpondef block** with the help of the OMCI protocol (ONT Management and Control Interface). This block enables connection of the subscriber ONT device to the station one.

#### 4 CONFIGURATION OF NTU-RG-1421G-WAC, NTU-RG-1421G-WZ, NTU-RG-1431G-W AND NTU-RG-1421GC-W VIA WEB INTERFACE. USER ACCESS

In order to configure the device it's necessary to connect to it in web browser (hypertext document viewer), such as Firefox or Google Chrome. To do this, enter the device IP address in the browser address bar (factory default IP: 192.168.1.1, subnet mask: 255.255.255.0).

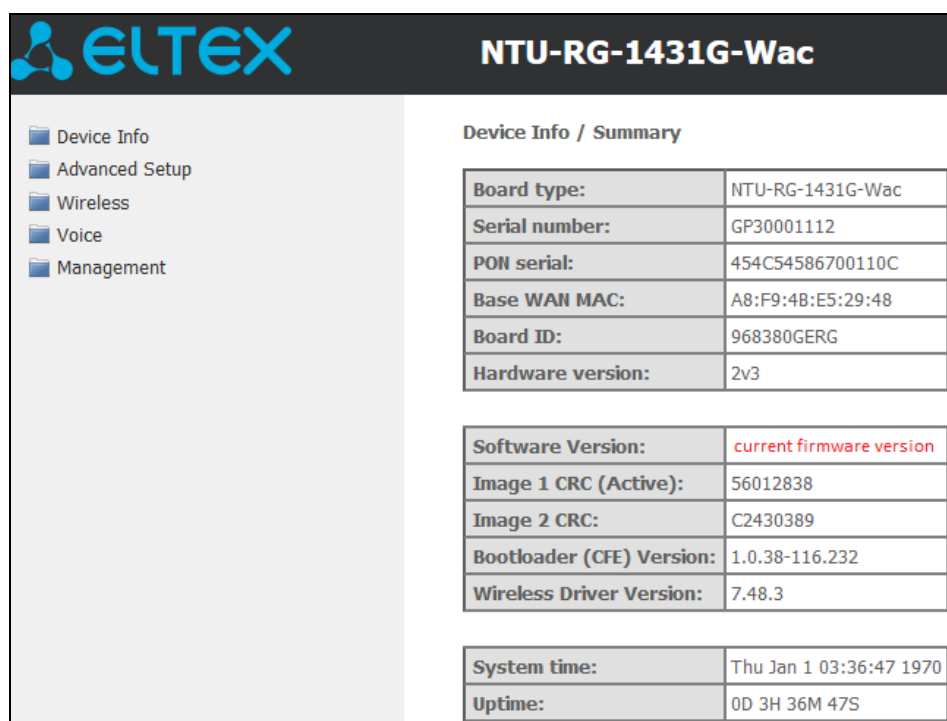
After entering IP address, the device requests username and password.



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

In order to prevent unauthorised access to the device, the password is recommended to be changed (see section 4.5.5).

Given below is a general view of the device configuration window. A navigation tree for object settings is in the left pane, while the settings editor is to the right.



Device Info / Summary	
Board type:	NTU-RG-1431G-Wac
Serial number:	GP30001112
PON serial:	454C54586700110C
Base WAN MAC:	A8:F9:4B:E5:29:48
Board ID:	968380GERG
Hardware version:	2v3
Software Version:	current firmware version
Image 1 CRC (Active):	56012838
Image 2 CRC:	C2430389
Bootloader (CFE) Version:	1.0.38-116.232
Wireless Driver Version:	7.48.3
System time:	Thu Jan 1 03:36:47 1970
Uptime:	0D 3H 36M 47S

## 4.1 The “Device Info” menu

### 4.1.1 The “Summary” submenu

Device Info / Summary	
Board type:	NTU-RG-1431G-Wac
Serial number:	GP30001112
PON serial:	454C54586700110C
Base WAN MAC:	A8:F9:48:E5:29:48
Board ID:	968380GERG
Hardware version:	2v3
Software Version:	current firmware version
Image 1 CRC (Active):	56012838
Image 2 CRC:	C2430389
Bootloader (CFE) Version:	1.0.38-116.232
Wireless Driver Version:	7.48.3
System time:	Thu Jan 1 03:41:58 1970
Uptime:	00 3H 41M 58S

- *Board type*—device model;
- *Serial number*—device serial number;
- *PON serial*—device serial number in PON network;
- *Base WAN MAC*—MAC address of the device WAN;
- *Board ID*;
- *Hardware Version*—hardware version number;
- *Software Version*;
- *Image 1 (Active) CRC*—checksum of the 1st firmware image;
- *Image 2 CRC*—checksum of the 2nd firmware image;
- *Bootloader (CFE) Version*—bootloader version number;
- *Wireless Driver Version*—Wi-Fi adapter version number;
- *System time*—current time of the device;
- *Uptime*—time from the last device restart.

### 4.1.2 The “WAN” submenu. The Status of Services

#### 4.1.2.1 The “General” submenu. General information

This tab displays general information about existing WAN interface configurations.

Device Info / WAN / General													
Interface	Description	Type	VlanMuxId	IPv6	Igmp Pxy	Igmp Src Enbl	MLD Pxy	MLD Src Enbl	NAT	Firewall	Status	IPv4 Address	IPv6 Address

#### 4.1.2.2 The “Detail” submenu. Detailed Information

The tab contains detailed information about existing configurations of the WAN interface.

The following information about services can be displayed:

- *WAN service x* – service name;
- *Interface* – interface name;
- *Type* – interface operation mode;
- *Connection type*;
- *NAT* – NAT status;
- *Firewall* – Firewall status;
- *Status* – connection status;
- *Connection Error* – server error (if the connection is not established);
- *IPv4 Address* – access address;
- *Primary DNS Server*<sup>1</sup>– address of the Primary DNS Server applied for operation;
- *Secondary DNS Server*<sup>1</sup>– address of the Secondary DNS Server applied for operation.

Device Info / WAN / Detail	
WAN service 0:	pppoe_veip0.40
Interface:	ppp0.1
Type:	PPPoE
Connection type:	IP_Routed
NAT:	Enabled
Firewall:	Enabled
Status:	Unconfigured
IPv4 Address:	(null)
Primary DNS Server:	192.168.100.1
Secondary DNS Server:	10.10.0.2

WAN service 1:	ipoe_veip0.50
Interface:	veip0.2
Type:	IPoE
Connection type:	IP_Routed
Status:	Unconfigured
IPv4 Address:	0.0.0.0

WAN service 2:	br_veip0.0
Interface:	veip0.3
Type:	Bridge
Connection type:	IP_Bridged
Status:	Connected
IPv4 Address:	0.0.0.0

#### 4.1.3 The “LAN” submenu. Monitoring of LAN Ports. Monitoring of Wi-Fi Interface Status

Status and parameters of wired and wireless LAN interfaces are available in this menu. Status, connection speed, and mode (duplex/half-duplex) are shown for wired connections.

Device Info / LAN	
Port 1	Up; 1000M full
Port 2	Down
Port 3	Down
Port 4	Down
Wi-Fi 2.4	Up
Wi-Fi 5	Up

#### 4.1.4 The “Statistics” submenu. Traffic flow information for device ports

The menu shows statistics of received and transmitted packets for WAN Service, LAN, and optical interface.

**LAN interface:**

Device Info / Statistics / LAN																
Interface	Received								Transmitted							
	Total				Multicast				Total				Multicast			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts
Port 1	40157	309	0	0	0	16	293	7668	73360	204	0	0	0	0	204	1540
Port 2	4112	49	0	0	0	5	44	1540	860	10	0	0	0	0	10	7520
Port 3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	9192
Port 4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	9192
Wi-Fi	0	0	0	17	0	0	0	0	399461	3743	0	2	0	0	3743	0
Wi-Fi (w11)	0	0	0	11	0	0	0	0	395831	3720	0	2	0	0	3720	0

Reset Statistics

<sup>1</sup> Only for INTERNET and VoIP

## WAN Service:

Device Info / Statistics / WAN Service

Interface	Description	Received								Transmitted							
		Total				Multicast		Unicast	Broadcast	Total				Multicast		Unicast	Broadcast
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts
Reset Statistics																	

## Optical interface:

If a device supports measurement of optical signal parameters<sup>1</sup>, the menu displays an additional table:

Device Info / Statistics / Optical							
Received				Transmitted			
Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
0	0	0	0	0	0	0	0
Reset Statistics							
Link Status	Optical Signal Level	Transmit Optical Level	Temperature	Vcc Voltage	Bias Current	Optical Video Level	
Down	No signal	2.18 dBm	55.1 C	3.32 V	16.04 mA	-1.092	

- *Link status*—optical link status;
- *Optical power level*—level of the received signal (1490nm);
- *Optical power level of transmitter*—level of the transmitted signal (1310nm);
- *Temperature*—temperature of SFF module;
- *Vcc voltage*—supply voltage;
- *Bias current*—bias current;
- *Optical Video Level*—optical CaTV signal level<sup>2</sup>.

In order to clear the statistics and start gathering it from the beginning, click the *Reset Statistic* button.

### 4.1.5 The “Route” submenu. Routing table preview

The menu shows the routing table.

Device Info / Route						
Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br1
Flags: U - up, G - gateway, H - host, R - reinstate, D - dynamic (redirect), M - modified (redirect), ! - reject						

<sup>1</sup> Optional

<sup>2</sup> Only for NTU-RG-1421GC-Wac

- *Destination*—destination IP address;
- *Gateway*—gateway IP address;
- *Subnet Mask*—subnet mask (Genmask);
- *Flag*—routing flag:
  - U—active route;
  - ! —inactive route, packets will be rejected;
  - G—the route uses gateway;
  - H—destination address is a separate host;
  - R—restored route;
  - D—the route was created after receiving a redirected ICMP message;
  - M—the route was changed by a redirected ICMP message;
- *Metrics*—route priority;
- *Service*—a service the route is associated with;
- *Interface*—an interface the route is associated with.

#### 4.1.6 The “ARP” submenu. Display of the ARP Protocol Cache

The ARP efficiency depends a lot on ARP cache presented in every host. The cache contains Internet addresses and corresponding MAC addresses. Every record is stored in cache for 5 minutes since its creation.

Device Info / ARP			
IP address	Flags	HW Address	Device
192.168.1.10	Complete	f8:32:e4:a2:31:34	br1

- *IP address*—client IP address;
- *Flags*—status flags:
  - *Completed*—client is active;
  - *Incomplete*—client does not respond to ARP queries;
- *MAC address*—client MAC address;
- *Device*—client interface.

#### 4.1.7 The “DHCP” submenu. Active DHCP leases

The DHCP table provides a list of active DHCP leases and their duration.

Device Info / DHCP					
Interface Name	Interface Type	Hostname	MAC Address	IP Address	Expires In
eth0.0	Ethernet	comm-240316	f8:32:e4:a2:31:34	192.168.1.10	23 hours, 15 minutes, 33 seconds

- *Interface Name*—interface that the address was obtained from;
- *Interface Type*—type of the interface;
- *Hostname*—network device name;
- *MAC address*—device MAC address;
- *IP address*—device address in local network that was chosen by router from the pool of IP addresses;
- *Expires In*—remaining time of the address lease.

#### 4.1.8 The “Wireless Stations” submenu. Connected wireless devices

The menu shows a list of authenticated wireless devices and their statuses.

Device Info / Wireless Stations

This page shows authenticated wireless stations and their status.

MAC	Associated	Authorized	SSID	Interface
-----	------------	------------	------	-----------

Refresh

The device information is shown in a table with the following parameters:

- *MAC* – device MAC address;
- *Associated* – SSID association status;
- *Authorized* – authorisation status;
- *SSID* – identifier of the network that the client belongs to;
- *Interface* – access interface.

Click the *Refresh* button to refresh the information.

#### 4.1.9 The “Wireless Monitor” submenu. Discovered Wi-Fi networks

This menu contains the list of discovered wireless networks.

Device Info / Wireless Monitor

This page shows known wireless networks.

2.4GHz ▾

SSID	BSSID	Channel	RSSI
5_floor_24_0	A8:F9:4B:B4:97:A0	13	-70 dBm
5_floor_24_1	A8:F9:4B:B4:97:A1	13	-68 dBm
tester3_2.4G	A8:F9:4B:CF:A8:61	13	-78 dBm
tester7_2.4G	A8:F9:4B:CF:9F:B9	13	-72 dBm
tester6	20:10:7A:BC:9F:10	1	-71 dBm
tester4	20:10:7A:A5:E6:5F	1	-76 dBm
ELTX-2.4GHz_WiFi_00A4	E0:D9:E3:6F:00:A6	1	-74 dBm
ELTX-2.4GHz_WiFi_142B	A8:F9:4B:BD:14:2D	1	-67 dBm
152-2	A8:F9:4B:DD:E9:99	2	-75 dBm
ELTEX-64B0	A8:F9:4B:CE:64:B1	4	-83 dBm
153-2	A8:F9:4B:D5:05:69	3	-72 dBm

Refresh

The device information is shown in the table with the following parameters:

- *2.4/5GHz*—frequency bands;
- *SSID*—wireless network ID;
- *BSSID*—MAC address of access point;
- *Channel*—AP operation channel;

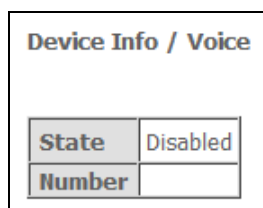


- *RSSI*—strength of AP signal received by ONT.

Click the *Refresh* button to refresh the information.

#### 4.1.10 The “Voice” submenu. Monitoring of telephone ports

The menu shows the status of FXS port and parameters of SIP account.



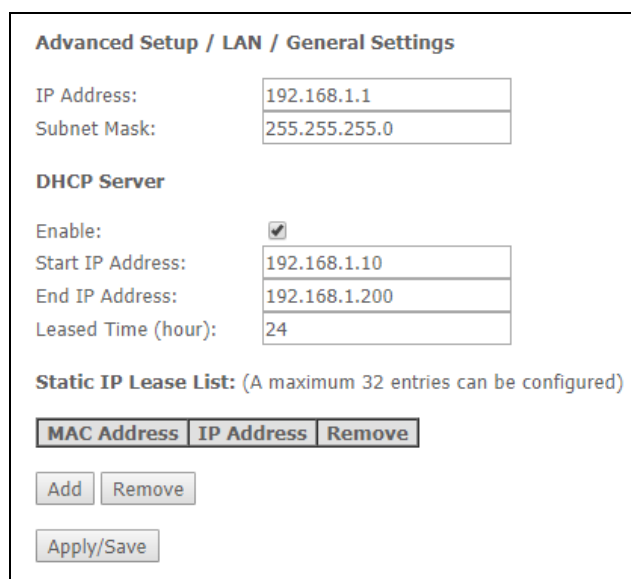
Device Info / Voice	
State	Disabled
Number	

- *Status*—the status of voice daemon;
- *Number*—phone number.

## 4.2 The “Advanced Setup” menu. Advanced configuration

### 4.2.1 The “LAN” submenu. Configuration of Main Parameters

The menu allows you to configure main parameters of the LAN interface.



**Advanced Setup / LAN / General Settings**

IP Address:

Subnet Mask:

**DHCP Server**

Enable: ☒

Start IP Address:

End IP Address:

Leased Time (hour):

**Static IP Lease List:** (A maximum 32 entries can be configured)

MAC Address	IP Address	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>		

- *IP Address*—device address in local network.

#### **DHCP Server**

DHCP server (Dynamic Host Configuration Protocol) enables automatic configuration of local PC to work in network. DHCP server automatically assigns IP addresses to each computer within a network.

- *Enable* — when checked, enable DHCP server (dynamically assign IP addresses from the following range);
- *Start IP Address* — starting address of the range;
- *End IP Address* — ending address of the range;
- *Leased Time (hour)* — address lease time (in hours).

## Static IP Lease List

The *DHCP Static IP Lease* tab is used to establish correspondence between leased IP addresses and devices' MAC addresses (mapping). To add a record into a table, click *Add*. You can establish up to 32 matches.

**DHCP Static IP Lease**

Enter the Mac address and Static IP address then click "Apply/Save".

MAC Address:

IP Address:

- *IP Address*— device IP address;
- *MAC Address*—MAC address.

Click the *Apply/Save* button to accept and save the changes.

### 4.2.2 The “NAT” submenu. NAT Settings

The use of the NAT settings can be efficient when the device operates in the router mode.

#### 4.2.2.1 The “Virtual Servers” submenu. Virtual server settings

*Virtual Server* is a router function designed to provide users with Internet access to servers located in your local network, e. g. to mail servers, WWW, and FTP. A device may have up to 32 records. ‘*NAT loopback*’ function allows you to address local area network devices using their global addresses.

**Advanced Setup / NAT / Virtual Servers**

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	NAT loopback	Remove
<div style="display: flex; justify-content: space-between; align-items: center;"> <span><input type="button" value="Add"/></span> <span><input type="button" value="Remove"/></span> </div>									

In order to add a record to the filtration table, click *Add* and fill in the fields of the displayed window.

**Advanced Setup / NAT / Virtual Servers**

Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified server.  
**NOTE: The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End".**  
**Remaining number of entries that can be configured:32**

Use Interface:

Service Name:

☒ Select a Service:

☐ Custom Service:

Server IP Address:

☒ Enable NAT loopback

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		

- Utilized interface.



**Only interfaces that are fit for operation in router mode with enabled network address translation will be available.**

- *Service name*—service settings:
  - *Select service*—select a preconfigured rule;
  - *Custom Service*—create new rules not listed in the *Select a service* list;
- *Server IP address*—IP address of the server in local network;
- *NAT loopback*—when checked, local area network users may access local servers by their external IP address or domain name.
- *External port (start)*—the first port in the port range accessed from the Internet;
- *External port (end)*—the last port in the port range accessed from the Internet;
- *Protocol*—the network protocol selected;
- *Internal port (start)*—the first internal port in the port range, which will receive redirected traffic from external port of router;
- *Internal port (end)*—the last internal port in the port range, which will receive redirected traffic from external port of router.

Click the *Apply/Save* button to accept and save the changes.

#### 4.2.2.2 The “Port Triggering” submenu. Port Triggering Settings

Router blocks all incoming connection requests by default. The Port Triggering function dynamically opens ports of external interface when a definite event occurs. The ports are then associated with corresponding PC ports in local network.

**Advanced Setup / NAT / Port Triggering**

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

Application Name	Trigger		Open			WAN Interface	Remove
	Protocol	Port Range Start End	Protocol	Port Range Start End			

Add
Remove

In order to add rules to the table, click the *Add* button. Click *Remove* in front of a selected rule to remove it.

### Advanced Setup / NAT / Port Triggering

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application) and click "Apply/Save" to add it.

**Remaining number of entries that can be configured:32**

Use Interface: pppoe\_veip0/ppp1.2

Application Name:

☒ Select an application: Select One

☐ Custom application:

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

Apply/Save

- Utilized interface.



**Only interfaces that are fit for operation in router mode with enabled network address translation will be available.**

- Application name—application settings:
  - Select application—select a preconfigured rule;
  - Custom an application—create new rules not listed in the Select an application list.

As opposed to the Virtual Server function, PC's IP address should not be fixed in LAN.

- Trigger Port Start—the first port in the range of ports performing the trigger function.
- Trigger Port End—the last port in the range of ports performing the trigger function.
- Trigger Protocol—the protocol used for trigger.
- Open Port Start—the first port in the range of ports which will be opened by router.
- Open Port End—the last port in the range of ports which will be opened by router.
- Utilized Protocol—the protocol used for opened ports.

Click the *Apply/Save* button to accept and save the changes.

### 4.2.2.3 The “DMZ Host” submenu. Demilitarized Zone Settings

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

Remove the IP address from the field to disable this option.

**Advanced Setup / NAT / DMZ Host**  
  

The Broadband Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

Enter the computer's IP address and click 'Apply/Save' to activate the DMZ host.

Clear the IP address field and click 'Apply/Save' to deactivate the DMZ host.

DMZ Host IP Address:

Click the *Apply/Save* button to accept and save the changes.

### 4.2.3 The “Security” submenu. Security Settings

This submenu allows you to configure the device security settings.

#### 4.2.3.1 The “IP Filtering” submenu. Address Filtering Settings

The *IP Filtering* function filters router traffic by IP addresses and ports.

#### Filtration Settings for Outgoing Traffic

**Advanced Setup / Security / IP Filtering / Outgoing**  
  

All outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters.

**WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.**

Choose Add or Remove to configure outgoing IP filters.

Filter Name	IP Version	Protocol	SrcMAC	SrcIP/PrefixLength	SrcPort	DstIP/PrefixLength	DstPort	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>								



All outgoing traffic will be transmitted by default. Rules created in the menu enable filtration of undesired traffic.

Click the *Add* button to add a new filtration rule.

**Advanced Setup / Security / IP Filter / Outgoing / Add**

The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter Name:

IP Version:

Protocol:

MAC address:

Source IP address[/prefix length]:

Source Port (port or port:port):

Destination IP address[/prefix length]:

Destination Port (port or port:port):

- *Filter Name*—filter text description;
- *IP protocol version*—IP protocol version;
- *Protocol*—selected protocol (TCP/UDP, TCP, UDP, ICMP);
- *MAC address*—source MAC address;
- *Source IP address[/prefix length]*—source IP address (prefix length can be specified after slash);
- *Source port (port or port:port)*—source port or a range of ports separated by a colon;
- *IP address intended use[/prefix length]*—destination IP address (prefix length may be specified after slash);
- *Destination port (port or port:port)*—destination port or a range of ports separated by a colon.

Click the *Apply/Save* to accept and save the settings.

### **Filtering Settings for Incoming Traffic**

**Advanced Setup / Security / IP Filtering / Incoming**

When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is BLOCKED. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure incoming IP filters.

Filter Name	Interfaces	IP Version	Protocol	SrcMAC	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>									



**When a firewall is turned on in a WAN or LAN interface, all incoming traffic which does not satisfy the set rules will be blocked.**

Click the *Add* button to add a new filtration rule.

**Advanced Setup / Security / IP Filter / Incoming / Add**

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter Name:

IP Version:

Protocol:

Source MAC address:

Source IP address[/prefix length]:

Source Port (port or port:port):

Destination IP address[/prefix length]:

Destination Port (port or port:port):

**WAN Interfaces (Configured in Routing mode and with firewall enabled) and LAN Interfaces**  
Select one or more WAN/LAN interfaces displayed below to apply this rule.

☒ Select All ☒ br1/br1

- *Filter Name*—filter text description;
- *IP Version*—IP protocol version;
- *Protocol*—the network protocol selected;
- *Source MAC address*—source MAC address;
- *Source IP address[/prefix length]*—source IP address (prefix length can be specified after slash);
- *Source Port (port or port:port)*—source port or port range can be specified after double point;
- *Destination IP address [/prefix length]*—destination IP address (prefix length may be specified after slash);
- *Destination Port (port or port:port)*—destination port or port range can be specified after double point.

#### WAN (configured in the router mode and having firewall enabled) and LAN Interfaces

- *Select All*—when checked, choose all available interfaces.

Or choose an interface from the list by selecting the checkbox next to it.

Click the *Apply/Save* to accept and save the settings.

#### 4.2.3.2 The “MAC Filtering Setup” submenu. Filtering Settings for MAC Addresses

MAC filtration allows traffic to be transferred or blocked depending on source and destination MAC addresses.

**Advanced Setup / Security / MAC Filtering Setup**

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

MAC Filtering Policy For Each Interface:  
**WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.**

Choose Add or Remove to configure MAC filtering rules.

Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
-----------	----------	-----------------	------------	-----------------	--------



**MAC filtration can be applied only to interfaces in the bridge mode.**

In order to change the global policy, set a flag in front of a corresponding interface and click the *Change Policy* button. Two options are available: FORWARDED and BLOCKED.

The created rules will block traffic with specified source/destination MAC addresses in the FORWARDED mode and allow it to pass in the BLOCKED mode.

### Add MAC Filter

Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "Apply/Save" to save and activate the filter.

Protocol Type: PPPoE

Destination MAC Address: 12:AF:56:78:1D:1C

Source MAC Address:

Frame Direction: LAN<=>WAN

WAN Interfaces (Configured in Bridge mode only)

br\_veip0/veip0.3

Apply/Save

- *Protocol type*—the selected protocol (PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP);
- *Destination MAC address*—destination MAC address;
- *Source MAC address*—source MAC address;
- *Frame direction*—transfer direction (LAN<=>WAN, LAN=>WAN, WAN=>LAN);
- *WAN interface (configured in Bridge mode only)*—allows a WAN interface to be selected from a drop-down list (only the interfaces in the bridge mode are available).

Click the *Apply/Save* to accept and save the settings.


#### 4.2.4 The “Parental Control” submenu: restriction settings

##### 4.2.4.1 The “Time Restriction” submenu. Session Time Restriction Settings

The menu allows schedule configuration (days and hours) for computers use. The schedule will be used to block Internet access for a definite computer in local network at a definite time.

### Advanced Setup / Parental Control / Time Restriction

A maximum 16 entries can be configured.

Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove
Mom	f8:32:e4:a2:31:34	x	x	x	x	x			16:30	23:59	

Add Remove

Click *Add* button to create a new schedule. You can add up to 16 records.



**Advanced Setup / Parental Control / Time Restriction / Add**

This page adds time of day restriction to a special LAN device connected to the Router. The 'Browser's MAC Address' automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to command window and type "ipconfig /all".

User Name

☒ Browser's MAC Address

☐ Other MAC Address

(xx:xx:xx:xx:xx:xx)

Days of the week	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Click to select	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

- *Username*—user name;
- *Browser's MAC Address*—automatically identified MAC address of the computer for which the schedule is created;
- *Another MAC Addresses (xx:xx:xx:xx:xx:xx)*—manually set MAC address of the computer for which the schedule is created;
- *Days of the week*—days when Internet access is blocked;
- *Start Blocking Time (hh:mm)*—the time when blocking starts (hh:mm);
- *End Blocking Time (hh:mm)*—the time when blocking ends (hh:mm).



**The restrictions will apply if the correct system time is set for the device.**

Click the *Apply/Save* button to add settings to the table.

#### 4.2.4.2 The "Url Filter" submenu. Internet Access Restriction Settings

*Url Filter*—is a function of comprehensive analysis and control of access to certain Internet resources. This parameter defines a list of prohibited/allowed URLs.

**Advanced Setup / Parental Control / URL Filter**

Please select the list type first then configure the list entries. Maximum 100 entries can be configured.

URL List Type: ☒ Exclude ☐ Include

Address	Port	Remove
vk.com	80	<input type="checkbox"/>

- *URL List Type*—type of the list:
  - *Exclude*—prohibited URLs;
  - *Include*—allowed URLs.

In order to add a new URL to a list, select the checkbox next to the corresponding list (*URL List Type*) and click the *Add* button.

**Advanced Setup / Parental Control / URL Filter / Add**  
Enter the URL address and port number then click "Apply/Save" to add the entry to the URL filter.  
  
URL Address:   
Port Number:  (Default 80 will be applied if leave blank.)

- *URL*—URL address;
- *Port Number*—port number (if the field is empty, port 80 will be used).

Click the *Apply/Save* button to add settings to the table.

#### 4.2.5 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. There are two options 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 often used in local networks where clients get IP addresses by DHCP and then register their names in a local DNS server.

**Advanced Setup / Dynamic DNS**  
  
The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your Broadband Router to be more easily accessed from various locations on the Internet.  
  
Choose Add or Remove to configure Dynamic DNS.  
  

Hostname	Username	Service	Interface	Remove
<div> <input type="button" value="Add"/> <input type="button" value="Remove"/> </div>				

To add a record, click *Add* button; to remove a record, click *Remove* button for the selected record.

**Advanced Setup / Dynamic DNS / Add**  
  
This page allows you to add a Dynamic DNS address from any of listed DDNS providers.  
  
D-DNS provider:   
  
Hostname:   
Interface:   
  
**DynDNS Settings**  
Username:   
Password:   
  
DynDNS Type:   
  
Wildcard: ☐

- *D-DNS provider*—type of D-DNS service (provider): *DynDNS.org*, *TZO.com*, *ZoneEdit.com*, *freedns.afraid.org*, *easyDNS.com*, *3322.org*, *DynSIP.org*, *No-IP.com*, *dnsomatic.com*, *sitelutions.com*;
- *Custom*—another provider chosen by user. In this case user will need to specify the provider's name and address:

**Advanced Setup / Dynamic DNS / Add**

This page allows you to add a Dynamic DNS address from any of listed DDNS providers.

D-DNS provider Custom

Hostname

Interface pppoe\_veip0/ppp0.1

**Custom D-DNS provider**

Username

Password

DDNS Provider Server Name

DDNS Provider URL

- *User name*—user name for the DDNS account;
  - *Password*—password for the DDNS account;
  - *DDNS Provider Server Name*—name of the DDNS provider;
  - *DDNS Provider address*—address of the DDNS provider.
- *Hostname*—host name registered at the DDNS provider;
  - *Interface*—access interface.

**The following fields will be available depending on the selected provider:**

**Advanced Setup / Dynamic DNS / Add**

This page allows you to add a Dynamic DNS address from any of listed DDNS providers.

D-DNS provider DynDNS.org

Hostname

Interface pppoe\_veip0/ppp0.1

**DynDNS Settings**

Username

Password

DynDNS Type Dynamic

Wildcard ☐

**Advanced Setup / Dynamic DNS / Add**

This page allows you to add a Dynamic DNS address from any of listed DDNS providers.

D-DNS provider
freedns.afraid.org ▼

Hostname

Interface
pppoe\_veip0/ppp0.1 ▼

**freedns.afraid.org Settings**

Username

Password

**Advanced Setup / Dynamic DNS / Add**

This page allows you to add a Dynamic DNS address from any of listed DDNS providers.

D-DNS provider
TZO.com ▼

Hostname

Interface
pppoe\_veip0/ppp0.1 ▼

**TZO Settings**

Email

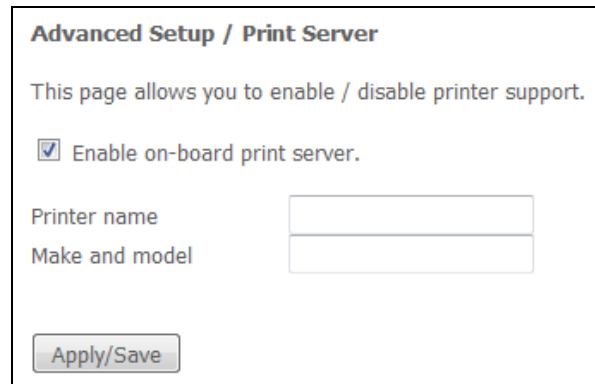
Key

- *User name*—user name for the DDNS account;
- *Password*—password for the DDNS account;
- *DynDNS Type*—type of the service you registered at your provider:
  - *Dynamic*—Dynamic DNS service is registered;
  - *Static*—Static DNS service is registered;
  - *Custom*—Custom DNS service is registered.
- *Wildcard*—when checked, a special DNS record is used which is referred to all subdomains and will correspond if a query sent to a subdomain, which does not exist. It is indicated as \* in the subdomain field, for example \*.domain.tld.;
- *Email*—email address for authentication;
- *Key*—key for the DDNS account.

Click the *Apply/Save* button to accept and save the changes.

#### 4.2.6 The “Print Server” submenu. Print Server Configuration

Print server is a software or hardware solution that allows users of wired or wireless networks to share a printer at home or at the office. This printer is completely independent from network computers and significantly reduces the burden on user's working environment. Besides that, print server establish continuous communication to printers, AIO, scanners and other office machines located on LAN.



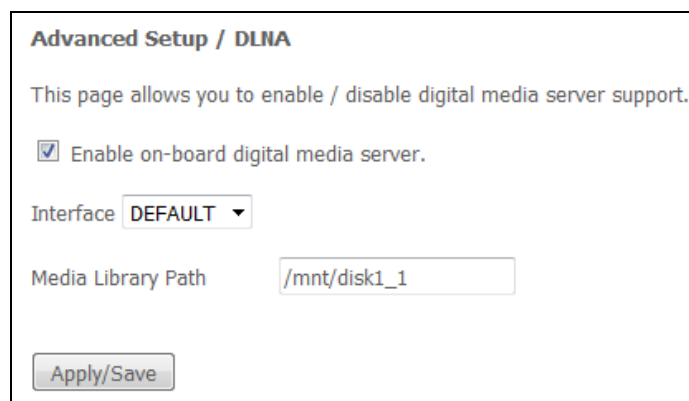
- *Enable on-board print server*—when checked, print server is enabled, otherwise it is disabled;
- *Printer name*—printer name;
- *Manufacturer and model*—printer manufacturer and model.

Click the *Apply/Save* to accept and save the settings.

#### 4.2.7 The “DLNA” submenu. DLNA server configuration

DLNA (Digital Living Network Alliance) is a set of standards that allow compatible devices to receive and transmit various media content via home network (pictures, music, videos), and view it in real time. That means, it is a technology that unites home computers, mobile phones, laptops and other home appliances into a single digital network. Devices supporting DLNA specification may be configured and combined into network automatically on user's request.

Transmission medium for media content is a home network (IP network). DLNA-compatible devices may connect to a home network using wired (Ethernet) or wireless (Wi-Fi) connections.

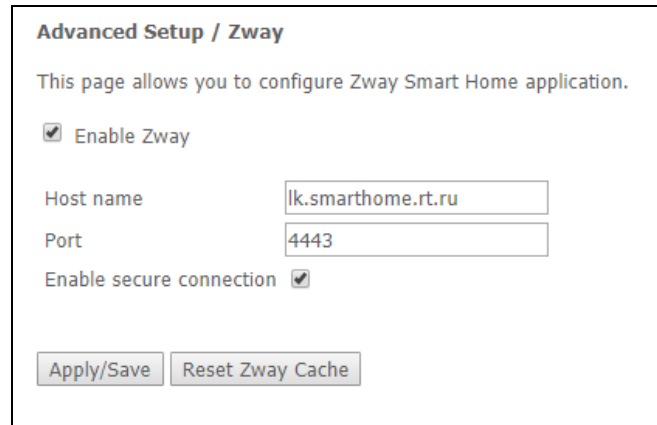


- *Enable on-board digital media server*—when checked, media server is enabled, otherwise it is disabled;
- *Interface*—name of the interface for server connection;
- *Media Library Path*—media file directory.

Click the *Apply/Save* to accept and save the settings.

#### 4.2.8 The “Z-Wave” menu

Use this menu to configure “Smart Home” parameters.



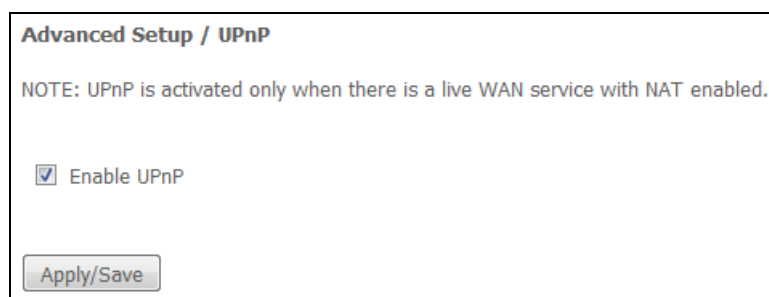
- *Enable Zway*—enable/disable “Smart Home” controller;
- *Host name*—specify IP address of “Smart Home” remote platform;
- *Port*—specify the platform port to which “Smart Home” controller is connected;
- *Enable secure connection*—set the flag if secure channel is used to share data with the platform;
- *Reset Zway cache*—when clicking the button, the controller is turned off; all information about the connection to the platform, linked sensors and scripts is deleted from it.

Click the *Apply/Save* to accept and save the settings.

#### 4.2.9 The “UPnP” submenu. Autoconfiguration of network devices

Use the menu to configure Universal Plug and Play (UPnP™) function.

UPnP ensures compatibility with network equipment, software and peripheral devices.



**Configure NAT on an active WAN interface, to use UPnP.**

Set the *Enable UPnP* flag to enable UPnP.

Click *Apply/Save* button to accept and save the settings.

## 4.3 The “Wireless” menu. Wireless network configuration

This section contains individual settings for each of the operating bands—2.4GHz and 5GHz.

### 4.3.1 The “Basic” submenu. General settings

This menu is intended for general setup of the LAN wireless interface and allows user to specify up to three wireless access points.

**Wireless / Basic**

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements. Click "Apply/Save" to configure the basic wireless options.

☒ Enable Wireless

**Wireless - Access Point:**

☒ Enable Access Point

☐ Hide Access Point

☐ Clients Isolation

☐ Disable WMM Advertise

☒ Enable Wireless Multicast Forwarding (WMF)

SSID:

BSSID:

Country:

Country RegRev:

Max Clients:

**Wireless - Guest/Virtual Access Points:**

Enabled	SSID	Hidden	Isolate Clients	Disable WMM Advertise	Enable WMF	Max Clients	BSSID
<input checked="" type="checkbox"/>	wl0_Guest1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	16	N/A
<input type="checkbox"/>	wl0_Guest2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	16	N/A
<input type="checkbox"/>	wl0_Guest3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	16	N/A

- *Enable Wireless* — enables Wi-Fi on the device.
- *Enable Access Point*—enable Hotspot2.0 support on the device;
- *Hide Access Point*—access point hidden operation mode (in this mode, wireless network SSID won't be broadcast by the router);
- *Clients Isolation*—when checked, wireless clients will not be able to interact with each other;
- *Disable WMM Advertise*—disable WMM (Wi-Fi Multimedia—a QoS for wireless networks);
- *Enable Wireless Multicast Forwarding (WMF)*—enable WMF;
- *SSID (Service Set Identifier)*—assign a wireless network name (case sensitive).



**Default device SSID is ELTX-2.4GHz\_WiFi\_\_aaaa/ELTX-5GHz\_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 (2.4/5GHz).**

- *BSSID*—MAC address of the access point;
- *Country*—specifies location (country);
- *Country RegRev*—specifies region ID (0-34 for Russia);
- *Max Clients*—the maximum possible number of simultaneously supported wireless connections.

Click the *Apply/Save* to accept the changes.

### 4.3.2 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.

**Wireless / Security**  
  

This page allows you to configure security features of the wireless LAN interface.  
You may setup configuration manually  
OR  
through Wi-Fi Protected Setup (WPS)  
Note: Only Push Button Connect (PBC) is used. If Hide Access Point enabled or Mac filter list is empty with "allow" chosen, WPS2 will be disabled

**WPS Setup**  
  

Enable WPS

Enabled

Set WPS AP Mode

Configured

  
  
**Manual Setup AP**  
  

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply/Save" when done.

Select SSID:

ELTX-2.4GHz\_WiFi\_2948

Network Authentication:

WPA2 -PSK

Protected Management Frames:

Disabled

WPA/WAPI passphrase:

••••••••

[Click here to display](#)

WPA Group Rekey Interval:

0

WPA/WAPI Encryption:

AES

WEP Encryption:

Disabled

Apply/Save

*WPS (Wi-Fi Protected Setup)*—a standard developed by Wi-Fi Alliance to simplify setup of wireless networks. The technology allows quick, secure, and simple setup of a wireless network without having in-depth knowledge of Wi-Fi technology and encryption protocols. WPS automatically sets the network name and configures data encryption to protect the network from unauthorised access. These operations should be manually done without WPS.

In order to establish a connection, user simply needs to press the WPS button located on the side panel of the device or use Web configuration to enter PIN code.

#### WPS Setup

- *Enable WPS* – to enable WPS access, select *Enable* from the drop-down list, if WI-FI network adapter of your device supports this configuration mode;



- *Set WPS AP mode*—sets WPS mode of the access point.

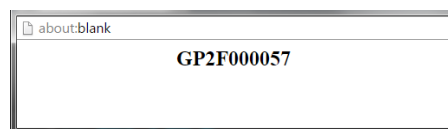


### Shortcomings of WPS

Wi-Fi routers supporting the WPS technology have a security vulnerability. This vulnerability allows attackers to retrieve passwords for WPA and WPA2 encryption protocols. The technology is vulnerable as it allows to brute-force the 8-digit network key (PIN).

#### Access point manual configuration:

- *Select SSID*—selects a name of a wireless network from the list;
- *Network Authentication*—selects a network authentication mode from the drop-down list:
  - *Open*—wireless network security features are disabled (in this mode, only WEP key can be used);
  - *Shared*—this mode enables user authentication by their SSID or WEP key;
  - *802.1x*—enables 802.1x standard (enables user authentication with a RADIUS server, WEP key is used for data encryption);
    - *RADIUS Server IP Address*;
    - *RADIUS Port*—port number of the RADIUS server The default port is 1812;
    - *RADIUS key*—a secret key for access to the RADIUS server.
  - *WPA2*—enables WPA2 (this mode uses WPA2 protocol, requires the utilization of a RADIUS authentication server);
    - WPA Group Rekey Interval – the period of time (in seconds) between automatic changes of WPA encryption keys used to strengthen wireless network security If you don't need to change encryption keys, enter null value into the field;
    - *RADIUS Port*—port number of the RADIUS server The default port is 1812;
    - *RADIUS key*—a secret key for access to the RADIUS server;
    - *WPA/WAPI Encryption*—selects a WPA/WAPI data encryption method: TKIP+AES, AES:
      - TKIP—the encryption protocol used for WPA It implements a more efficient mechanism of key change management in comparison with WEP;
      - AES—128-bit block encryption algorithm with 128/192/256-bit key, generally used for WPA2).
  - *WPA2-PSK*—enable WPA2-PSK (this mode uses WPA2-PSK protocol, doesn't require the utilization of a RADIUS authentication server);
    - *WPA/WAPI Password*—a secret phrase. Sets a password; a string of 8-63 ASCII characters. To view a secret phrase, click '*Click here to display*' link, and password will be shown in a pop-up window.



**Default network key corresponds to device serial number. Serial number is printed on a sticker, which is located on device housing.**

**When changing a password, you have to specify a 10-character combination. Password should contain numbers and Latin characters in upper and lower case.**

- *WPA Group Rekey Interval*—the period of time (in seconds) between automatic changes of WPA encryption keys used to strengthen wireless network security If you don't need to change encryption keys, enter null value into the field.
- *WPA/WAPI Encryption*—selects a WPA/WAPI data encryption method: TKIP+AES, AES:

- TKIP—the encryption protocol used for WPA. It implements a more efficient mechanism of key change management in comparison with WEP;
- AES—128-bit block encryption algorithm with 128/192/256-bit key, generally used for WPA2).
- *Mixed WPA2/WPA*—includes a combination of WPA2/WPA (this encryption mode uses WPA2 and WPA protocols, requires the utilization of a RADIUS authentication server);
  - *WPA2 Preauthentication*—pre-authentication of the wireless client in other wireless access points in the specified range. During authentication, communication is provided by the current wireless access point;
  - *Network Re-auth Interval*—time interval for repeated authentication. The parameter defines how often the access points sends an authentication message to clients and requires a reply with valid authentication data;
  - *WPA Group Rekey Interval*—the period of time (in seconds) between automatic changes of WPA encryption keys used to strengthen wireless network security. If you don't need to change encryption keys, enter null value into the field.
  - *RADIUS Server IP Address*—IP address of the RADIUS server;
  - *RADIUS Port*—port number of the RADIUS server. The default port is 1812;
  - *RADIUS key*—a secret key for access to the RADIUS server;
  - *WPA/WAPI Encryption*—selects a WPA/WAPI data encryption method: TKIP+AES, AES:
    - TKIP—the encryption protocol used for WPA. It implements a more efficient mechanism of key change management in comparison with WEP;
    - AES—128-bit block encryption algorithm with 128/192/256-bit key, generally used for WPA2);
- *Mixed WPA2/WPA-PSK*—includes a combination of WPA2/WPA-PSK (this encryption mode uses WPA2-PSK and WPA-PSK protocols, requires the utilization of a RADIUS authentication server)
  - *WPA/WAPI Password*—a secret phrase. Sets a password; a string of 8-63 ASCII characters. To view a secret phrase, click [Click here to display](#) link, and password will be shown in a pop-up window.



**Default network key corresponds to device serial number. Serial number is printed on a sticker, which is located on device housing. When changing a password, you have to specify a 10-character combination. Password should contain numbers and Latin characters in upper and lower case.**

- *WPA Group Rekey Interval*—the period of time (in seconds) between automatic changes of WPA encryption keys used to strengthen wireless network security. If you don't need to change encryption keys, enter null value into the field.
- *WPA/WAPI Encryption*—selects a WPA/WAPI data encryption method: TKIP+AES, AES:
  - TKIP—the encryption protocol used for WPA. It implements a more efficient mechanism of key change management in comparison with WEP
  - AES—128-bit block encryption algorithm with 128/192/256-bit key, generally used for WPA2)



**Make sure that the wireless adapter of a computer supports selected encryption type. The most secure protection of a wireless channel is reached by joint operation of access point and**

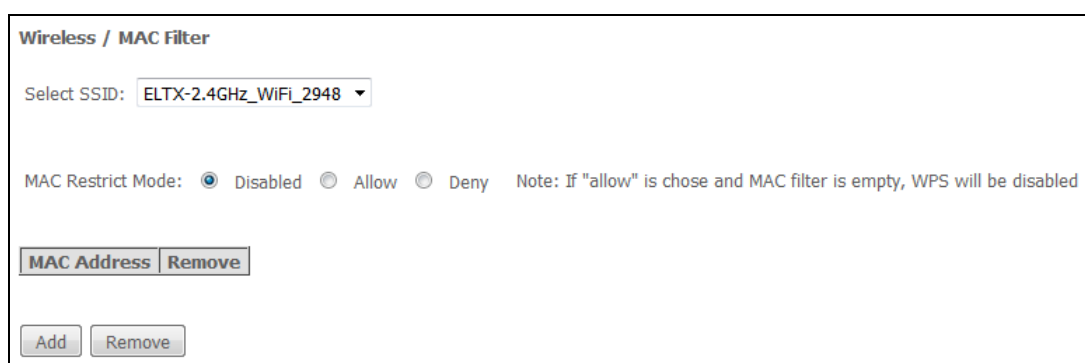
## RAIUS server (for authentication of wireless clients).

- *WEP Encryption*—select *Enable* in the drop down list to enable WEP encryption;
  - *Encryption*—64- or 128-bit key encryption;
  - *Current Network Key*—the key that will be used for connection;
  - *Network Key 1..4*—allows specification of 4 different keys, which comprise of 10 hex characters of 5 ASCII characters<sup>1</sup> for 64-bit encryption. Other options are 26 hex characters or 13 ASCII characters for 128-bit encryption.

Click the *Apply/Save* to accept the changes.

### 4.3.3 The “MAC Filtering” submenu. Filtering Settings of MAC Addresses

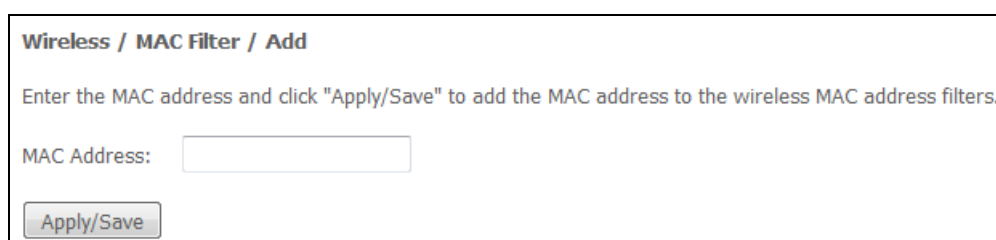
The menu allows filters configuration for MAC addresses.



The screenshot shows a web interface titled "Wireless / MAC Filter". It contains a dropdown menu for "Select SSID" with the value "ELTX-2.4GHz\_WiFi\_2948". Below this is a "MAC Restrict Mode" section with three radio buttons: "Disabled" (selected), "Allow", and "Deny". A note states: "Note: If 'allow' is chose and MAC filter is empty, WPS will be disabled". At the bottom, there are two buttons: "Add" and "Remove".

- *Select SSID*—the identifier of the wireless network, for which a rule will be created;
- *MAC Restrict Mode*—filtration mode for MAC addresses;
  - *Disabled*—filter will be disabled;
  - *Allow*—filters allowed addresses;
  - *Deny*—filters denied addresses.

In order to add a MAC address to the filtration table, click *Add* and enter the address into the *MAC address* field of the displayed menu.



The screenshot shows a web interface titled "Wireless / MAC Filter / Add". It contains a text input field for "MAC Address:". Below the field is an "Apply/Save" button.

Click the *Apply/Save* to accept the changes.

<sup>1</sup> ASCII—is a set of 128 characters for machine representation of capital and lower case Latin characters, digits, punctuation marks, and special symbols.

#### 4.3.4 The “Wireless Bridge” submenu. Wireless Connection Settings in Bridge Mode

Use this menu to specify access point operation mode: either access point or wireless bridge.

When the bridge mode is used, MAC addresses of remote bridges should be specified. This mode is used to establish a wireless connection between two individual networks.

**Wireless / Bridge**

This page allows you to configure wireless bridge features of the wireless LAN interface. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access. Click "Refresh" to update the remote bridges. Wait for few seconds to update. Click "Apply/Save" to configure the wireless bridge options.

Bridge Restrict:

Remote Bridges MAC Address:

Remote Bridges MAC Address:

In *Wireless/Bridge* mode, you can configure the following settings:

- *Bridge Restrict*—select bridge operation mode:
  - *Enabled*—enable filtering for MAC addresses (only specified addresses are allowed);
  - *Enabled (scan)*—search for remote bridges;
  - *Disabled*—no restrictions for MAC addresses;
- *Remote Bridges MAC Address*—addresses of remote bridges.



**Router does not support the Wi-Fi Multimedia (WMM) function in the bridge mode.**

Click *Refresh* to refresh information on available remote bridges.

Click the *Apply/Save* button to accept and save the changes.

### 4.3.5 The “Advanced” submenu

Use this menu to configure advanced settings of the wireless network.

**Wireless / Advanced**

This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used. Click "Apply/Save" to configure the advanced wireless options.

Band:	2.4GHz																											
Channel:	Auto	Current: 1 (interference: acceptable)																										
Auto Channel Timer(min)	15																											
Standard:	n																											
Auto Channel Set:	Full																											
Allowed Channels:	<table> <tr> <td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td> </tr> <tr> <td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td> </tr> </table>	1	2	3	4	5	6	7	8	9	10	11	12	13	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
1	2	3	4	5	6	7	8	9	10	11	12	13																
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>																
802.11n/EWC:	Auto																											
Bandwidth:	Auto	Current: 20MHz																										
Control Sideband:	Lower	Current: N/A																										
802.11n Rate:	Auto																											
802.11n Protection:	Auto																											
RIFS Advertisement:	Auto																											
RX Chain Power Save:	Disable	Power Save status: Full Power																										
RX Chain Power Save Quiet Time:	10																											
RX Chain Power Save PPS:	10																											
54g™ Rate:	1 Mbps																											
Multicast Rate:	Auto																											
Basic Rate:	Default																											
Fragmentation Threshold:	2346																											
RTS Threshold:	2347																											
DTIM Interval:	1																											
Beacon Interval:	100																											
Global Max Clients:	16																											
XPress™ Technology:	Disable																											
Transmit Power:	100%																											
WMM(Wi-Fi Multimedia):	Enable																											
WMM No Acknowledgement:	Disable																											
WMM APSD:	Enable																											
Beamforming Transmission (BFR):	Enable																											
Beamforming Reception (BFE):	Enable																											

Apply/Save
Default

- **Band**—set the frequency band (2.4/5GHz);
- **Channel**—active channel of the router. Changing operating channel can eliminate interference or problems that occur in wireless network operation. It is recommended to set this value to ‘Auto’ to avoid the interference caused by the neighbouring networks.
- **Auto Channel Timer (min)**—time period (minutes) after which the router will search for an optimal wireless channel. This parameter is available when Auto channel is selected (enter 0 to disable).
- **Standard**—set 802.11 standard.
- **Auto Channel Set**—defines automatic channel selection mode:

- *Full*—automatic selection mechanism scans and selects a channel from the list of available channels.
- *Legacy*—automatic selection mechanism scans and selects a channel from the list of channels supported by legacy devices (only for 2.4GHz band).
- *Custom*—automatic selection mechanism scans and selects a channel from the list of channels defined by the user in *Allowed Channel* settings.
- *802.11n/EWC*—compatibility mode for 802.11n Draft2.0 and EWC (Enhanced Wireless Consortium) equipment.
- *Bandwidth*—define the channel width to 20MHz or 40MHz. In 40MHz mode, two adjacent 20MHz bands are used to increase the channel bandwidth.
- *Control Sideband*—select the second channel (Lower or Upper) in 40MHz mode.
- *802.11n Rate*—define connection rate.
- *802.11n Protection*—when enabled, security will be enhanced at the cost of the bandwidth.
- *RIFS Advertisement*—Reduced Interframe Space, reduces interval between data units (PDUs), increases Wi-Fi efficiency.
- *OBSS Co-Existence*—tolerance setting for the chosen mode (20MHz or 40MHz). When set to *Enabled*, the optimal device operation mode will be selected with regard to the *Bandwidth* parameter, otherwise operation mode will depend only on *Bandwidth* parameter value.
- *RX Chain Power Save Quiet Time*—time period during which the traffic must be below the PPS value before the power saving feature will be activated.
- *RX Chain Power Save PPS*—the upper limit of PPS (packet per second). If the packets intensity of the WLAN interface does not exceed this value during the time specified in *RX Chain Power Save Quiet Time*, the power saving mode is turned on.
- *54g™ Rate*—set the transfer rate in compatibility mode for 54g™ devices.
- *Multicast Rate*—set the transfer rate for multicast traffic.
- *Basic Rate*—basic transfer rate.
- *Fragmentation Threshold*—set the fragmentation threshold in bytes. If the packet size exceeds the specified value, the packet will be fragmented into parts of a suitable size.
- *RTS Threshold*—if the packet size is smaller than RTS threshold value, RTS/CTS mechanism (with request to send/clear to send packets) won't be used.
- *DTIM Interval*—time period, upon the expiration of which, broadcast and multicast packets placed in the buffer will be delivered to wireless clients.
- *Beacon Interval*—time period used for transmission of informational packets, that indicate the activity of the access point, to the wireless network.
- *Max Clients*—the maximum number of wireless clients.
- *XPress™ Technology*—enables bandwidth boost up to 27% in 802.11g networks. In mixed 802.11g and 802.11b networks, XPress™ Technology can boost the bandwidth up to 75%.
- *Transmitter Power*—define the access point signal power.
- *WMM (Wi-Fi Multimedia)*—set Wi-Fi Multimedia (WMM) mode. This mode enables fast and high quality transmission of audio and video content simultaneously with data transmission.
- *WMM No Acknowledgement*—when this mode is used, the receiving side won't acknowledge received packets. In a low interference environment, it allows to increase the efficiency of transmission; in a high interference environment, efficiency of transmission will decrease.
- *WMM APSD*—enables automatic switching to the power saving mode.
- *Beamforming Transmission (BFR)*—beamforming feature allows to mitigate the wireless signal interference and enhance the quality of Wi-Fi connection.
- *Beamforming Reception (BFE)*—beamforming feature that allows to enhance the quality of Wi-Fi connection.

Click the *Apply/Save* button to accept and save the changes.

### 4.3.6 The “Connection wizard” submenu

Use this menu to configure wireless LAN interface.

You can enable or disable the wireless LAN interface, configure the wireless network name (SSID) and set a password (line of 8-63 ASCII characters).

**Connection wizard**

☐

Enable Wireless 2.4GHz:

Wireless network name (SSID):

Wireless network password:

ELTX-2.4GHz\_WiFi\_19E0

GP37000025

☐

Enable Wireless 5GHz:

Wireless network name (SSID):

Wireless network password:

ELTX-5GHz\_WiFi\_19E0

GP37000025

Apply/Save

Click the Apply/Save button to accept and save the changes.

## 4.4 The “Storage Service” menu. File storage service

### 4.4.1 The “Storage Device Info” submenu. Information about connected USB devices

This menu shows a list of connected storage devices. The following information is provided:

**Storage Service / Storage Device Info**

The Storage service allows you to use Storage devices with modem to be more easily accessed

VolumeName	FileSystem	Total Space	Used Space	Action
------------	------------	-------------	------------	--------

- *Volume name*– device name;
- *File System* – type of file system;
- *Unmount* – click this button to safely remove the device.

### 4.4.2 The “User Accounts” submenu. Configuration of Samba users

Use the menu to configure Samba user accounts.

**Storage Service / User Accounts**

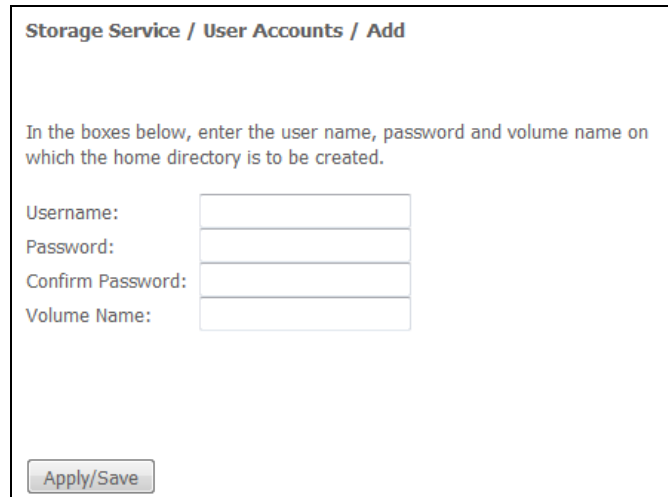
Choose Add, or Remove to configure User Accounts.

UserName	HomeDir	Remove
----------	---------	--------

Add

Remove

To add record, click *Add* button. In order to remove a record, set flag in the *Remove* column in front of the corresponding record and click the *Remove* button.



**Storage Service / User Accounts / Add**

In the boxes below, enter the user name, password and volume name on which the home directory is to be created.

Username:

Password:

Confirm Password:

Volume Name:

- *User name* – login used to access the network resource;
- *Password* – password used to access the network resource;
- *Confirm password* – password confirmation;
- *Volume name* – path to network resource (the name of the connected storage device is shown on the *Storage Device Info* page).

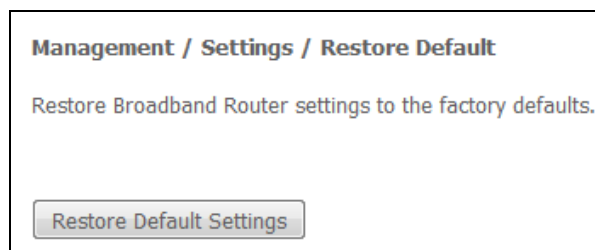
Click the *Apply/Save* to accept and save the settings

## 4.5 The “Management” menu. Device Management

### 4.5.1 The “Settings” submenu

#### 4.5.1.1 The “Restore Default” submenu

Use this menu to restore the factory default device settings. After that, the device reboots.



**Management / Settings / Restore Default**

Restore Broadband Router settings to the factory defaults.

**When the operation is completed, all settings will be lost.**

Click *Restore Default Settings* button to restore the default settings. When factory reset is completed, the device will be automatically rebooted.



#### 4.5.2 The “PON Password” submenu. Change the PON access password

Use this menu to change the password for ONT authorization on the PON station device.

**Management / PON Password**  

Use the fields below to enter up to 10 characters and click "Apply/Save" to change or create passwords.  
 Note: Password cannot contain a space.

Current PON Password: 0000000000

New PON Password:

To change the password, enter 10 characters into the *New PON Password* field. Click the *Apply/Save* button to accept and save the changes. Settings will be applied after the device reboot.



**We do not recommend changing password unassisted as it may lead to the loss of communication with the station device.**

#### 4.5.3 The “Internet time” submenu. System Time Settings

**Management / Internet Time**  

This page allows you to the modem's time configuration.

☒ Automatically synchronize with Internet time servers

First NTP time server:	Other	ntp.local
Second NTP time server:	None	
Third NTP time server:	None	
Fourth NTP time server:	None	
Fifth NTP time server:	None	

Time zone offset: (GMT+03:00) Moscow, St. Petersburg, Volgograd

Use this tab to configure system time of the device.

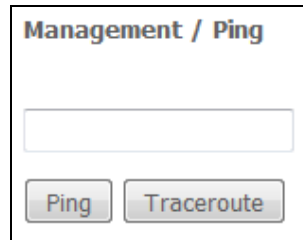
- *Automatically synchronize with Internet time servers*—when checked, enables automatic synchronisation with Internet precision time servers;
- *First NTP time server*—the main precision time server;
- *Second NTP time server*—the second precision time server (none—do not use supplementary servers);
- *Third NTP time server*—the third precision time server (none—do not use supplementary servers);
- *Fourth NTP time server*—the fourth precision time server (none—do not use supplementary servers);
- *Fifth NTP time server*—the fifth precision time server (none—do not use supplementary servers);
- *Time zone offset*—time zone according to UTC.



**Choosing the *Other* option in the drop-down list of servers activates a window to the right where the address of the precision time server should be manually entered.**

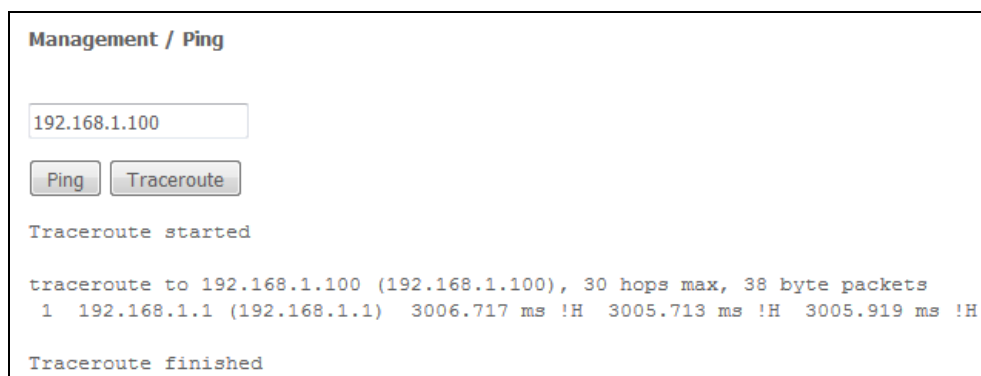
#### 4.5.4 The “Ping” submenu. Test the Availability of Network Devices

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



The screenshot shows the 'Management / Ping' submenu. It features a title bar 'Management / Ping', a text input field, and two buttons labeled 'Ping' and 'Traceroute'.

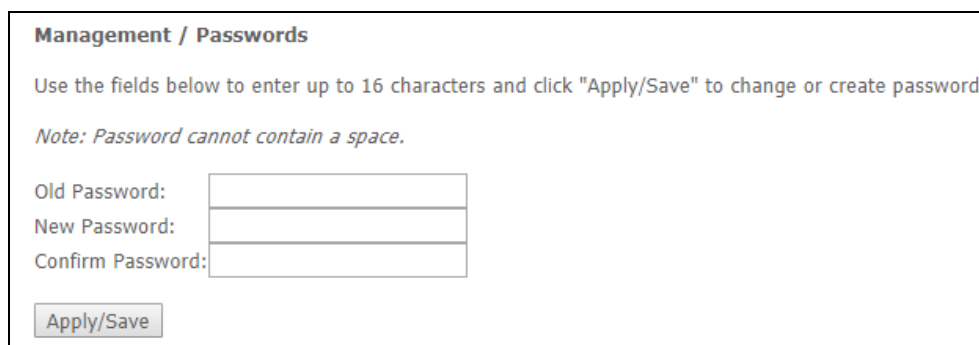
In order to check availability of a connected device, enter its IP address into the field and click the *Ping* button. Click the *TraceRoute* button to view the route tracing. The information will be displayed on this page of the web interface.



The screenshot shows the 'Management / Ping' submenu with the IP address '192.168.1.100' entered in the text field. The 'Ping' button is highlighted. Below the buttons, the text 'Traceroute started' is displayed, followed by a pre-formatted output of a traceroute command: 'traceroute to 192.168.1.100 (192.168.1.100), 30 hops max, 38 byte packets' and a single line of results: '1 192.168.1.1 (192.168.1.1) 3006.717 ms !H 3005.713 ms !H 3005.919 ms !H'. At the bottom, the text 'Traceroute finished' is shown.

#### 4.5.5 The “Password” submenu. Access control configuration (setting passwords)

Use the menu to change a device access password.



The screenshot shows the 'Management / Passwords' submenu. It has a title bar 'Management / Passwords', a paragraph of instructions: 'Use the fields below to enter up to 16 characters and click "Apply/Save" to change or create password.', and a note: 'Note: Password cannot contain a space.'. Below the note are three text input fields labeled 'Old Password:', 'New Password:', and 'Confirm Password:'. At the bottom is an 'Apply/Save' button.

To change the password, enter the current password, then enter a new password and confirm it.

Click the *Apply/Save* button to accept and save the changes.

## 4.5.6 The “System Log” submenu. System Log Review and Configuration

### 4.5.6.1 The “Configuration” submenu. System Log Configuration

Use the menu to configure events occurring on the router.

**Management / System Log / Configuration**

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both', events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both', events will be recorded in the local memory.

Select the desired values and click 'Apply/Save' to configure the system log options.

Log: ☒ Disable ☐ Enable

Log Level: Debugging

Display Level: Error

Mode: Local

Linux Kernel Console  
Display Level (printk): Error

Send CMS logs to syslog (require reboot): ☒ Disable ☐ Enable

Apply/Save

- *System log* – enable/disable system log;
- *Log level* – verbosity of the event log. Severity levels in the descending order:
  - *Emergency*;
  - *Warning*;
  - *Critical*;
  - *Debug*.
- *Display Level* – display level of the event log messages;
- *Operation mode* – log operation mode:
  - *Local* – all events are returned to the router through the buffer;
  - *Remote* – all events are returned to Syslog server;
  - *Both* – both mode are enabled;
  - *USB flash driver* – sending events on the USB flash driver;
- *Linux Kernel Console Display Level (printk)* – displays level of messages in Linux console;
- *Send CMS logs to syslog* – enables/disables CMS messages transmission to the system log.

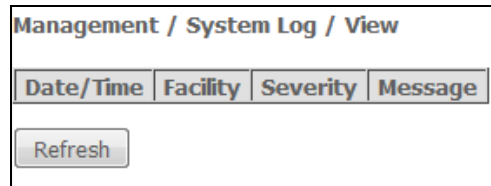
The following settings are available in the *Remote* mode:

- *Server IP address* – IP address of the Syslog server which stores all events;
- *Server UDP port* – port number of the Syslog server.

Click the *Apply/Save* button to accept and save the changes.

#### 4.5.6.2 The “View” submenu. System Log Display

The menu is used to configure display of router's events.



Date/Time	Facility	Severity	Message
-----------	----------	----------	---------

Refresh

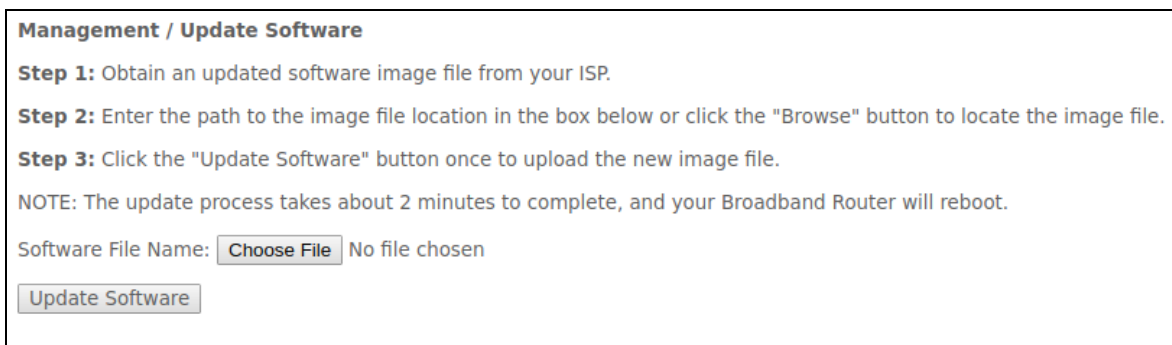
Use the *Refresh* button to refresh the information.

#### 4.5.7 The “Update Software” submenu

In order to update software, select the software in the *Software File name* field (use the *Choose File* button) and click *Update Software*.



**Do not switch off or reboot the device during software update. The firmware update takes a few minutes to complete and then the device will reboot.**



**Management / Update Software**

**Step 1:** Obtain an updated software image file from your ISP.

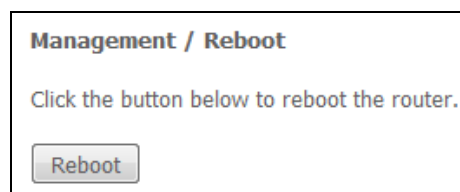
**Step 2:** Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.

**Step 3:** Click the "Update Software" button once to upload the new image file.

NOTE: The update process takes about 2 minutes to complete, and your Broadband Router will reboot.

Software File Name:  No file chosen

#### 4.5.8 The “Reboot” submenu. Device Reboot



**Management / Reboot**

Click the button below to reboot the router.

Click the *Reboot* button to reboot the device. The rebooting process takes a few minutes to complete.

## NTU-RG ACCEPTANCE CERTIFICATE AND WARRANTY

NTU-RG \_\_\_\_\_ optical network terminal with Serial No. \_\_\_\_\_ complies with technical specifications RPTL.465600.108TU and is qualified for operation.

Equipment shipping and storage should be conducted in accordance with GOST 15150 Conditions 5 and Conditions 1 respectively.

The manufacturer, Eltex Enterprise Ltd., guarantees that optical network gateway complies with technical specifications RPTL.465600.108TU under operational conditions described in this manual, which should be maintained by the user.

Warranty period—1 year. Manufacturing date—see on label.

The device does not contain precious materials.

Director

signature

A. N. Chernikov  
full name

Head of the Quality Control Department

signature

S. I. Igonin  
full name

Manufacturer Information:  
Eltex Enterprise Ltd.  
29v Okružhnaya St.,  
Novosibirsk 630020  
E-mail: eltex@eltex-co.ru

Made in Russia

